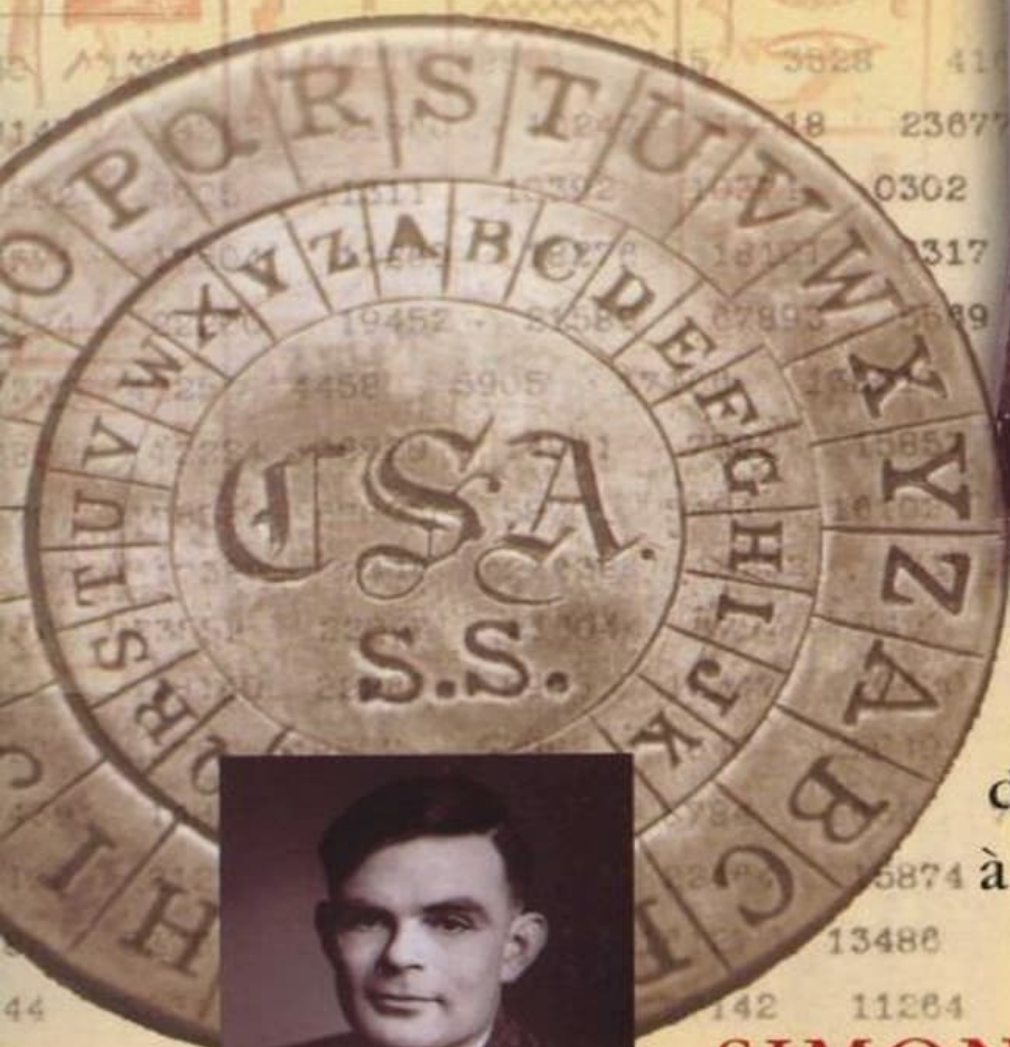


Histoire des codes secrets



De l'Égypte
des Pharaons
à l'ordinateur
quantique

SIMON SINGH

JC Lattès

Simon Singh

HISTOIRE DES CODES SECRETS

De l'Égypte des Pharaons
à l'ordinateur quantique

*Traduit de l'anglais par
Catherine Coqueret*

JC Lattès

Sommaire

Introduction

1 Le chiffre de Marie, reine d'Écosse

2 Le chiffre indéchiffrable

3 La mécanisation du codage

4 À l'attaque d'Enigma

5 La barrière de la langue

6 Alice et Bernard s'affichent en public

7 Pretty Good Privacy.

8 Saut quantique dans le futur

Concours

Annexes

Glossaire

Remerciements

Éléments de bibliographie

Crédits photographiques

Index

Titre de l'édition originale
THE CODE BOOK
publiée en 1999 par Fourth Estate Limited,
6 Salem Road, London W24BU

© Simon Singh, 1999
© 1999, éditions Jean-Claude Lattès pour la
traduction française.

ISBN 978-2-7096-4421-1

Du MÊME AUTEUR

Le Dernier Théorème de Fermat, Lattès, 1998.

*À ma mère et à mon père
Sawaran Kaur et Mengha Singh*

« L'envie de pénétrer les secrets est profondément ancrée dans l'âme humaine — même le moins curieux des esprits s'enflamme à l'idée de détenir une information refusée à d'autres. Certains ont la chance d'exercer un métier qui leur demande d'élucider des mystères, mais la plupart d'entre nous sont réduits, pour satisfaire ce besoin, à résoudre des casse-tête artificiels, inventés pour notre distraction. Les romans policiers et les mots croisés suffisent au plus grand nombre, la résolution des codes secrets peut être la quête de quelques-uns. »

John Chadwick

Le Déchiffrement du Linéaire B

Introduction

Depuis des millénaires, les rois, les reines et les généraux ont dû se doter de moyens de communication efficaces pour gouverner leurs pays ou commander leurs armées. Dans le même temps, ils étaient conscients des risques encourus si leurs messages tombaient entre les mains de l'ennemi. Ce fut la crainte de ces interceptions qui fut à l'origine du développement des codes et des chiffres, techniques utilisées pour déguiser un message afin que seul son destinataire désigné puisse le lire.

Le souci de confidentialité a entraîné les nations à créer des services secrets, chargés d'assurer la sécurité des communications par l'invention et la mise en œuvre des meilleurs codes possibles. Parallèlement, les décodeurs ennemis essayaient de briser ces codes. Les briseurs de code sont des alchimistes de la linguistique, une tribu mystique tentant de convertir des symboles sans signification en mots porteurs de sens. L'histoire des codes et des chiffres est une suite ininterrompue de batailles entre les codeurs et les briseurs de code, une compétition intellectuelle lourde de répercussions sur le cours de l'histoire.

En écrivant l'*Histoire des codes secrets*, j'avais deux objectifs principaux. Le premier était de tracer les grandes lignes de l'évolution des codes. Évolution est un terme tout à fait approprié, car le développement des codes peut être regardé comme un combat évolutif. Un code est soumis à de constantes attaques par les briseurs de code. Lorsque ces derniers ont trouvé une nouvelle arme pour exploiter les faiblesses d'un code, celui-ci cesse d'être utilisable. Ou il disparaît, ou il évolue vers une nouvelle version mieux défendue — qui fonctionnera jusqu'à ce que les décrypteurs aient trouvé son point faible, et ainsi de suite. On peut rapprocher cette situation du combat mené contre des bactéries infectieuses. Les bactéries vivent, se développent et survivent jusqu'à ce que les médecins aient découvert un antibiotique qui les tue. Les bactéries sont alors obligées d'évoluer et de déjouer l'antibiotique et, si elles y parviennent, elles proliféreront à nouveau et se réinstalleront. Les bactéries sont contraintes en permanence à surmonter les attaques des nouveaux antibiotiques.

La lutte incessante entre concepteurs et briseurs de codes a permis une série de remarquables percées scientifiques. Les concepteurs ont cherché à élaborer des codes toujours plus sophistiqués pour protéger les communications, alors que les décrypteurs imaginaient perpétuellement des méthodes plus performantes pour les attaquer. Dans leurs efforts pour préserver ou pénétrer le secret, les deux parties ont utilisé divers champs de disciplines et de technologies, des mathématiques à la linguistique, de la théorie de l'information à la théorie quantique. En retour, ces domaines ont été enrichis par leurs recherches. Leur travail a accéléré le développement technologique, notamment dans le cas de l'ordinateur.

L'histoire est ponctuée de codes qui ont décidé de l'issue de batailles et ont causé la perte de rois ou de reines. Aussi ai-je pu faire appel à des récits d'intrigues politiques et à des affaires entraînant la vie ou la mort pour illustrer les moments décisifs du développement des codes. L'histoire des codes est si riche que j'ai été obligé de laisser de côté maints événements passionnants, et mon relevé est loin d'être exhaustif. Pardon, si j'ai omis votre anecdote préférée ou votre héros favori, mais j'ai établi une bibliographie afin de satisfaire les lecteurs curieux d'étudier le sujet dans tous ses détails.

En dehors de l'évolution des codes et de leur influence sur le cours de l'histoire, le second objectif du livre est de montrer que le sujet est plus actuel que jamais. Alors que l'information prend une importance toujours croissante, et que la révolution dans les communications bouleverse la société, de la même manière le codage des messages, appelé cryptage, jouera un rôle toujours plus grand dans notre vie quotidienne. Aujourd'hui, alors que nos appels téléphoniques rebondissent sur des satellites et que nos *e-mail* passent par divers ordinateurs, ces deux voies peuvent aisément être infiltrées, violant ainsi notre vie privée. Parallèlement, tandis qu'il se fait toujours plus de commerce sur Internet, des défenses doivent être instaurées pour mettre à l'abri les entreprises et leurs clients. Le cryptage est le seul moyen de protéger notre intimité, ou de garantir le succès d'un marché digital. L'art de la communication secrète, aussi appelé cryptographie, fournira à l'âge de l'information ses verrous et ses clefs.

Toutefois, la demande croissante du public en matière de cryptage se heurte à la nécessité d'appliquer les lois et d'assurer la sécurité nationale. Pendant des décennies, la police et les services secrets ont utilisé des écoutes pour rassembler des preuves contre terroristes et syndicats du

crime, mais le récent développement de codes très résistants tend à diminuer l'intérêt de ces enregistrements. À l'aube du XXI^e siècle, les défenseurs des droits individuels poussent à un usage répandu du cryptage pour préserver l'intimité des personnes privées, et l'on trouve dans le même camp les sociétés commerciales qui réclament un cryptage sûr pour Internet. De leur côté, les forces de l'ordre font pression sur les gouvernements pour qu'ils restreignent l'usage du codage. La question est : à quoi attribuons-nous le plus de prix, au respect de notre vie personnelle ou à une police plus efficace ? Et peut-on trouver un compromis ?

Bien que la cryptographie ait maintenant de vastes répercussions sur les activités civiles, la cryptographie militaire demeure un domaine important. On a dit que la Première Guerre mondiale avait été la guerre des chimistes, parce que le gaz moutarde et le chlore y furent employés pour la première fois, et que la Deuxième Guerre mondiale avait été celle des physiciens, en raison de l'explosion de la bombe atomique. De même, on défend quelquefois l'idée que la Troisième Guerre mondiale serait la guerre des mathématiciens, dans la mesure où ceux-ci contrôleront la prochaine arme de guerre déterminante, l'information.

En retraçant l'évolution des codes et leur rôle dans l'histoire, je me suis permis un petit détour. Le chapitre 5 décrit le déchiffrement de diverses écritures anciennes, notamment le Linéaire B et les hiéroglyphes égyptiens. En principe, la cryptographie concerne des communications qui sont délibérément rédigées de façon à être tenues secrètes face à l'ennemi, alors que les écritures anciennes ne cherchaient pas à être indéchiffrables : nous avons simplement perdu la capacité de les lire. Toutefois, les compétences requises pour comprendre le sens de textes archéologiques sont très proches des techniques de déchiffrement. Depuis que j'ai lu *Le Déchiffrement du Linéaire B*, de John Chadwick, qui raconte comment fut éclairci un texte de l'Antiquité méditerranéenne, je suis émerveillé par les prouesses intellectuelles de ces hommes et de ces femmes qui ont réussi à déchiffrer les écritures de nos ancêtres, nous permettant ainsi de découvrir leurs civilisations, leurs religions et leur vie quotidienne.

Je dois m'excuser auprès des puristes pour le titre de ce livre. *L'Histoire des codes secrets* ne parle pas que de codes. Le mot « code » évoque un système particulier pour assurer des communications, système qui est de moins en moins en usage. Un code consiste à remplacer un mot ou une phrase par un autre mot, un nombre ou un symbole. Par

exemple, les agents secrets ont des noms de code, qui sont utilisés à la place de leur nom véritable afin de masquer leur identité. Autre exemple : la phrase « Attaque à l'aube » pourrait être remplacée par le mot de code « Jupiter », et ce mot envoyé à un commandant sur le champ de bataille sans éclairer l'ennemi. Si le quartier général et le commandant se sont préalablement entendus, le sens du mot « Jupiter » sera clair pour son destinataire, mais sa signification inintelligible pour l'ennemi.

Une possibilité autre que le code est le chiffre, technique qui s'applique à un niveau plus fondamental, c'est-à-dire que ce sont les lettres, et non les mots, que l'on change. Ainsi, chaque lettre d'une phrase peut être remplacée par la lettre qui la suit dans l'alphabet : a par B, b par C, etc. Dans ce cas, « Attaque à l'aube » devient « BUUBRVF B M'BVCF ». Les chiffres font partie intégrante de la cryptographie, et ce livre aurait dû s'intituler *Histoire du chiffre et du code secrets*. J'ai décidé de sacrifier la précision à l'efficacité.

Lorsque le besoin s'en fait sentir, je donne une définition des termes techniques utilisés en cryptographie. Il arrivera cependant que j'utilise une expression peut-être techniquement un peu large, mais que j'estime plus compréhensible aux non-spécialistes. Par exemple, pour parler d'une personne s'efforçant de percer un chiffre, il m'arrive d'employer l'expression *briseur de code* au lieu de celle, plus appropriée, de *briseur de chiffre*. Je ne le fais que lorsque le contexte rend les choses évidentes. Un glossaire figure à la fin du livre mais, le plus souvent, le jargon cryptographique est transparent, comme *texte clair* pour le message avant le cryptage, et *texte chiffré* pour le message crypté.

Je voudrais attirer l'attention sur le problème rencontré par tout auteur traitant ce sujet : la cryptographie est, pour une grande part, une science secrète. De nombreux héros de ce livre n'obtinrent jamais de reconnaissance pour leur travail de leur vivant, parce que leur contribution ne pouvait être saluée publiquement aussi longtemps qu'elle était utilisée par les militaires ou les diplomates. J'ai pu toutefois rencontrer des experts du quartier général des communications du gouvernement britannique (GCHQ) qui m'ont fourni des précisions sur une extraordinaire étude faite dans les années 70, et qui venait d'être libérée du classement *secret-défense*. Grâce à cette ouverture, trois des plus grands cryptanalystes au monde peuvent maintenant recevoir les lauriers qu'ils méritent.

Le dernier chapitre de ce livre est consacré à un regard prospectif sur l'avenir des chiffres et des codes. Il s'agit de deviner qui, de l'inventeur de code ou du briseur de code, l'emportera finalement. Les concepteurs de codes créeront-ils jamais un code réellement infrangible, aboutissement de leur quête du secret absolu ? Ou bien les décrypteurs construiront-ils une machine capable de déchiffrer n'importe quel message ? Sachant que certains des cerveaux les plus brillants au monde, disposant de moyens financiers considérables, travaillent dans des laboratoires secrets, je peux imaginer que certaines de mes conclusions du dernier chapitre sont peut-être déjà dépassées. À l'instant où j'affirme que les ordinateurs quantiques — machines capables de briser tous les chiffres utilisés de nos jours — en sont encore à leurs premiers balbutiements, il est possible que quelqu'un en ait déjà construit un. Heureusement pour moi, les seules personnes aptes à relever ce type d'erreur sont précisément celles à qui leur fonction interdit de les révéler.

1

Le chiffre de Marie, reine d'Écosse

Au matin du samedi 15 octobre 1586, Marie Stuart pénétra dans la salle d'audience bondée du château de Fotheringhay. Des années d'emprisonnement et l'apparition de rhumatismes avaient laissé leurs traces sur elle, cependant elle restait digne, calme et indiscutablement royale. Assistée par son médecin, elle s'avança au-delà des juges, des officiels et des spectateurs jusqu'au trône placé au centre de la longue pièce étroite. Marie avait cru que le trône était là pour elle, mais elle s'était trompée. Il symbolisait une absente, l'ennemie qui la poursuivait : la reine Elizabeth. Marie fut doucement entraînée de l'autre côté de la pièce, vers le siège de velours cramoisi destiné à l'accusée.

Marie, reine d'Écosse, était jugée pour trahison. Elle était accusée d'avoir pris part à un complot tendant à assassiner la reine Elizabeth, afin de s'emparer pour elle-même de la couronne d'Angleterre. Sir Francis Walsingham, Premier secrétaire de la reine Elizabeth, avait déjà fait arrêter les autres conspirateurs, avait obtenu leurs aveux et les avait fait exécuter. À présent, il voulait prouver que Marie avait été l'âme du complot et qu'elle méritait également la mort.

Walsingham savait que, pour obtenir la condamnation de Marie, il devait convaincre Elizabeth de sa culpabilité. Si celle-ci détestait Marie, elle avait plusieurs raisons pour hésiter devant une exécution. Premièrement, Marie était reine d'Écosse, et beaucoup se demandaient si une cour anglaise avait autorité pour juger la souveraine d'un État étranger. Deuxièmement, exécuter Marie pouvait créer un précédent. Si l'État était habilité à tuer une reine, on pouvait craindre que des rebelles n'hésitent pas à en tuer une autre. Enfin, Elizabeth et Marie étaient cousines, et cette parenté embarrassait la reine d'Angleterre. Elizabeth n'entérinerait cette exécution que si Walsingham établissait formellement que Marie avait été partie prenante dans le complot.



Fig.1 Marie Stuart, reine d'Écosse.

Celui-ci était l'œuvre d'un groupe de jeunes aristocrates catholiques anglais qui voulaient déposer la protestante Elizabeth de son trône, pour l'y remplacer par Marie, leur coreligionnaire. S'il était évident que Marie était pour les conjurés comme une figure de proue, il n'était pas établi qu'elle leur eût donné sa bénédiction. En réalité, Marie avait bien autorisé le complot. La difficulté, pour Walsingham, était d'apporter la preuve irréfutable d'un lien concret entre elle et les conspirateurs.

Marie était assise, seule, au banc des accusés, vêtue d'une simple robe de velours noir. Dans les affaires de trahison, l'accusé n'avait pas droit à un avocat, ni de faire citer des témoins. On n'avait même pas donné à Marie de secrétaire pour l'aider à préparer sa défense. Pourtant, sa position ne lui apparaissait pas désespérée, car elle avait pris la

précaution de ne correspondre avec les comploteurs qu'en utilisant un chiffre. Ce chiffre transformait ses mots en une série de signes vides de sens, et Marie pensait que, même si Walsingham avait mis la main sur les lettres, il ne pouvait avoir aucune idée de leur teneur et qu'elles ne pourraient donc pas être utilisées contre elle.

Malheureusement pour Marie, Walsingham n'était pas seulement Premier secrétaire, il était aussi le chef de l'espionnage anglais. Il avait intercepté les lettres de Marie, et connaissait l'homme capable de les déchiffrer. Depuis des années, Thomas Phelippes avait déchiffré les messages de tous ceux qui conspiraient contre la reine Elizabeth. S'il pouvait décrypter les lettres échangées entre les conjurés et Marie, alors la mort de celle-ci serait inévitable. Si, au contraire, le chiffre de Marie se révélait assez fort pour protéger ses secrets, elle avait une chance de vivre. Pour la première fois, une vie dépendait directement de la résistance d'un chiffre.

Évolution de l'écriture secrète

Les plus anciens exemples d'écriture codée sont rapportés par Hérodote, qui retrace dans ses *Histoires* les conflits entre la Grèce et la Perse, au V^e siècle avant J.-C. Pour Hérodote, ce fut l'art de l'écriture secrète qui épargna à la Grèce d'être conquise par Xerxès, le monarque perse.

La vieille inimitié entre la Grèce et la Perse entra dans une crise aiguë au moment où Xerxès commençait à construire Persépolis, la nouvelle capitale de son royaume. Des cadeaux et des tributs arrivèrent de tout l'Empire et des États voisins, à l'exception notable d'Athènes et Sparte. Déterminé à punir cette insolence, Xerxès déclara : « Nous étendrons l'empire de la Perse jusqu'à ce que ses frontières se confondent avec le ciel de dieu, afin que le soleil n'éclaire aucune terre au-delà de la nôtre. » Il consacra les cinq années suivantes à rassembler secrètement la plus grande armée jamais connue, et en 480 avant J.-C. s'estima prêt à lancer une attaque surprise.

Cependant, l'armement de la Perse avait été dévoilé par Demaratus, un Grec expulsé de son pays, qui vivait dans la ville perse de Suse. Bien qu'exilé, il demeurait fidèle à la Grèce et décida d'envoyer un message pour prévenir les Spartiates du plan d'invasion de Xerxès. Selon Hérodote, « il y avait grand danger à être découvert. Demaratus ne trouva qu'un seul moyen pour permettre au message de passer : il gratta la cire sur une paire de tablettes de bois pliantes, il inscrivit sur le bois les projets de Xerxès, puis couvrit à nouveau de cire le message. Les tablettes, apparemment vierges, ne soulevèrent aucune réaction chez les gardes tout au long du parcours. Lorsque cet envoi atteignit sa destination, personne n'en devina le secret jusqu'à ce que Cléomène, la fille de Gorgo, épouse de Léonidas, suggère d'enlever la cire afin de découvrir le message. Ce qui fut fait, le message fut révélé, lu, et transmis ensuite à d'autres Grecs. » Cet avertissement poussa les Grecs à s'équiper et à s'armer. Le rapport des mines d'argent, perçu par l'Etat et jusqu'alors partagé entre les citoyens, fut consacré à la construction de deux cents bateaux de guerre.

Xerxès ne bénéficiait donc plus de l'avantage de la surprise, et le 23 septembre 480 avant J.-C., lorsque la flotte perse s'approcha de la baie

de Salamine, près d'Athènes, les Grecs étaient prêts. Ils laissèrent délibérément les bateaux perses pénétrer dans la baie. Les Grecs savaient que leurs bateaux, plus petits et moins nombreux, auraient le dessous en pleine mer, mais qu'à l'intérieur de la baie ils pouvaient l'emporter sur les Perses. Le vent changeant de direction contraignit les Perses à affronter les Grecs sur leur terrain. Le *Princesse Artemis*, entouré sur trois côtés, tenta de regagner la haute mer, mais ne réussit qu'à éperonner un autre bateau de son camp. Une panique s'ensuivit, et d'autres collisions. Les Grecs lancèrent alors une attaque sans merci. En une seule journée, les forces formidables de la Perse avaient été mises en déroute.

La ruse de Demaratus pour assurer le secret de la communication consistait simplement à cacher le message. Hérodote rapporte un autre incident où dissimuler le message suffit à en assurer le secret. Il conte l'histoire d'Histaïaeus qui souhaitait encourager Aristagoras de Milet à se soulever contre le roi de Perse. Histaïaeus rase la tête de son messager, écrit le message sur son crâne, et ensuite attendit que les cheveux repoussent (à cette époque, on n'avait pas la même notion de l'urgence !). Le messager put voyager sans encombre, les mains vides. À l'arrivée, il rase de nouveau son crâne, et le tendit à lire au destinataire.

Le mode de communication secrète obtenu en dissimulant l'existence du message est appelé la *stéganographie*, mot élaboré à partir des mots grecs *steganos*, voulant dire couvert, et *graphein*, écriture. Pendant deux mille ans après Hérodote, des formes diverses de stéganographie ont été utilisées dans le monde entier. Par exemple, dans la Chine ancienne, on écrivait des messages sur une fine soie, qui était ensuite glissée dans une minuscule boule recouverte de cire. Le messager n'avait plus qu'à avaler la boule. Au XVI^e siècle, le scientifique italien Giovanni Porta décrit comment cacher un message dans un œuf dur. On fabrique une encre avec une once d'alun pour une pinte de vinaigre et on l'utilise pour écrire sur la coquille. La solution pénètre à travers la coquille poreuse et dépose sur la surface du blanc d'œuf durci le message qu'on lira aisément après avoir épluché l'œuf. La stéganographie inclut aussi l'usage de l'encre invisible. Dès le I^{er} siècle après J.-C., Pline l'Ancien expliquait comment on fait de l'encre invisible avec le lait de l'euphorbe *tithymallus* : l'encre séchée est transparente, et l'on fait réapparaître le texte, coloré en brun, par un léger chauffage. Beaucoup de fluides organiques riches en

carbone ont la même propriété. Ce fait n'est pas ignoré des espions du XX^e siècle qui ont abandonné l'écriture invisible d'origine classique, pour improviser avec leur propre urine.

La longévité de la stéganographie prouve qu'elle offre un minimum de sécurité, mais elle souffre d'une faiblesse fondamentale : si le messenger est fouillé et le message découvert, le contenu de la communication secrète est immédiatement révélé. L'interception du message suffit à annihiler toute sécurité. Une garde consciencieuse peut fouiller automatiquement toute personne franchissant la frontière, gratter toute tablette cirée, chauffer les feuilles de papier vierges, éplucher les œufs durs, ou bien raser la tête des gens... et le message sera inévitablement découvert.

C'est pourquoi, parallèlement à la stéganographie, se développa la *cryptographie*, du grec *kryptos*, signifiant caché. Le but de la cryptographie n'est pas de dissimuler la présence du message, mais plutôt d'en cacher le contenu, procédé que l'on nomme cryptage. Afin de le rendre incompréhensible, on brouille le message suivant un protocole mis au point préalablement par l'expéditeur et le destinataire. Ce dernier n'aura plus qu'à inverser le procédé pour rendre le message lisible, alors que l'ennemi, s'il ne connaît pas le protocole de brouillage, trouvera difficile, voire impossible, de rétablir le texte original.

Bien que la cryptographie et la stéganographie soient des techniques indépendantes, il est possible de brouiller et de cacher à la fois le message, pour un maximum de sécurité. Par exemple, le micropoint est une forme de stéganographie qui devint courante pendant la Seconde Guerre mondiale. Des agents allemands en Amérique latine réduisirent une page de texte photographiée à un point de moins d'un millimètre de diamètre, et posèrent ensuite ce micropoint au-dessus du point final dans une lettre apparemment anodine. Ce fut en 1941 que le FBI repéra le premier micropoint, en appliquant une directive qui conseillait d'observer le moindre miroitement sur la surface d'une lettre, révélateur d'un film. Bientôt les Américains purent lire le contenu de la plupart des micropoints interceptés, sauf lorsque les agents allemands avaient pris la précaution supplémentaire de brouiller le message avant de le réduire en micropoint. Dans ces cas où la cryptographie se combinait à la stéganographie, les Américains étaient parfois capables d'intercepter les communications sans réussir à en tirer des informations sur les activités de l'espionnage allemand. De ces deux modes de communication

secrète, la cryptographie est évidemment la plus performante car elle dissimule à l'ennemi le sens du message.

On peut diviser à son tour la cryptographie en deux branches, la *transposition* et la *substitution*. Dans la transposition, les lettres du message sont simplement redistribuées, engendrant un anagramme. Pour de très brefs messages, comme un simple mot, cette méthode est peu sûre car il n'y a guère de variantes pour redistribuer une poignée de lettres. Par exemple un mot de trois lettres ne peut être tourné que dans six positions différentes, ainsi *col* ne peut se transformer qu'en *col*, *clo*, *ocl*, *olc*, *lco*, *loc*. Bien entendu, lorsque le nombre de lettres croît, le nombre d'arrangements se multiplie rapidement, et il devient impossible de retrouver le texte original sans connaître le procédé de brouillage. *Par exemple, regardez cette courte phrase*. Elle ne comporte que 35 lettres, et pourtant il y a plus de 50 000 000 000 000 000 000 000 000 000 000 possibilités de les disposer. Si une personne pouvait vérifier une disposition par seconde, et si toute la population du globe y travaillait jour et nuit, cela prendrait plus de mille fois la durée de vie de l'univers pour vérifier tous les arrangements.

Une transposition des lettres au hasard semble offrir un très haut niveau de sécurité, puisqu'il serait presque impossible pour un intercepteur de déchiffrer même une courte phrase. Mais il y a un inconvénient. La transposition engendre un anagramme extrêmement difficile et si les lettres sont mises pêle-mêle, sans rime ni raison, débrouiller l'anagramme sera aussi difficile pour le destinataire que pour l'intercepteur. Pour que la transposition soit efficace, l'ordonnancement des lettres doit suivre un système rigoureux, sur lequel expéditeur et destinataire se sont préalablement entendus. Les écoliers s'amusent ainsi à s'envoyer des messages avec une transposition dite « en dents de scie ». Il s'agit d'écrire le message sur deux lignes, une lettre sur la ligne supérieure, une lettre sur la ligne inférieure. On enchaîne ensuite la suite des lettres de la ligne inférieure à celle de la ligne supérieure, pour réaliser le message crypté, comme ci-dessous :

TON SECRET EST TON PRISONNIER ; S'IL FUT TU DEVIENDRAS SON PRISONNIER
↓
T N E R T S T N R S N I R I F I T D V E D A S N R S N I R
O S C E E T O P I O N E S L U T U E I N R S O P I O N E
↓
T N E R T S T N R S N I R I F I T D V E D A S N R S N I R O S C E E T O P I O N E S L U T U E I N R S O P I O N E

Le destinataire n'aura qu'à inverser le procédé. Il y a diverses autres formes de transposition systématique, incluant d'écrire ce message en dents de scie sur trois lignes au lieu de deux, et de les enchaîner ensuite de la même façon. On peut aussi faire jouer des paires de lettres, afin que la première et la deuxième échangent leur place, de même pour la troisième et la quatrième et ainsi de suite. Une autre forme de transposition utilise le premier dispositif de cryptographie militaire connu, la *scytale* spartiate, remontant au V^e siècle avant J.-C. La scytale consiste en un bâton de bois autour duquel est enroulée une bande de cuir ou de parchemin, comme le montre la [figure 2](#). L'expéditeur écrit son message sur toute la longueur de la scytale et déroule ensuite la bande qui apparaît alors couverte d'une suite de lettres sans signification. Le messenger emportera la bande de cuir et, l'ayant roulée en torsade, l'utilisera parfois comme ceinture, les lettres restant cachées à l'intérieur. En 404 avant J.-C., Lysandre de Sparte vit arriver un messenger ensanglanté, l'un des cinq survivants d'un éprouvant voyage depuis la Perse. Le messenger tendit sa ceinture à Lysandre qui l'entoura autour de sa scytale et apprit que Pharnabaze de Perse s'apprêtait à l'attaquer. Grâce à la scytale, Lysandre se prépara à cette attaque et la repoussa.

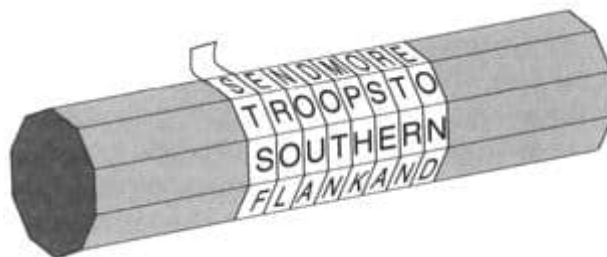


Fig. 2 Lorsqu'on enlève de la scytale la lanière de cuir, celle-ci semble porter une suite de lettres incohérente. La lanière devra être enroulée autour d'une autre scytale de même diamètre pour que le message se recompose.

Une possibilité autre que la transposition est la substitution. L'une des premières descriptions de cryptage par substitution apparaît dans le *Kàma-sùtra*, texte écrit au v^e siècle *après* J.-C. par le brahmane Vàtsyàyana, mais fondé sur des manuscrits du IV^e siècle *avant* J.-C. Le *Kàma-sùtra* recommande que les femmes apprennent soixante-quatre arts, entre autres cuisiner, s'habiller, masser et élaborer des parfums. La liste comprend aussi quelques domaines moins évidents, comme la prestidigitation, les échecs, la reliure et la tapisserie. Le numéro 45 sur la liste est le *mlecchita-vikalpà*, l'art de l'écriture secrète, qui doit leur permettre de dissimuler leurs liaisons. L'une des techniques conseillées

consiste à apparier au hasard les lettres de l'alphabet et à substituer ensuite dans le message original la nouvelle lettre de la paire à celle d'origine. Si nous appliquons ce procédé à notre alphabet, nous pouvons apparier les lettres comme suit :

A	D	H	I	K	M	O	R	S	U	W	Y	Z
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
V	X	B	G	J	C	Q	L	N	E	F	P	T

Ainsi au lieu d'écrire « rendez-vous à minuit », l'expéditeur écrira LUSXUT-AQEN V CGSEGZ. Cette forme est appelée un chiffre de substitution, car chaque lettre du texte original est remplacée par une lettre différente, complétant ainsi l'action du chiffre de transposition. La transposition conserve à chaque lettre son identité, mais change sa position, alors que la substitution change l'identité de chaque lettre, mais lui garde sa position.

Le premier usage révélé d'un chiffre de substitution dans un contexte militaire apparaît dans la *Guerre des Gaules*, de Jules César. César raconte comment il envoya un jour un cavalier gaulois porter une lettre à Cicéron qui était assiégé dans son camp sur la Sambre, et sur le point de se rendre. César lui annonçait qu'il arrivait à son secours avec des légions. La substitution consista à remplacer les lettres romaines par des lettres grecques, rendant ainsi le message, s'il était saisi, incompréhensible pour l'ennemi. César rapporte les péripéties de la remise du message : « Les instructions au messenger furent, s'il ne pouvait approcher, de jeter un javelot portant la lettre attachée à sa courroie à l'intérieur du camp retranché. Craignant un danger, le Gaulois lança le javelot, comme on l'en avait instruit. Le hasard le fit se ficher dans la tour, et nos troupes ne le virent pas pendant deux jours. Le troisième jour, un soldat l'aperçut, le descendit et le porta à Cicéron. Celui-ci lut la lettre et la proclama ensuite aux troupes rassemblées, pour la plus grande joie de tous. »

César utilisa si souvent des écritures cryptées que Valerius Probus écrivit sur ses chiffres un traité complet, qui ne nous est malheureusement pas parvenu. Mais dans les *Vies des douze Césars* de Suétone, nous avons une description détaillée de l'un des chiffres de substitution utilisés par Jules César. Celui-ci remplaçait simplement chaque lettre du message par la lettre venant trois places après elle dans

l'alphabet. Les cryptographes s'expriment souvent en termes d'*alphabet clair*, l'alphabet utilisé pour écrire le message original, et *alphabet chiffré*, pour les lettres substituées à celles d'origine. Lorsqu'on place l'alphabet clair au-dessus de l'alphabet chiffré, comme sur la [figure 3](#), on voit bien que l'alphabet chiffré a été décalé de trois lettres. Depuis, ce type de substitution est souvent appelé chiffre décalé de César ou simplement *chiffre de César*. Chiffre est le nom donné à toute forme de substitution cryptographique, dans laquelle chaque lettre est remplacée par une autre ou par un symbole.

alphabet clair	a b c d e f g h i j k l m n o p q r s t u v w x y z
alphabet chiffré	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
texte clair	veni, vidi, vici
texte chiffré	YHQL, YLGL, YLFL

Fig.3 Chiffre de César appliqué à un court message. Ce chiffre est fondé sur un alphabet chiffré qui est décalé d'un certain nombre de places (ici, trois) par rapport à l'alphabet usuel. En cryptographie, la convention veut que l'on écrive l'alphabet usuel en minuscules et l'alphabet chiffré en majuscules. De même, le message original, ou texte clair, est écrit en minuscules et le message crypté, ou texte chiffré, est écrit en majuscules.

Bien que Suétone ne mentionne qu'un glissement de trois lettres chez César, il est clair qu'en appliquant cette méthode entre une lettre et les vingt-cinq autres, on peut obtenir 25 chiffres différents. En fait, si nous ne nous en tenons pas à faire glisser les lettres de l'alphabet mais que nous nous permettons de recréer un alphabet chiffré en disposant les lettres de toutes les manières possibles, nous obtiendrons un nombre bien plus élevé de chiffres différents. Il y a plus de 400 000 000 000 000 000 000 000 000 redistributions possibles, ce qui engendre un nombre similaire de procédés de chiffrement.

Chaque chiffre peut être envisagé dans les termes d'une méthode générale de cryptement, appelée *algorithme*, et d'une clef, qui fixe avec précision les détails d'un cryptage particulier. Dans ce cas, l'algorithme entraîne la substitution de chaque lettre de l'alphabet clair par une lettre d'un alphabet chiffré, et cet alphabet chiffré peut être établi par n'importe quelle redistribution de l'alphabet clair. La clef fixe l'alphabet chiffré précis utilisé pour un texte crypté défini. La relation entre algorithme et clef est illustrée par la [figure 4](#).

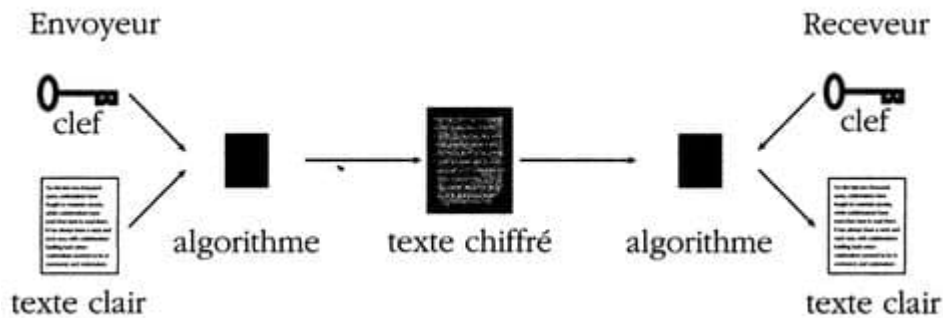


Fig. 4 Pour crypter un message, l'envoyeur passe par un algorithme de cryptage. L'algorithme est un système général de cryptage, et doit être précisé par une clef. Appliquer la clef et l'algorithme ensemble à un texte clair engendre un message crypté, ou texte chiffré. Celui-ci peut être intercepté par l'ennemi au cours de sa transmission, mais l'ennemi ne sera pas en mesure de le déchiffrer. Le receveur, qui connaît la clef et l'algorithme utilisés par l'envoyeur, est capable de reconstituer le texte clair du message.

En général, si l'ennemi intercepte un message crypté, il peut assez facilement appréhender l'algorithme, mais il ne connaît pas la clef. Il peut se douter que chaque lettre du texte clair a été remplacée par une lettre différente, en appliquant un certain alphabet chiffré, mais il a peu de chances de savoir lequel a été utilisé. Si la clef est tenue secrète entre l'expéditeur et le destinataire, alors l'ennemi ne peut déchiffrer le message intercepté. L'importance de la clef, par rapport à l'algorithme, est un principe de base de la cryptographie qui fut définitivement établi en 1883 par le linguiste hollandais Auguste Kerckhoffs Van Nieuwenhof dans son traité *La cryptographie militaire*. Principe de Kerckhoffs : « La sécurité d'un système de cryptement ne doit pas dépendre de la préservation du secret de l'algorithme. La sécurité ne repose que sur le secret de la clef. »

En plus du secret absolu sur la clef, un chiffre bien sécurisé doit avoir tout un choix de clefs possibles. Par exemple, si l'envoyeur utilise le chiffre décalé de César pour un message, le cryptage s'avère assez faible, car il y a que 25 clefs potentielles. Du point de vue de l'ennemi, s'il intercepte le message et soupçonne que l'algorithme utilisé est celui de César, il n'aura à essayer que 25 possibilités. Alors que si l'envoyeur utilise un principe de substitution plus général, qui permette à l'alphabet chiffré d'être constitué des lettres de l'alphabet clair dans n'importe quel ordre, il faudra chercher la clef entre 400 000 000 000 000 000 000 000 000 possibilités. Pour l'ennemi, si le message est intercepté et l'algorithme connu, il reste face à l'invraisemblable défi de tester toutes ces clefs. Si un agent ennemi pouvait vérifier une clef par seconde, cela lui prendrait environ un milliard de fois la durée de vie de l'univers pour les essayer toutes et déchiffrer le message.

alphabet clair	a b c d e f g h i j k l m n o p q r s t u v w x y z
alphabet chiffré	J L P Q W I Q B C T R Z Y D S K E G F X H U O N V M
texte clair	e t t u, B r u t e ?
texte chiffré	W X X H, L G H X W ?

Fig. 5 Exemple d'algorithme de substitution monoalphabétique dans lequel chaque lettre du texte clair est remplacée par une autre lettre selon une clef. La clef est définie par l'alphabet chiffré, qui peut être n'importe quelle distribution de l'alphabet clair.

La beauté de ce genre de chiffre réside dans sa simplicité d'application, jointe à un haut niveau de sécurité. Il est facile de fixer une clef qui consiste simplement à décider de l'ordre des 26 lettres dans l'alphabet chiffré et il est en même temps pratiquement impossible pour l'ennemi de vérifier toutes les clefs, d'où une force de frappe qualifiée de brute. La simplicité de la clef est importante car les deux correspondants doivent la connaître et plus elle est simple, moins il y a de possibilités d'erreur.

En fait il est possible d'appliquer une clef encore plus simple, si l'on accepte une légère réduction du nombre des clefs potentielles. Au lieu de redispenser au hasard les lettres de l'alphabet clair, on choisit un *mot-clef*, ou une *phrase-clef*. Par exemple, prenons « Julius Caesar » comme phrase-clef, et commençons par supprimer les espaces et les lettres qui sont répétées (JULISCAER). Utilisons la suite obtenue comme début de l'alphabet chiffré. Le reste de l'alphabet chiffré n'est que le résultat d'un simple enchaînement qui commence où finit la phrase-clef, en omettant les lettres qui figurent déjà dans celle-ci. Ainsi l'alphabet chiffré se présentera comme suit :

alphabet clair	a b c d e f g h i j k l m n o p q r s t u v w x y z
alphabet chiffré	J U L I S C A E R T V W X Y Z B D F G H K M N O P Q

L'avantage d'un alphabet chiffré conçu sur ce modèle réside dans la facilité de se rappeler le mot-clef ou la phrase-clef, et donc de mémoriser aisément l'alphabet chiffré. C'est important, car si les correspondants doivent le porter par écrit, l'ennemi peut mettre la main sur le papier et déchiffrer toutes les communications écrites sur cette base. Si la clef peut être gardée en tête, il y a moins de chances pour qu'elle parvienne à l'ennemi. Évidemment le nombre des principes de chiffrement engendrés par des phrases-clefs est moins grand que le nombre de ceux créés sans restriction, mais il est tout de même très élevé et il serait impossible à l'ennemi de déchiffrer un message saisi en essayant toutes les phrases possibles.

C'est à cause de sa simplicité et de sa force que le principe de substitution a dominé la technique des écritures masquées pendant le premier millénaire après J.-C. On avait là un moyen de communication sûr, et l'on ne sentait pas le besoin d'un développement plus poussé. Sans nécessité, pas de motivation pour une nouvelle invention. La balle était maintenant dans le camp des briseurs de code, qui essayaient de faire céder le chiffre de substitution. N'y avait-il vraiment pas moyen pour l'intercepteur de déchiffrer le message crypté ? Nombre de savants de l'Antiquité tenaient le principe de substitution pour inviolable, grâce à la multiplicité de combinaisons possibles, et pendant des siècles les faits semblèrent leur donner raison. Mais les décodeurs finirent par trouver un raccourci à l'épuisante recherche de toutes les clefs. Au lieu de prendre des milliards d'années, briser un chiffre n'était plus qu'une affaire de minutes. Cette découverte se fit en Orient et demanda la rencontre miraculeuse de la linguistique, des statistiques et de la dévotion religieuse.

Les cryptanalystes arabes

À l'âge d'environ quarante ans, Mahomet prit l'habitude de se rendre régulièrement dans une grotte du mont Hira, à côté de La Mecque. C'était une retraite, un lieu pour la prière, la méditation et la contemplation. Ce fut pendant ces périodes de profonde réflexion, vers 610, que l'archange Gabriel apparut à Mahomet, et proclama qu'il devait se faire le messager de Dieu. Cette révélation fut la première d'une série qui se poursuivit jusqu'à la mort du Prophète, quelque vingt ans plus tard.

Ces révélations furent consignées par divers scribes pendant la vie du Prophète, mais seulement par fragments, et le soin fut laissé à Abu Bakr, premier calife de l'Islam, de les réunir en un seul texte. Ce travail fut poursuivi par Umar, le deuxième calife et par sa fille Hafsa, et achevé par Othman, le troisième calife. Chacune des révélations constitua l'un des 114 chapitres du Coran. Le calife au pouvoir devait poursuivre l'œuvre du Prophète, soutenir ses enseignements et répandre sa parole. Entre la désignation d'Abu Bakr en 632 et la mort du quatrième calife, Ali, en 661, l'islam se développa jusqu'à ce que la moitié du monde soit d'obédience musulmane. En 750, après un siècle de consolidation, l'apparition de la dynastie des califes abbassides marqua le début de l'âge d'or de la civilisation islamique. Arts et sciences se développèrent également. Les artisans islamiques nous ont laissé des peintures murales magnifiques, des ornements somptueusement sculptés et les tissages les plus élaborés de l'histoire, cependant que la présence de quantité de mots arabes — tels algèbre, alcalin, zénith... — dans la terminologie scientifique nous rappelle l'apport des savants.

La richesse de la culture islamique était, pour une grande part, le résultat d'une époque de prospérité et de paix. Moins soucieux de conquêtes que leurs prédécesseurs, les califes abbassides préférèrent se consacrer à l'établissement d'une société organisée et riche. Des impôts plus faibles encourageaient l'activité économique, en même temps que des lois sévères réprimaient la corruption et protégeaient les citoyens. Le tout reposait sur une administration efficace et qui avait souvent recours au cryptage pour assurer la sécurité de ses communications. Outre les délicates affaires d'État, des documents montrent que les officiels usaient

aussi du secret pour les levées d'impôts. D'autres preuves nous sont fournies par de nombreux manuels administratifs, comme, au x^e siècle, le manuel du secrétaire, *Adab-al-Kuttab*, qui contient une partie consacrée à la cryptographie.

Les fonctionnaires utilisaient couramment un alphabet chiffré qui n'était qu'une redistribution de l'alphabet clair, comme nous l'avons vu plus haut, mais ils employaient aussi des chiffres comportant d'autres symboles. Par exemple, *a* dans l'alphabet clair peut être remplacé par # dans l'alphabet chiffré, *b* par + et ainsi de suite. Le chiffre de substitution monoalphabétique est le nom générique donné à tout principe de substitution qui remplace les lettres de l'alphabet clair par d'autres lettres ou des symboles. Tous les chiffres de substitution que nous avons rencontrés jusqu'ici dans ce livre relèvent de cette catégorie.

Si les Arabes s'étaient contentés de faire usage du principe de substitution, ils ne mériteraient pas une mention particulière dans l'histoire de la cryptographie. Mais les Arabes parvinrent à rompre les chiffres. Ils inventèrent la *cryptanalyse*, ou capacité à décrypter un message sans en connaître la clef. Les cryptanalystes arabes réussirent à trouver le moyen de briser le chiffre de substitution alphabétique, resté inviolé pendant plusieurs siècles.

La cryptanalyse ne pouvait être inventée que par une civilisation ayant atteint un niveau élevé de connaissance dans plusieurs disciplines, dont les mathématiques, les statistiques et la linguistique. L'Islam demande des lumières dans toutes les sphères de l'activité humaine, et atteindre ce but réclame la connaissance ou *ilm*. Chaque musulman doit essayer d'appréhender tous les domaines et le succès économique des califats abbassides permit aux érudits d'avoir le temps, l'argent et les moyens nécessaires pour atteindre leur but. Ils s'approprièrent les avancées des civilisations précédentes en se procurant des textes égyptiens, babyloniens, indiens, chinois, farses, syriens, arméniens, hébreux et romains, qu'ils traduisirent en arabe. En 815, le calife Al-Màmun créa à Bagdad la *Bait al-Hikmah* (Maison de la Sagesse), réunissant une bibliothèque et un centre de traduction.

Au fur et à mesure qu'elle acquérait ces connaissances, la civilisation islamique était aussi en mesure de les répandre, grâce à la fabrication du papier apprise des Chinois. La manufacture de papier engendra la profession de *warraqueen*, ou « manipulateurs de papier », véritables

machines à photocopier humaines qui copiaient les manuscrits et les fournissaient à l'industrie naissante de l'édition. Des dizaines de milliers de livres étaient ainsi publiés chaque année, et dans un seul quartier de Bagdad on relevait plus de cent librairies. À côté de classiques comme *Les Mille et Une Nuits*, ces librairies vendaient des ouvrages sur tous les sujets imaginables, et contribuaient à la formation de la société la plus cultivée au monde.

Mais l'invention de la cryptanalyse repose aussi sur le développement de l'érudition religieuse. D'importantes écoles de théologie furent créées à Basra, Kufa et Bagdad, où des théologiens étudiaient les révélations de Mahomet telles qu'elles se présentaient dans le Coran. Ils souhaitaient reconstituer la chronologie des révélations, qu'ils établissaient en comptant la fréquence des mots contenus dans chaque texte. La théorie était que l'usage de certains mots étant relativement récent, si une révélation contenait un nombre important de ces mots, cela indiquait que sa place dans la chronologie était tardive. Les théologiens étudiaient aussi le *Hadith*, qui rassemble les propos quotidiens du Prophète. Ils tentaient de démontrer que chaque sentence pouvait être réellement attribuée à Mahomet et étudiaient pour cela l'étymologie des mots et la construction des phrases, afin de vérifier si certains textes étaient bien conformes à la forme linguistique de l'expression du Prophète.

D'une manière significative, les études religieuses ne se limitèrent pas à l'examen des mots. Elles analysèrent aussi les lettres individuellement, et découvrirent en particulier que certaines lettres étaient plus utilisées que d'autres. Les lettres *a* et *l* sont les plus courantes en arabe, en particulier à cause de l'article *al*, alors que la *lettre j* apparaît dix fois moins souvent. Cette observation apparemment anodine conduira à la première grande découverte en cryptanalyse.

dans les archives ottomanes d'Istanbul, est intitulé *Manuscrit sur le déchiffrement des messages cryptographiques*. Bien qu'il comporte des commentaires détaillés sur les statistiques, la phonétique et la syntaxe arabes, l'essentiel de son système tient en deux courts paragraphes :

Une façon d'élucider un message crypté, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte en clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre. Nous appellerons la lettre apparaissant le plus souvent la « première », la suivante la « deuxième », la suivante la « troisième », et ainsi de suite pour chaque lettre figurant dans le texte.

Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et nous relevons de même ses symboles. Nous remplaçons le symbole le plus fréquent par la lettre « première » du texte clair, le suivant par la « deuxième », le suivant par la « troisième », et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre.

Pour plus de clarté, transposons l'explication d'Al-Kindi dans le cadre de notre alphabet. Il est nécessaire d'étudier un texte en français banal assez long — peut-être même plusieurs — afin d'établir la fréquence de chaque lettre de l'alphabet. En français, *e* est la lettre la plus répandue, suivie par *a*, puis par *i*, comme le montre le [tableau 1](#). Maintenant, examinons le texte chiffré en question, et appliquons cette table des fréquences. Si la lettre la plus présente dans le texte chiffré est *J*, il semblera probable qu'il est mis pour *e*. Et si la deuxième lettre la plus fréquente est *P*, c'est sans doute en remplacement de *a*, et ainsi de suite. Grâce à la technique d'Al-Kindi, appelée *analyse des fréquences*, il n'est plus nécessaire de vérifier chacune des milliards de clefs potentielles, il est possible de découvrir le contenu d'un message brouillé simplement en analysant la fréquence des caractères dans le texte chiffré.

Lettre	%
A	9,42

B	1,02
C	2,64
D	3,39
E	15,87
F	0,95
G	1,04
H	0,77
I	8,41
J	0,89
K	$\approx 0,00$
L	5,34
M	3,24
N	7,15
O	5,14
P	2,86
Q	1,06
R	6,46
S	7,90
T	7,26
U	6,24
V	2,15

W	≈ 0,00
X	0,30
Y	0,24
Z	0,32

Tableau 1 Cette table de fréquences est basée sur des textes provenant de journaux ou de romans, pour un échantillonnage d'environ 10 000 caractères.

Toutefois il n'est pas possible d'appliquer systématiquement la recette d'Al-Kindi, car les fréquences du [tableau 1](#) ne représentent qu'une moyenne, et ne répondront pas aux fréquences dans chaque texte. Par exemple, un court message faisant état des effets de l'atmosphère sur les mouvements de quadrupèdes rayés en Afrique, faussera l'analyse de fréquence : « De Zanzibar à la Zambie et au Zaïre, des zones d'ozone font courir les zèbres en zigzags zinzins ! » En général, plus un texte est court, plus il s'éloignera des fréquences standard, et s'il comporte moins d'une centaine de lettres, le message s'avérera difficile à déchiffrer. Des textes plus longs ont davantage de chances de suivre les fréquences moyennes, mais ce n'est pas toujours le cas. En 1969, Georges Perec écrivit un roman de 200 pages, *La Disparition*, qui n'employait pas un seul mot contenant la lettre e. Encore plus remarquable est le fait que le critique et romancier anglais Gilbert Adair réussit à traduire *La Disparition* en anglais, en respectant le principe de Perec. Intitulée *A void*, la traduction d'Adair est parfaitement lisible (voir Annexe A). Si le livre entier était crypté sur la base d'un code de substitution alphabétique, une tentative de déchiffrement simple aboutirait à une impasse, en raison de la disparition totale de la lettre la plus couramment utilisée d'ordinaire.

Ayant exposé le premier outil de la cryptanalyse, je poursuivrai avec un exemple montrant l'utilisation de l'analyse des fréquences dans le déchiffrement d'un texte. J'ai essayé de ne pas parsemer ce livre d'exemples de cryptanalyse, mais j'aimerais faire une exception pour l'analyse des fréquences parce qu'elle constitue l'outil de base de la cryptographie, et que je crois utile de montrer son fonctionnement et d'entrer ainsi dans l'esprit du cryptanalyste. Si l'analyse requiert un

raisonnement logique, on verra qu'elle demande aussi un certain degré d'astuce, d'intuition, de souplesse et de conjectures.

Cryptanalyse d'un texte chiffré

Imaginons que nous avons intercepté le message chiffré transcrit ci-dessous. Nous savons que le texte est en français et qu'il a été brouillé grâce à un chiffre de substitution alphabétique, mais nous n'avons aucune idée de la clef. Nous allons donc appliquer l'analyse des fréquences. Ce qui suit vous guidera pas à pas dans la cryptanalyse du texte chiffré, mais, si vous préférez, vous pouvez tenter de faire cette analyse tout seul.

BAELXEJ JCKJ ZA JANBH HSXGXWXL XMXPJ LCEEA XK
GCP JGCPH DPOH. FKXEL AOOA AKJ JAGNPEA
O'SPHJCPGA LA NX'GKD OA HXMAJPAG, AOOA HA
OAMX, YXPXH OA HCO LAMXEJ OA HCKMAGXPE AJ
OKP LPJ : « IGXEL GCP, LABKPH NPOOA AJ KEA
EKPJH RA J'XP GXZCEJA OAH GAZPJH LA O'XEZPAE
JANBH AJ OAH OAIAELAH LAH GCPH BXHHAH.
BKPH-RA NA BAGNAJJGA LA HCOOPZPJAG KEA
DXMAKG LA MCJGA NXRAHJA ? »
ABPOCIKA-ZCEJAH LAH NPOOA AJ KEA EKPJH

Le premier réflexe de n'importe quel cryptanalyste va être d'analyser la fréquence des lettres, avec le résultat suivant :

Lettre	Fréquence	
	Occurences	%
A	61	19,5
B	8	2,4
C	14	4,5
D	3	1,0
E	19	6,1

F	1	0,3
G	18	5,7
H	28	8,9
I	3	1,0
J	28	8,9
K	16	5,1
L	15	4,8
M	7	2,2
N	9	2,9
O	23	7,3
P	26	8,3
Q	0	0
R	3	1,0
S	2	0,6
T	0	0
U	0	0
V	0	0
W	1	0,3
X	20	6,4
Y	3	1,0
Z	6	1,9

Tableau 2 Analyse de fréquences du message codé

Comme on pouvait s’y attendre, les fréquences des lettres sont très variables. La question est : pouvons-nous, grâce à elles, identifier certaines des lettres d’origine ? Le texte chiffré est assez court, aussi ne pouvons-nous pas nous fier absolument à l’analyse des fréquences. Il serait aventureux d’affirmer que la lettre A, la plus répandue dans le texte chiffré, est mise pour la lettre *e*, la plus répandue en français, ou que la huitième lettre la plus rencontrée, le G, est mis pour la huitième lettre la plus fréquente en français, à savoir le *u*. Une application automatique des concordances nous donnerait du charabia. Le premier mot par exemple BAELXEJ nous *donnerait peronra*.

Toutefois, si nous nous fixons sur les trois lettres qui apparaissent le plus souvent, soit A, H et J, nous pouvons supposer que ces lettres les plus présentes dans le texte chiffré correspondent aussi aux trois lettres les plus fréquentes en français, bien que pas nécessairement dans le même ordre. Imaginons donc que :

A = e, a ou i
H = e, a ou i
J = e, a ou i

Afin de renforcer notre raisonnement, nous allons procéder à une analyse plus subtile. Au lieu de relever simplement la présence de ces lettres, nous allons voir si on les rencontre plusieurs fois à côté d'une même autre lettre. Par exemple, la lettre A apparaît-elle plus souvent avant ou après certaines lettres ? La réponse à cette question sera une bonne indication pour juger si A est mis pour une voyelle ou une consonne. Par exemple, on sait que la lettre *e* peut se trouver avant ou après presque toutes les consonnes, mais que la lettre *t* a peu de chances d'accompagner *b, d, f, g, k, m, q, v*

Dans le tableau ci-dessous, on choisit les trois lettres les plus présentes dans le texte crypté A, H et J et l'on note leur nombre d'apparitions à l'intérieur des mots avant ou après chaque lettre de l'alphabet crypté :

[illegible]

La lettre A par exemple apparaît à côté de plus de la moitié des lettres (13) et il n'y en a que 8 qu'elle évite totalement (les lettres ne figurant pas dans le texte, telles Q, T, U, V, n'étant pas comptées). Ceci permet de penser que la lettre A est sans doute mise pour une voyelle. La présence très importante de cette lettre, rapportée à la fréquence des lettres en français où le *e* figure en tête avec un pourcentage d'apparitions très grand par rapport aux suivantes (*e* : 15,87 % ; *a* : 9,42 % ; *i* : 8,41 %) nous incite à essayer le *e* pour le A.

Notons que le A se trouve 13 fois à côté du O, en particulier dans des mots courts OA, AOOA, OAH. Le O apparaît donc doublé, et susceptible d'être placé avant et après la même voyelle *e*. Le O est probablement une consonne, qui intervient dans des articles ou des auxiliaires, mots brefs et répétés. Si nous écrivons :

OA, AOOA, OAH
- e, e - - e, - e -

nous avons envie de compléter avec un l. Le H serait alors un s, ce qui n'est pas invraisemblable compte tenu de sa présence à côté des autres lettres. Un coup d'œil au texte crypté nous montre de nombreux H en fin de mot, ce qui paraît raisonnable puisque le *s* termine les noms au pluriel.

OA, AOOA, OAH
le, elle, les

La lettre J apparaît 12 fois à côté du A, en particulier dans un mot de deux lettres AJ que l'on relève 4 fois. AJ peut figurer pour *en* ou *et*, puisque *es* est exclu si H = s. S'appuyer sur des mots d'une ou deux lettres est un truc utilisé couramment en cryptographie et qui rend de grands services. Cela nous est facile dans notre exemple, mais dans la réalité les cryptographes ne font pas ce genre de cadeau et télescopent les mots sans laisser entre eux le moindre blanc.

Puisque nous bénéficions des espaces, réfléchissons aussi que certaines lettres sont plus souvent accolées que d'autres en français. Le *e* ne touche que rarement les autres voyelles (dans œil, si, exemple a contrario). Le *d* et le *m* sont près du *e* dans 75 % des cas et le *l* dans plus de 50 % des cas. Il est rare de trouver quatre consonnes ou plus à la suite.

Dans ce cas, la dernière sera nécessairement le *s* du pluriel. Quant aux lettres doubles, leur fréquence est la suivante : *s, l, m, r, t, n, p, e, c, f*.

Nanti de ces enseignements, nous allons tenter de déterminer les lettres voisines de celles que nous avons identifiées. Nous avons vu que *J* pourrait être *n* ou *t*. Nous allons trancher très vite : le premier mot du texte se termine par *J* et le deuxième commence et finit par *J*. En français, le *n* ne se prête pas couramment à ces positions, alors que le *t* convient. Nous pouvons donc maintenant tenir que :

A = e
H = s
J = t
O = l

Nous allons remplacer dans le texte chiffré ces quatre lettres par leur lettre d'origine. Grâce à l'usage des capitales pour le texte chiffré et des minuscules pour le texte clair, nous pourrions utiliser très aisément ce document pour progresser.

BeELXEt tCKt Ze teNBs sSXGXWXL XMXPt LCEEe XK GCP
tGCPs DPls. FKXEL elle eKt teGNPEe l'SPstCPGe Le NX'GKD le
sXMetPeG elle se leMX, YXP sX le sCl LeMXEt le sCKMeGXPE et
IKP LPt.

Sur ces quelques lignes, faisons déjà quelques réflexions. Le *C* a des chances d'être une voyelle : nous le trouvons après *t* dans *tCKt* et surtout entre *s* et *l* dans *sCl*. Sachant qu'il ne peut être un *e*, puisque c'est *A*, on peut opter pour *o*, ce qui donne *sol*, et *toKt*. Ce *K*, nous le retrouvons dans *eKt* précédé de *elle* : *elle eKt*. Là encore ce ne peut être un *s* (qui est *H*), un *u* conviendrait : *elle eut*. Dans *toKt*, nous obtiendrions tout. Ceci est vraisemblable. Donc *K = u* et *C = o*. Nous avons maintenant 6 lettres pour continuer le texte.

: « IGXEL GoP, LeBuPs NPlle et uEe EuPts Re t'XP GXZoEte les
GeZPts Le l'XEZPeE teNBs et les leleELes Les GoPs BXsses. BuPs-Re
Ne BeGNettGe Le sollPZPteG uEe DXMeuG Le MotGe NXReste ? »

Ici encore, prenons les mots courts. *Re* précède *t'XP*, et suit *EuPts* ; *t'XP* devrait être un verbe précédé du *t'*, selon toute probabilité, le *R = j*. Alors nous lirions : *je t'XP*. *Je t'ai*, peut-être, puisque le *a* et le *i* ne sont pas encore révélés. Si le *P = i*, alors *NPlle* devient *Nille*, et *EuPts*

devient : Euits. Nous lisons : Nille et uEe Euits et nous sommes tentés de dire : Mille et une nuits. Soit : $N = m$ et $E = n$.

Transcrivons la suite :

eBiloIue — Zontes des mille et une nuits.

$Z = c$, évidemment, et eBiloIue doit être épilogue, soit : $B = p$ et $I = g$.

Nous pourrions maintenant reprendre tout le texte en remplaçant les lettres par celles que nous avons trouvées, et deviner ensuite les autres grâce au contexte. Mais revenons donc à l'alphabet. Nous avons reconstitué une bonne partie de l'alphabet chiffré. Voyons ci-dessous où nous en sommes :

clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
chiffré	X	-	Z	-	A	-	I	S	P	R	-	O	N	E	C	B	-	-	H	J	K	-	-	-	-	-

Des lettres comme X pour a et Z pour c tendent à faire croire que Y serait mis pour b. À l'autre bout, HJK ressemblent à une suite dont le I est sorti. Nous l'avons d'ailleurs vu sous g. L'alphabet chiffré ici utilisé offre donc à la fois un glissement de trois lettres (XYZ sont au début), comme dans le chiffre de César, et un mot-clef ; puisque certaines lettres ne sont pas à leur place, elles font partie de ce mot-clef. Le mot-clef commence sous le d et se termine probablement avec le C puisque, à partir de là, on peut rétablir un ordre. B (le c est déjà placé) D (e déjà placé) F ou G (l'un doit figurer dans le mot-clef) HJK.

clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
chiffré	X	Y	Z	L	A	D	I	S	P	R	-	O	N	E	C	B	-	G	H	J	K	M	-	-	-	W

Revenons au texte pour y trouver d'autres éléments. Reprenons le début avec les lettres dont nous disposons :

penLant tout ce temps, sSaGaWaL aMait Lonne au Goi tGois Dils.

Le sens de la phrase nous indique que nous pouvons sans risque remplacer L par d, M par v et G par r. D serait alors f. Puisque nous sommes face à un texte tiré des *Mille et Une Nuits*, sSara Wad est

forcément Sharazad. Donc S = h et W = z. Le déchiffrement avance très vite maintenant et ces lettres vont nous aider à remplir l'alphabet chiffré. L'enchaînement fin-début W-XYZ nous confirme le décalage. Le mot-clef, hors lettres répétées, est : LADISPR-ONEC. La disparition (T = k) semble évident. Restent EC, qui font penser à Perec. Le mot-clef est donc : *la disparition Perec*, dont nous avons parlé plus haut (le p et le r de Perec sont déjà dans *la disparition*). L'alphabet chiffré est maintenant complet et par suite le texte aussi.

clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
chiffré	X	Y	Z	L	A	D	I	S	P	R	T	O	N	E	C	B	F	G	H	J	K	M	Q	U	V	W

Pendant tout ce temps Sharazad avait donné au roi trois fils. Quand elle eut terminé l'histoire de Ma'ruf le savetier, elle se leva, baisa le sol devant le souverain et lui dit : « Grand Roi, depuis mille et une nuits je t'ai raconté les récits de l'ancien temps et les légendes des rois passés. Puis-je me permettre de solliciter une faveur de Votre Majesté ? »

Épilogue - Contes des Mille et une nuits

La Renaissance en Occident

Entre 800 et 1200, alors que les Arabes connaissaient une période de brillante réussite intellectuelle, l'Europe restait plongée dans les ténèbres. Quand Al-Kindi jetait les bases de la cryptanalyse, les Européens se battaient encore avec les rudiments de la cryptographie. Les seules institutions en Europe qui encourageaient l'étude des écritures secrètes étaient les monastères, où des moines étudiaient la Bible pour y découvrir des significations cachées, fascinante idée qui a perduré jusqu'à nous, (voir Annexe C).

Les moines médiévaux étaient intrigués par le fait que l'Ancien Testament contenait des exemples manifestes de cryptographie. Il comporte par exemple des textes cryptés selon l'*atbash*, forme traditionnelle d'un chiffre de substitution hébreu. L'*atbash* consiste à remplacer chaque lettre, en ayant compté quelle place elle occupe dans l'alphabet, par la lettre occupant la même place en partant de la fin de l'alphabet. En français cela signifie que *a* est remplacé par *Z*, *b* par *Y* et ainsi de suite. Le terme *atbash* découle lui-même de la substitution qu'il qualifie, puisqu'il est formé d'après la première lettre de l'alphabet hébreu *aleph*, suivie de la dernière *taw*, puis de la seconde, *bet*, et de l'avant-dernière *shin*. Un exemple d'*atbash* figure dans Jérémie 25, 26 où le nom de Sheshak est substitué à Babel ; la première lettre de Babel est *bet*, deuxième lettre de l'alphabet hébreu, et elle est remplacée par *shin*, l'avant-dernière, la deuxième lettre de Babel est aussi *bet* et donc, également remplacée par *shin*, et la dernière est *lamed*, la douzième de l'alphabet hébreu, qui est remplacée par *kaf*, la douzième en partant de la fin.

L'*atbash* et d'autres chiffres bibliques du même ordre n'étaient sans doute employés que pour apporter du mystère au texte, non pour en occulter le sens, mais ce fut suffisant pour éveiller un intérêt pour la cryptographie. Les moines européens commencèrent par redécouvrir les anciens chiffres de substitution, puis ils en inventèrent d'autres et réintroduisirent bientôt la cryptographie dans la civilisation occidentale. Le premier livre européen à décrire les méthodes de la cryptographie fut écrit au XIII^e siècle par le moine franciscain anglais, Roger Bacon. Sa *Lettre sur les œuvres d'art et sur la nullité de la magie* proposait sept

méthodes pour tenir les messages secrets et mettait en garde : « Un homme est fou s'il écrit un secret autrement que sous une forme le dérobant à la compréhension du commun des mortels. »

Au XIV^e siècle, l'usage de la cryptographie se répandit largement, les alchimistes et les scientifiques en usant pour protéger leurs découvertes. Bien que plus connu pour ses œuvres littéraires, Geoffrey Chaucer était aussi astronome et cryptographe, et il est l'auteur d'un des plus célèbres cryptages européens. Dans son *Traité de l'Astrolabe*, il propose quelques notes additionnelles intitulées *The Equatore of the Planetis*, qui contiennent plusieurs passages cryptés. Le principe de Chaucer remplaçait des lettres du texte d'origine par des symboles, par exemple *b* par δ . Un texte chiffré composé de symboles étranges, plutôt que de lettres, peut sembler plus compliqué à première vue, mais il n'en est rien. Le procédé de cryptage et le degré de sécurité sont exactement les mêmes.

Au XV^e siècle, la cryptographie était florissante en Europe. La renaissance des arts, des sciences, la quête de l'érudition alimentèrent les capacités de la cryptographie, en même temps que la multiplication des complots politiques créait la nécessité du secret des communications. L'Italie, en particulier — constituée d'États indépendants dont chacun essayait de déjouer les manœuvres des autres —, offrait un cadre idéal à la cryptographie. La diplomatie y déployait une intense activité, chaque cour ayant des ambassadeurs dans toutes les autres cours. Tous ces ambassadeurs recevaient de leurs monarques respectifs des instructions fixant la politique à mener et, en réponse, ils renvoyaient toutes les informations qu'ils pouvaient glaner. Il y avait bien là de quoi encourager la cryptographie, aussi chaque État créa-t-il bientôt son bureau du chiffre, et chaque ambassadeur fut-il flanqué d'un secrétaire du chiffre.

Simultanément, la cryptanalyse commençait à émerger en Occident. Les diplomates s'étaient à peine familiarisés avec les techniques protégeant le secret de leurs communications que déjà d'autres personnes s'employaient à les faire céder. Il est fort probable que la cryptanalyse ait été mise au point par des Européens sans références extérieures, mais on ne peut négliger la possibilité qu'elle soit venue des pays arabes. Les découvertes de l'Islam influèrent sur le renouveau scientifique en Europe, et la cryptanalyse peut avoir figuré parmi les techniques importées.

Le premier grand cryptanalyse européen fut sans doute le Vénitien Giovanni Soro, secrétaire du chiffre en 1506. Sa réputation s'était répandue à travers l'Italie et les États amis envoyaient à Venise des messages à cryptanalyser. Même le Vatican, pourtant actif centre de renseignements, envoya à Soro des messages impénétrables tombés entre ses mains. En 1526, le pape Clément VII lui confia deux textes cryptés, et tous deux furent retournés au Vatican après un déchiffrement réussi. Aussi lorsque l'un de ses propres messages cryptés fut intercepté par les Florentins, le pape en envoya une copie à Soro pour que celui-ci le rassure sur son intangibilité. Soro affirma qu'il n'avait pas pu briser le chiffre du pape, ce qui signifiait que les Florentins en seraient tout aussi incapables. Peut-être s'agissait-il d'une astuce pour endormir les cryptographes du Vatican : Soro ne tenait peut-être pas à mettre en évidence les faiblesses du chiffre du pape, ce qui aurait amené le Vatican à élaborer un chiffre mieux défendu, que Soro aurait eu plus de difficulté à pénétrer.

Dans toute l'Europe, d'autres cours royales commençaient à employer d'habiles cryptanalystes, comme, en France, Philibert Babou, au service de François I^{er}. Babou s'était taillé une réputation d'opiniâtreté en travaillant jour et nuit, des semaines durant, pour venir à bout d'un déchiffrement. (Malheureusement pour lui, cet emploi du temps permit au roi d'entretenir une liaison durable avec son épouse !) Vers la fin du XVI^e siècle, brilla François Viète, éprouvait un plaisir particulier à briser les chiffres espagnols. Les cryptographes espagnols, plus naïfs, semble-t-il, que leurs pairs étrangers, eurent peine à croire que leurs messages secrets étaient transparents pour les Français. Le roi Philippe II alla se plaindre jusqu'au Vatican, prétendant que la seule explication possible aux prouesses de Viète était qu'il fut d'intelligence avec le diable, et réclamait sa mise en jugement devant un tribunal ecclésiastique pour ses activités démoniaques. Mais le pape savait que ses propres cryptanalystes lisaient les messages espagnols depuis des années, et il rejeta la royale pétition. Cette histoire fit bientôt le tour des experts en chiffre, et les cryptographes espagnols furent la risée de l'Europe.

À la même époque des pays qui avaient pris conscience de la faiblesse du principe de substitution alphabétique s'efforçaient de mettre au point un chiffrement plus efficace. L'une des améliorations les plus simples consista dans l'introduction de signes *nuls*, lettres ou symboles qui ne se substituaient pas aux lettres, mais n'étaient que de simples blancs sans

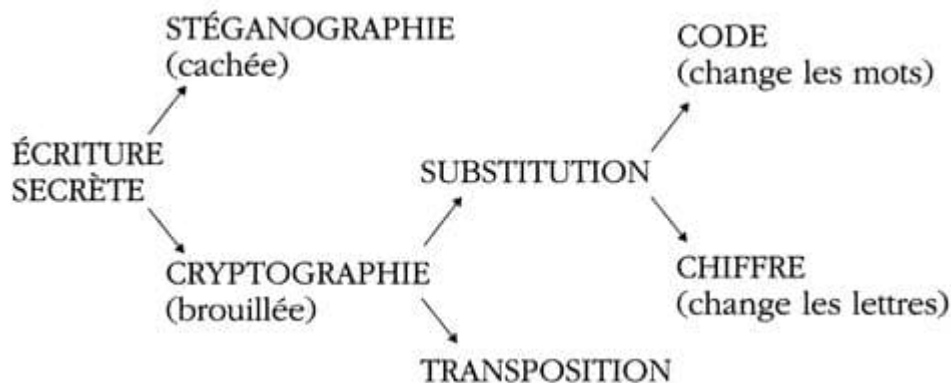
signification. Par exemple, on pourrait remplacer chaque lettre de l'alphabet par un nombre choisi entre 1 et 99, ce qui laisserait 73 nombres qui ne représenteraient rien et qui seraient répartis au hasard dans le texte chiffré, irrégulièrement. Les nuls ne poseront aucun problème au destinataire qui saura qu'il ne doit pas en tenir compte, mais ils déconcerteront l'intercepteur en apportant une confusion préjudiciable à l'analyse des fréquences. Une variante consistait à mal orthographier le message clair avant de le chiffrer. *Sessi ha kom eifai dêfassé lè fhrekans*. Le destinataire qui connaît la clef du chiffre saura retrouver cette phrase sous le cryptage et réussira à en saisir le sens malgré son orthographe fantaisiste, mais la tâche du cryptanalyste ennemi sera rendue plus difficile.

Une autre voie pour étayer le chiffre de substitution consista à introduire des mots de code. Le *code* a un sens très large dans le langage usuel, et est souvent employé pour désigner n'importe quelle méthode apportant le secret aux communications. Ce mot a pourtant un sens précis et ne s'applique réellement qu'à une certaine forme de substitution. Jusqu'ici, nous sommes restés sur l'idée du remplacement d'une lettre par une autre lettre, un nombre ou un symbole. Mais on peut passer à un autre niveau, et remplacer chaque mot par un autre mot ou symbole. Ceci s'appelle un code. Par exemple :

assassinez = D,
chantage = P,
capture = J,
protéger = Z,
général = ϵ ,
roi = Ω ,
ministre = Ψ ,
prince = 9,
immédiatement = 08,
aujourd'hui = 73,
cette nuit = 28,
demain = 43.

Message clair = assassinez le roi cette nuit
Message codé = D — Ω — 28

Techniquement, un *code* utilise la substitution au niveau des mots ou des phrases, alors qu'un *chiffre* le fait au niveau des lettres. Si l'on se sert d'un chiffre, on *chiffre* et on *déchiffre*. Dans le cas d'un code, on *code* et on *décode*. Les termes *crypter* et *décrypter* sont plus généraux et s'appliquent également aux textes brouillés à l'aide de codes ou de chiffres. La [figure 7](#) offre un court résumé de ces définitions. Je respecterai le plus souvent cet usage, mais il peut m'arriver de parler de briseurs de code pour des briseurs de chiffres — la dernière formule serait plus exacte, mais la première est d'un usage courant.



[Fig. 7](#) Les différentes formes d'écriture secrète.

À première vue, les codes semblent offrir plus de sécurité que les chiffres, car les mots sont infiniment moins vulnérables aux analyses de fréquence que les lettres. Pour déchiffrer un chiffre alphabétique vous n'avez à identifier que 26 lettres alors que pour venir à bout d'un code vous devez identifier le sens de centaines, parfois de milliers de mots de code. Pourtant si nous examinons les codes de plus près nous voyons qu'ils ont deux points faibles comparés aux chiffres. D'abord, une fois que l'expéditeur et le destinataire ont d'un commun accord chiffré les 26 lettres de l'alphabet (la clef), ils peuvent appliquer cette clef à n'importe quel message, mais pour avoir la même faculté avec un code, ils auront dû préalablement définir un mot de code pour chacun des milliers de mots qui pourraient figurer dans le texte clair. Le répertoire des mots de code ressemblera à un dictionnaire. En d'autres termes, composer ce recueil est un travail considérable, et se promener avec n'est guère commode.

Ensuite, la saisie de ce répertoire par l'ennemi est dramatique. Toutes les communications lui deviennent intelligibles, il faudra donc élaborer au plus vite un autre code, puis le diffuser à tout le réseau concerné en assurant sa sécurité, parfois le faire parvenir aux ambassadeurs en poste

dans tous les États étrangers, etc. Il est certainement plus facile de bouleverser un alphabet chiffré et de le faire apprendre par cœur pour le distribuer et l'utiliser.

Dès le XVI^e siècle, les cryptanalystes virent les points faibles des codes et firent plutôt confiance aux chiffres ou, quelquefois, à des *nomenclatures*. Une nomenclature réunit un alphabet chiffré, et un certain nombre de mots de code. En dépit de l'addition de ces mots de code, une nomenclature n'est pas beaucoup plus efficace qu'un chiffre simple, car l'essentiel du message peut être déchiffré grâce à l'analyse des fréquences, et les mots codés sont aisément devinés grâce au contexte. Non seulement les meilleurs cryptanalystes résolvaient les problèmes posés par une nomenclature, mais ils étaient aussi capables de venir à bout de textes mal orthographiés, ou comportant des signes nuls. Au total, ils réussissaient à déchiffrer la totalité des messages. Par leur habileté ils révélaient un flot constant de secrets qui affectaient l'histoire de l'Europe. Nulle part peut-être l'impact de la cryptanalyse ne fut plus dramatiquement illustré que dans le cas de Marie Stuart, reine d'Écosse.

Le complot Babington

Le 24 novembre 1542, les armées d'Henry VIII défaisaient l'armée écossaise à la bataille de Solway Moss. Henry VIII était en position de se rendre maître de l'Écosse, et de dérober à Jacques V sa couronne. Après la bataille, le roi d'Écosse s'effondra, physiquement et mentalement, et il se retira dans le palais de Falkland. Même la naissance de sa fille Marie, deux semaines plus tard, ne ranima pas le roi : il ne survécut qu'une semaine et mourut, à l'âge de trente ans, apaisé peut-être par la certitude d'avoir un héritier. Le bébé devenait reine d'Écosse.

Marie était née prématurément et l'on craignit d'abord qu'elle ne vive pas. Des rumeurs couraient en Angleterre sur la mort de l'enfant, mais ce n'était là que l'expression des désirs de la cour anglaise, qui aurait aimé voir l'Écosse déstabilisée. En fait, Marie était forte et en bonne santé, et, à l'âge de neuf mois, le 9 septembre 1543, elle fut couronnée dans la chapelle du château de Stirling, entourée de trois comtes qui portaient pour elle la couronne royale, le sceptre et l'épée.

Paradoxalement, le jeune âge de Marie donna un répit à l'Écosse, car il aurait été peu chevaleresque pour Henry VIII de profiter de la mort récente de son roi pour envahir un pays où régnait maintenant une enfant. Le roi d'Angleterre décida plutôt de courtiser Marie, dans l'espoir de la marier à son fils Édouard, mariage qui aurait réuni les deux royaumes sous un souverain Tudor. Il initia cette manœuvre par la libération des nobles écossais capturés à Solway Moss, à condition qu'ils plaident en Écosse en faveur de cette union.

Toutefois, après avoir sérieusement envisagé l'offre d'Henry, la cour d'Écosse rejeta sa demande et lui préféra un mariage avec François, dauphin de France. L'Écosse choisissait l'alliance avec une nation catholique, décision qui convenait à la mère de Marie, Marie de Guise, dont le propre mariage avait été conclu pour sceller le lien entre l'Écosse et la France. Marie et François étaient encore des enfants, mais, plus tard, François monterait sur le trône de France avec Marie. D'ici là, la France protégerait l'Écosse contre toute agression anglaise.

Cette protection était rassurante au moment où Henry VIII, renonçant à la diplomatie, passait à l'intimidation pour persuader les Écossais que son fils serait un meilleur parti pour leur reine. Ses troupes pillaient,

saccageaient les récoltes, incendiaient les villages, attaquaient bourgs et villes tout au long de la frontière. On nomma *Rough Wooing* cette rude manière de prétendre à la main de la jeune reine, qui se poursuivit après la mort d'Henry VIII, en 1547. Sous Édouard VI, le prétendant éconduit, les attaques culminèrent avec la bataille de Pinkie Clough, où l'armée écossaise fut mise en déroute. Il fut alors décidé, pour sa sécurité, d'envoyer sans attendre Marie en France, où l'on préparerait son mariage avec François. Le 7 août 1548, âgée de six ans, elle s'embarquait en direction du port de Roscoff.

Les quelques années que Marie passa à la cour de France furent les plus heureuses de sa vie. Elle était protégée, environnée de luxe, et de plus en plus amoureuse du dauphin. On les maria lorsqu'elle eut seize ans, et, l'année suivante, François II et Marie étaient roi et reine de France. Tout semblait réuni pour un retour triomphal en Écosse, mais bientôt son mari, de santé fragile, tomba gravement malade. Une infection à l'oreille, chronique depuis son enfance, s'était aggravée. L'infection envahit le cerveau où un abcès se développa. En 1560, un an après leur couronnement, François II était mort et Marie, veuve.

À compter de cette date, la vie de Marie ne fut plus que tragédie. Elle regagna l'Écosse en 1561, et découvrit son pays transformé. Pendant sa longue absence, Marie avait grandi dans la foi catholique, alors que ses sujets écossais se tournaient de plus en plus vers l'Église protestante. Marie se plia aux vœux de la majorité, et les premières années de son règne furent assez heureuses, mais en 1565 elle épousa lord Henry Stewart, comte de Darnley : ce fut le premier pas vers sa chute. Darnley était un homme bas et brutal, et devant sa cruauté et son avidité les nobles écossais retirèrent à Marie leur soutien. Marie fut elle-même le témoin horrifié de la barbarie de son époux lorsqu'il tua sous ses yeux son secrétaire, David Riccio. Il devenait évident pour tout le monde qu'il fallait se débarrasser de Darnley. Il n'est pas établi si l'attentat fut fomenté par Marie ou par la noblesse écossaise mais, dans la nuit du 9 février 1567, une explosion détruisit la maison de Darnley. Alors qu'il tentait de fuir, Darnley fut étranglé. Ce mariage n'avait apporté qu'un seul bonheur à Marie : la naissance de son fils et héritier, Jacques.

Le troisième mariage de Marie avec James Hepburn, quatrième comte de Bothwell, ne fut guère plus réussi. La noblesse protestante d'Écosse, qui ne croyait plus en sa reine catholique, l'emprisonna et la contraignit à abdiquer en faveur de son fils Jacques VI, âgé de quatorze mois. La régence était confiée à son demi-frère, le comte de Moray. Un an plus

tard, en 1568, Marie s'évadait, rassemblait une armée de six mille hommes et tentait de remonter sur le trône. Ses soldats affrontèrent l'armée du régent près du petit village de Langside, et Marie put suivre la bataille du haut d'une colline. Bien que plus nombreuses, ses troupes manquaient de discipline, et Marie comprit qu'elles allaient être taillées en pièces. Elle s'enfuit. Le plus simple pour elle aurait été de se diriger vers l'est pour gagner la côte et d'embarquer pour la France, mais pour cela elle aurait dû franchir des terres loyales à son demi-frère. Aussi choisit-elle de se diriger vers le sud, vers l'Angleterre, dans l'espoir que sa cousine, la reine Elizabeth, lui donnerait asile.

C'était une terrible erreur. Tout ce qu'Elizabeth lui offrit, ce fut une autre prison. Le motif officiel de cette arrestation était le meurtre de Darnley, mais la vraie raison était que Marie posait un problème à sa cousine, car les catholiques anglais la tenaient pour la vraie reine d'Angleterre. Par sa grand-mère Elizabeth Tudor, sœur aînée d'Henry VIII, Marie avait en effet des droits au trône, même si ceux d'Elizabeth I^{re}, seule descendante directe d'Henry, semblaient mieux fondés. Pour les catholiques anglais, cependant, Elizabeth n'était pas légitime, car elle était la fille d'Anne Boleyn, la deuxième femme d'Henry, épousée après son divorce de Catherine d'Aragon, divorce que le pape n'avait pas admis. Si le divorce d'Henry n'était pas valable pour les catholiques anglais, ils ne pouvaient tenir pour valide son mariage ultérieur avec Anne Boleyn, ni accepter Elizabeth pour reine. Pour eux, elle n'était qu'une bâtarde et une usurpatrice.

Marie fut emprisonnée successivement dans divers châteaux et manoirs. Si Elizabeth la considérait comme un danger, nombre d'Anglais admiraient l'élégance de ses manières, son intelligence et sa bonté. William Cecil, ministre d'Elizabeth, évoquait la manière adroite et sucrée dont elle séduisait les hommes, et Nicolas White, l'émissaire de Cecil, faisait une remarque similaire : « Elle allie à une distinction séduisante un esprit brillant, voilé de douceur. » Mais, les années passant, Marie perdit de son éclat, sa santé se détériora et elle commença à perdre espoir. Son geôlier, sir Amyas Paulet, un puritain, était insensible à ses charmes et la traitait de plus en plus durement.

En 1586, après dix-huit années d'emprisonnement, elle ne jouissait plus d'aucun privilège. Elle était enfermée à Chartley Hall, dans le Staffordshire, et n'était plus autorisée à se rendre à Buxton pour prendre les eaux, ce qui avait été jusque-là un secours pour sa santé chancelante. Lors de son dernier séjour à Buxton, elle avait gravé avec un diamant sur

la vitre d'une fenêtre : « Buxton, toi dont les eaux chaudes ont rendu le nom illustre, sans doute ne te reviendrai-je plus. Adieu. » Elle se doutait évidemment qu'on allait lui supprimer cette dernière liberté. Le chagrin de Marie était aggravé par le comportement de son fils, le roi Jacques VI d'Écosse, alors âgé de dix-neuf ans. Elle avait longtemps espéré s'évader et regagner l'Écosse pour y partager le pouvoir avec son fils, qu'elle n'avait pas revu depuis qu'il avait un an. Mais Jacques n'éprouvait guère d'affection pour sa mère. Il avait été élevé par les ennemis de Marie, et ceux-ci lui avaient appris que sa mère avait tué son père pour épouser son amant. Jacques la méprisait et craignait, si elle revenait, qu'elle ne lui reprenne la couronne. Sa haine pour Marie s'afficha lorsqu'il rechercha un mariage avec Elizabeth I^{re}, la responsable de l'incarcération de sa mère (et de trente ans son aînée !). Elizabeth déclina l'offre.

Marie écrivait à son fils, pour tenter de le gagner à sa cause, mais ses lettres n'atteignaient jamais la frontière écossaise. À cette époque, toutes les lettres de Marie étaient saisies, et la correspondance venue de l'extérieur était retenue par son geôlier. Le moral de Marie était au plus bas, tout espoir semblait perdu. C'est dans ces circonstances désespérées que, le 6 janvier 1586, lui parvint un surprenant paquet de lettres.

Ces lettres émanaient de ses partisans sur le continent, et avaient été introduites clandestinement dans sa prison par Gilbert Gifford, un catholique qui avait quitté l'Angleterre en 1577 et avait été formé à la prêtrise par le Collège anglais de Rome. Revenu en Angleterre en 1585, il semblait désireux de servir Marie et avait approché l'ambassade de France à Londres, où une pile de courrier pour elle était en attente. L'ambassade savait que, si elle acheminait les lettres par la voie officielle, Marie ne les verrait jamais, aussi l'offre de Gifford de faire passer en fraude ce courrier à Chartley Hall avait-elle été acceptée. Cette livraison fut la première d'une série, et Gifford entama une carrière de courrier, transmettant aussi les réponses de Marie. Il avait trouvé un moyen habile pour faire entrer les lettres à Chartley Hall. Il portait les messages au brasseur local qui les emballait dans une poche de cuir cachée ensuite dans une bonde creuse qui fermait une barrique de bière. Le brasseur livrait la barrique au château, où l'un des serviteurs de Marie récupérait la bonde et portait à la reine d'Écosse son contenu. Le procédé marchait aussi bien dans l'autre sens.

À la même époque, et à l'insu de Marie, un plan pour son évasion était fomenté dans les tavernes de Londres. L'âme du complot était un certain Anthony Babington, âgé seulement de vingt-quatre ans, bel homme et

bon vivant. Babington nourrissait un ressentiment profond contre une société qui avait mal traité sa famille, sa religion et lui-même. La répression policière exercée contre les catholiques atteignait des sommets de violence, les prêtres étaient accusés de trahison et toute personne surprise à leur donner asile pouvait être rouée, mutilée et écartelée. La messe était interdite et les familles restées fidèles au pape devaient payer des taxes qui les ruinaient. La haine de Babington était nourrie par l'exécution de son arrière-grand-père, lord Darcy, décapité pour sa participation au *Pilgrimage of Grace*, un soulèvement catholique contre Henry VIII.

La conspiration fut initiée un soir de mars 1586. Babington et six de ses proches étaient réunis dans une auberge appelée The Plough (La Charrue), à l'extérieur de la Barrière du Temple. Selon l'historien Philippe Caraman, « il attirait vers lui par son charme exceptionnel et sa personnalité des jeunes gens catholiques de son rang, galants, aventureux et désireux de défendre leur religion en ces temps d'oppression ; prêts donc pour n'importe quelle périlleuse entreprise qui puisse servir cette cause ». En quelques mois, un plan fut établi pour libérer Marie, assassiner Elizabeth, et fomenter ensuite une rébellion que viendrait soutenir une invasion de l'étranger. Les conspirateurs étaient d'avis que le complot ne pouvait être mené sans la bénédiction de Marie, mais il n'y avait apparemment pas moyen de communiquer avec elle. Sur ces entrefaites, le 6 juillet 1586, Gifford se présenta à la porte de Babington. Il apportait une lettre de Marie, expliquant qu'elle avait entendu parler de Babington par ses partisans de Paris et qu'elle attendait qu'il se manifeste. En réponse, Babington rédigea une lettre détaillée où il traçait les grandes lignes de son projet et faisait référence à l'excommunication d'Elizabeth par le pape Pie V en 1570 qui, pensait-il, légitimait son assassinat.

*Moi-même assisté de dix gentilshommes et d'une
centaine de nos compagnons entreprendrons de délivrer
votre Personne royale des mains de ses ennemis.*

*Pour l'élimination de l'usurpatrice, envers qui nous
nous considérons relevés du devoir d'obéissance par son
excommunication, il y a six nobles jeunes gens, tous mes
amis intimes, qui, avec le zèle qu'ils portent à la cause
catholique, et pour le service de Votre Majesté, se
chargeront de la terrible exécution.*

Comme à l'accoutumée, Gifford passerait ce message dans la bonde d'une barrique, à l'insu des gardiens de Marie. Ceci peut être considéré comme une forme de stéganographie, puisque la lettre était cachée. Par une précaution complémentaire, Babington chiffra sa lettre afin que, si jamais le geôlier de Marie l'interceptait, il ne puisse la déchiffrer, le complot restant protégé par le secret. Il utilisa un chiffre qui n'était pas simplement une substitution alphabétique mais plutôt une nomenclature, telle qu'on la voit sur la [figure 8](#). Elle était constituée de 23 symboles qui remplaçaient les lettres de l'alphabet (sauf j, v, et w), ainsi que de 36 symboles représentant des mots ou des phrases. Il y avait en outre quatre nuls et un symbole qui signifiait que la lettre suivante était une lettre doublée.

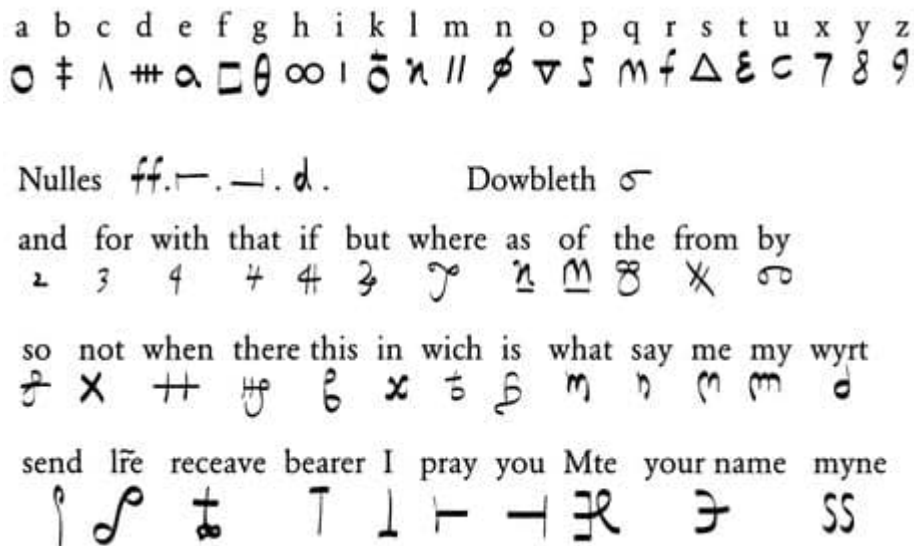


Fig. 8 La nomenclature de Marie Stuart, composée d'un alphabet chiffré et de mots de code.

Gifford mena à bien ses expéditions avec assurance et astuce. Ses pseudonymes, comme M. Colerdin, Pietro ou Cornelys, l'aidaient à traverser le pays sans attirer de soupçons et ses contacts dans la communauté catholique lui procuraient des asiles sûrs entre Londres et Chartley Hall. Pourtant, à chaque fois que Gifford se rendait à Chartley Hall ou en revenait, il faisait un détour. Car Gifford était un traître, un agent double. Dès 1585, avant même son retour en Angleterre, il avait écrit à sir Francis Walsingham, Premier secrétaire de la reine Elizabeth pour lui offrir ses services. Gifford savait que son passé catholique lui offrait un masque parfait pour pénétrer les complots contre la reine Elizabeth. Dans sa lettre à Walsingham, il écrivait : « J'ai entendu parler du travail que vous faites et je souhaite vous servir. Je n'ai ni

scrupules, ni peur du danger. Quoi que vous m'ordonniez, je l'accomplirai. »

Walsingham était le plus impitoyable des ministres d'Elizabeth. C'était un personnage machiavélique, qui dirigeait l'espionnage et était responsable de la sécurité de la reine. Il avait trouvé à son arrivée un petit réseau d'espions qu'il avait rapidement développé sur le continent, où de nombreux complots se tramaient. Après sa mort, on découvrit qu'il recevait des rapports réguliers provenant de douze points en France, neuf en Allemagne, quatre en Italie et trois aux Pays-Bas, et qu'il entretenait des informateurs à Constantinople, Alger et Tripoli.

Walsingham recruta Gifford, et ce fut lui qui lui ordonna d'approcher l'ambassade de France pour se proposer comme courrier. Et donc, chaque fois que Gifford ramassait un message de ou pour Marie, il le portait d'abord à Walsingham. Celui-ci le passait à ses contrefacteurs qui brisaient le sceau de chaque lettre, en copiaient le contenu, puis scellaient à nouveau la lettre originale avec un cachet identique avant de la rendre à Gifford. La lettre apparemment intacte était remise à Marie ou à ses correspondants, qui ignoraient tout de cette interception.

Quand Gifford remit à Walsingham la lettre de Babington pour Marie, Le Premier secrétaire avait déjà abordé les codes et les chiffres grâce à la lecture d'un livre du cryptographe italien Jérôme Cardano qui, précurseur de Braille, proposait une forme d'écriture pour les aveugles, basée sur le toucher. Le livre de Cardan avait éveillé l'intérêt de Walsingham, mais c'est un déchiffrement par le cryptanalyste flamand Philippe Van Marnix qui lui fit comprendre le pouvoir que lui donnerait la présence à ses côtés d'un briseur de codes. En 1577, Philippe II d'Espagne correspondait avec son demi-frère et coreligionnaire catholique, don Juan d'Autriche, qui contrôlait la plus grande partie des Pays-Bas. Une lettre de Philippe faisant état d'un plan pour envahir l'Angleterre fut interceptée par Guillaume d'Orange, qui la confia à Marnix, son secrétaire du chiffre. Marnix déchiffra le plan, et Guillaume transmit l'information à Daniel Rogers, un agent anglais en poste sur le continent, lequel prévint à son tour Walsingham. Les Anglais renforcèrent leur défense, ce qui suffit à faire annuler l'entreprise.

Convaincu dès lors de l'intérêt de la cryptanalyse, Walsingham créa à Londres une école du chiffre et s'assura les services de Thomas Phelippes, un homme « de petite taille, maigre à l'extrême, la tête couronnée de cheveux jaune foncé, la barbe jaune clair, le visage dévoré par la petite vérole, la vue courte, âgé d'environ trente ans ». Phelippes

était un linguiste qui parlait français, italien, espagnol, latin et allemand, et, surtout, il était l'un des meilleurs cryptanalystes d'Europe.

Phelippes se jetait sur tout message expédié par Marie ou à elle destiné. C'était un maître de l'analyse des fréquences, et il travaillait vite. Il établit la fréquence de chaque lettre, et s'efforça de trouver des équivalences pour celles qui apparaissaient le plus souvent. Lorsqu'il aboutissait à une impasse, il revenait en arrière et tentait d'autres substitutions. Peu à peu, il identifia les nuls, les diversions cryptographiques, et les mit de côté. Il ne restait plus à lire qu'un certain nombre de mots de code, dont le sens pouvait être deviné d'après le contexte.

Quand Phelippes déchiffra le message de Babington à Marie, proposant clairement d'assassiner Elizabeth, il dépêcha immédiatement ce texte diabolique à son maître. À ce moment, Walsingham aurait pu fondre sur Babington, mais il voulait davantage que l'exécution d'une poignée de rebelles. Il prit son temps, espérant que Marie répondrait et autoriserait le complot, ce qui permettrait de l'y impliquer. Walsingham souhaitait de longue date la mort de la reine d'Écosse, mais il savait qu'Elizabeth répugnait à faire exécuter sa cousine. S'il pouvait prouver que Marie fomentait un attentat contre la vie d'Elizabeth, alors la reine serait bien forcée de donner son accord à l'exécution de sa rivale. Les espoirs de Walsingham furent bientôt comblés.

Le 17 juillet, Marie répondit à Babington, signant ainsi son propre arrêt de mort. Elle s'exprimait ouvertement à propos du *projet*, montrant un souci particulier d'être elle-même libérée au moment de l'assassinat d'Elizabeth, ou même avant, sinon la nouvelle pouvait en parvenir à son geôlier, qui n'hésiterait peut-être pas à la tuer. Avant d'arriver à Babington, la lettre fit le détour usuel chez Phelippes. Ayant cryptanalysé le précédent message, il déchiffra aisément celui-ci, le lut et le marqua du signe de la potence : n.

Walsingham avait toutes les preuves nécessaires pour accuser Marie et Babington, mais il n'était pas encore satisfait. Pour détruire tout à fait la conspiration, il avait besoin du nom de tous ses membres. Il demanda à Phelippes de forger, d'après le texte clair ci-dessous, un post-scriptum à ajouter à la fin de la lettre de Marie. C'était un autre des talents de Phelippes, qui se disait capable « d'imiter l'écriture d'un homme, s'il l'avait vue une fois, aussi bien que si l'homme avait écrit lui-même » (voir [figure 9](#)).

« J'aimerais connaître les noms et qualités des six gentilshommes qui accompliront notre dessein ; car il se peut que je sois en mesure, connaissant les parties en cause, de vous donner des directives ultérieures qu'il vous faudra suivre ; faites-moi savoir de temps en temps où vous en êtes et, aussitôt que possible, dans le même but, qui est déjà engagé et dans quelle mesure chacun est impliqué. »

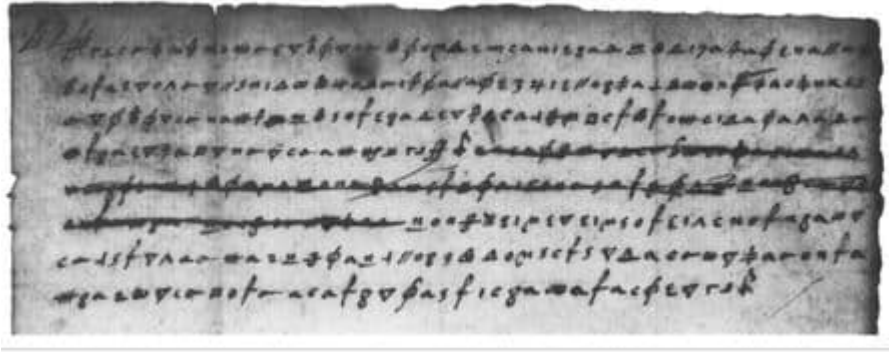


Fig. 9 Le faux post-scriptum ajouté par Thomas Phelippes au message de Marie. On peut le déchiffrer en se reportant au chiffre de Marie sur la [figure 8](#).

Le chiffre de Marie Stuart démontre clairement qu'un chiffre faible peut être plus dangereux que pas de chiffrement du tout. Aussi bien Marie que Babington écrivirent explicitement leurs intentions, alors que s'ils avaient correspondu en clair, ils auraient fait allusion à leurs plans de manière plus discrète. De plus, leur confiance dans le code les rendait vulnérables au faux forgé par Phelippes. La plupart du temps, expéditeur et destinataire ont une telle confiance dans l'inviolabilité de leur chiffre qu'ils ne peuvent imaginer que l'ennemi puisse le démarquer et insérer un texte forgé par lui. L'utilisation correcte d'un chiffre bien défendu donne donc un avantage évident à l'envoyeur et au receveur, alors que le mauvais usage d'un chiffre faible peut engendrer un très illusoire et dangereux sentiment de sécurité.

Dès qu'il eut reçu la lettre et son post-scriptum, Babington se prépara à partir pour l'étranger afin d'organiser l'invasion, et il dut se présenter dans les services de Walsingham pour l'obtention d'un passeport. Le moment aurait été idéal pour saisir le traître, mais le bureaucrate en charge, John Scudamore, ne s'attendait pas à ce que l'homme le plus recherché d'Angleterre se présente à sa porte. Scudamore ne disposait d'aucune assistance de police, aussi entraîna-t-il vers une taverne proche un Babington sans méfiance, gagnant ainsi du temps pour que son adjoint rameute quelques soldats. Un moment plus tard, on apporta à la taverne un mot pour Scudamore qui lui annonçait l'imminence de

l'interpellation. Babington remarqua cette note. Il dit tranquillement qu'il allait payer la bière et le repas, se leva en laissant près de la table son manteau et son épée, comme s'il devait revenir dans un instant. Au lieu de cela il s'échappa par la porte de derrière et gagna le bois de St. John, puis Harrow. Pour modifier son allure aristocratique, il coupa ses cheveux court, et colora sa peau avec du brou de noix. Il échappa à la capture pendant dix jours, mais, le 15 août, Auguste Babington et ses six affidés étaient pris et conduits à Londres. Les cloches de toutes les églises de la ville sonnaient ensemble en signe de triomphe. Comme le rapporte l'historien William Camden, leurs exécutions atteignirent un sommet dans l'horreur : « On coupa la corde qui les pendait, on les émascula, ils furent étripés vivants et conscients, puis écartelés. »

Le 11 août, Marie Stuart et sa suite avaient été autorisées, privilège exceptionnel, à se promener à cheval sur les terres de Chartley Hall. Alors que Marie parcourait les landes, elle aperçut quelques cavaliers qui approchaient, et pensa immédiatement qu'il devait s'agir des hommes de Babington qui venaient la délivrer. Mais il apparut vite que ces cavaliers étaient là pour l'arrêter, et non pour la libérer. Marie était impliquée dans le complot Babington et inculpée sous le chef de la *Loi d'Association*, loi votée par le Parlement en 1584 pour condamner toute personne convaincue de conspiration contre Elizabeth.

Le procès se déroula au château de Fotheringhay, un lieu triste et désolé au milieu des plaines marécageuses de l'est de l'Angleterre. Il commença le mercredi 15 octobre, en présence de deux présidents de la Cour suprême, de quatre autres juges, du ministre de la Justice, du ministre des Finances et de divers comtes, chevaliers et barons. Au fond de la salle d'audience, des places étaient offertes aux spectateurs, villageois de la région ou serviteurs des magistrats, tous désireux de voir la reine d'Écosse humiliée quémander le pardon et plaider pour sauver sa tête. Mais Marie resta digne et maîtresse d'elle-même tout au long du procès. Sa principale défense consista à nier tout rapport avec Babington. « Puis-je être tenue pour responsable des projets que quelques hommes désespérés ont élaborés sans que je le sache et que j'y participe ? » demandait-elle. Sa déposition ne tenait guère face à l'évidence.

Marie et Babington avaient fait confiance à un chiffre pour tenir leurs plans secrets, mais ils vivaient à une époque où la cryptographie perdait de son efficacité devant les avancées de la cryptanalyse. Leur chiffre aurait résisté à des décrypteurs amateurs, mais il n'avait aucune chance

face à un expert en analyse de fréquences. Dans la galerie réservée aux spectateurs, Phelippes attendait tranquillement que l'on sorte les preuves qu'il avait établies en déchiffrant les lettres.

Le deuxième jour, Marie continua à nier avoir été au courant du complot. À l'issue des débats, elle confia son sort aux juges, leur pardonnant à l'avance leur décision inévitable. Dix jours plus tard, la Chambre Étoilée se réunit à Westminster et statua. Marie était coupable « d'avoir toléré et élaboré depuis le 1^{er} juin des manœuvres ayant pour but l'élimination et la mort de la reine d'Angleterre ». La Cour recommandait la peine de mort, et Elizabeth signa l'ordre d'exécution.

Le 8 février 1587, dans la grande salle du château de Fotheringhay, une assistance de trois cents personnes se réunit pour assister à la décapitation. Walsingham ne voulait pas faire de Marie une martyre, aussi ordonna-t-il que le billot, les vêtements de Marie et tous les objets relatifs à l'exécution soient brûlés, afin d'éviter qu'ils ne se transforment en reliques. De plus, il organisa pour la semaine suivante des funérailles grandioses pour son gendre, sir Philip Sidney. Celui-ci, personnage populaire et héroïque, avait été tué en combattant les catholiques aux Pays-Bas, et Walsingham pensa qu'une impressionnante manifestation en son honneur tarirait la compassion inspirée par Marie. De son côté, Marie était tout aussi déterminée à faire de sa dernière apparition un geste de défi, l'occasion de réaffirmer sa foi catholique et d'inspirer ceux de ses partisans qui continueraient la lutte après elle.

Le doyen de Peterborough présidait à la cérémonie. Marie prononça à haute voix ses propres prières pour le salut de l'Église catholique d'Angleterre, pour son fils et pour Elizabeth. Avec en tête la devise de sa famille « En ma fin est mon commencement », elle se recueillit et s'approcha du billot. Les bourreaux lui demandèrent son pardon, et elle répondit : « Je vous pardonne du fond du cœur, car maintenant j'espère que vous allez mettre un terme à tous mes malheurs. » Richard Wingfield rapporte ses derniers moments dans le *Récit des derniers jours de la reine d'Écosse* :

Alors elle se coucha sur le billot très calmement et, étendant bras et jambes, elle prononça In manus tuas domine trois ou quatre fois, et la dernière fois, alors que l'un des bourreaux la maintenait légèrement d'une main, l'autre la frappa de la hache à deux reprises pour couper la tête, qui resta cependant liée par un peu de cartilage.

Elle n'émit à cet instant presque aucun son et ne se mut aucunement de l'endroit où elle reposait. Ses lèvres s'ouvrirent et se fermèrent pendant un quart d'heure après qu'on lui eut coupé la tête.

L'un des bourreaux tirant ensuite sur ses jarretières découvrit son petit chien qui s'était blotti sous ses vêtements. On ne put l'en sortir que par la force et sans réussir à le séparer du cadavre, contre lequel il vint se blottir, entre la tête et les épaules, incident qu'on s'empressa de relever.



Fig. 10 Exécution de Marie Stuart.

2

Le chiffre indéchiffrable

Pendant des siècles, jusqu'au développement de l'analyse des fréquences dans les pays arabes, puis en Europe, la simple substitution alphabétique avait été suffisante pour garantir le secret des communications. La tragique aventure de Marie Stuart fut une illustration dramatique de la faiblesse de cette simple substitution et, dans la bataille entre cryptographes et cryptanalystes, il est clair que les seconds avaient pris le dessus. N'importe qui envoyant un message devait accepter son éventuelle interception et sa lecture par un ennemi expert en déchiffrement.

Il était donc de la responsabilité des cryptographes de concevoir un nouveau chiffre, plus robuste, qui fût capable de déjouer la cryptanalyse. Bien que pareil chiffre ne soit apparu qu'à la fin du XVI^e siècle, on peut en faire remonter l'origine au savant florentin Léon Battista Alberti, au XV^e siècle. Né en 1404, Alberti fut l'une des figures majeures de la Renaissance : peintre, compositeur, poète et philosophe, auteur de la première approche scientifique de la perspective, d'un traité sur la mouche domestique, et d'une oraison funèbre pour son chien. C'est probablement comme architecte qu'il est le plus connu, pour avoir dessiné la première fontaine de Trevi à Rome et pour le premier traité d'architecture imprimé le *De Re Aedificatoria*, qui a agi comme un catalyseur pour le passage du style gothique au style Renaissance.

Autour de 1460, alors qu'il se promenait dans les jardins du Vatican, Alberti tomba sur son ami Leonardo Dato, le secrétaire pontifical, qui souleva dans la conversation quelques points délicats de cryptographie. Cette discussion fortuite décida Alberti à écrire un essai sur le sujet, esquissant ce qu'il pensait être une nouvelle forme de codage. Jusque-là, un chiffrement par substitution ne mettait en œuvre qu'un seul alphabet chiffré pour crypter un message. Alberti proposa d'utiliser deux ou plusieurs alphabets chiffrés en passant de l'un à l'autre au cours du

chiffrement, et par là, de semer la confusion chez des cryptanalystes potentiels.

alphabet ordinaire :	a b c d e f g h i j k l m n o p q r s t u v w x y z
alphabet chiffré 1 :	F Z B V K I X A Y M E P L S D H J O R G N Q C U T W
alphabet chiffré 2 :	G O X B F W T M Q I L A P Z J D E S V Y C R K U H N

Nous avons ici deux alphabets chiffrés, et nous pouvons crypter un message en les alternant. Pour crypter *hello*, nous changerions la première lettre *h* pour A, selon le premier alphabet chiffré, mais la seconde lettre *e*, selon le second alphabet, deviendrait F. Pour coder la troisième lettre, nous retournons au premier alphabet chiffré, et pour la quatrième au second. Cela fait que le premier *l* est codé P, tandis que le second est codé A. La lettre finale *o* devient D d'après le premier alphabet. Le message chiffré complet est donc AFPAD. L'avantage crucial du système d'Alberti est que la même lettre dans le texte original n'apparaît pas nécessairement comme la même lettre dans le texte chiffré.

Bien qu'il ait effectué, ce faisant, la percée la plus significative dans le cryptage depuis plus de mille ans, Alberti échoua à développer son concept en un système complet. Cette tâche devait revenir à plusieurs chercheurs qui travaillèrent sur ses idées après lui : Jean Trithème, un abbé allemand né en 1462, Giovanni Porta, un savant italien né en 1535, et Blaise de Vigenère, diplomate français né en 1523.

Vigenère se familiarisa avec les écrits de ces auteurs à Rome où, âgé de vingt-six ans, il passa deux années en mission diplomatique. Initialement, son intérêt pour la cryptographie était purement pratique, et lié à son activité diplomatique. Une dizaine d'années plus tard, Vigenère considéra qu'il avait mis de côté assez d'argent pour abandonner la carrière et se consacrer à l'étude. C'est seulement à ce moment qu'il examina en détail les idées d'Alberti, Trithème et Porta, tramant grâce à elles un nouveau chiffre, cohérent et puissant.



[Fig.11](#) Blaise de Vigenère.

Bien qu'Alberti, Trithème et Porta en aient fourni les bases, c'est du nom de Vigenère que ce chiffre nouveau fut baptisé, en l'honneur de l'homme qui lui donna sa forme finale. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets codés distincts pour crypter un message. La première étape consiste à construire un *carré de Vigenère*, tel que montré sur le [tableau 3](#), fait de l'alphabet clair suivi de 26 alphabets chiffrés, chacun d'eux étant décalé d'une lettre supplémentaire par rapport au précédent. Ainsi, la ligne 1 est un alphabet ayant un *décalage de César* d'une unité, la ligne 2 un décalage de deux unités, et

ainsi de suite. La ligne supérieure du carré, en minuscules, est l'alphabet clair, et vous pouvez en chiffrer chaque lettre selon l'un quelconque des 26 alphabets chiffrés. Par exemple, si le numéro 2 est choisi, la lettre *a* est chiffrée C, mais si l'on choisit le 12, alors le *a* est transcrit M.

Tableau 3 Carré de Vigenère

Clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Si l'expéditeur n'utilisait qu'un seul de ces alphabets pour chiffrer le message tout entier, ce serait l'application simple du chiffre de César, c'est-à-dire une forme très faible de cryptage, aisément déchiffrée par un intercepteur ennemi. Mais, le chiffre de Vigenère impose d'utiliser une ligne différente du carré de Vigenère pour crypter chaque lettre. Plus

précisément, l'expéditeur pourrait encrypter la première lettre selon la ligne 5, la deuxième selon la ligne 14, la troisième selon la ligne 21, et ainsi de suite.

Pour débrouiller le message, il est important que le destinataire ait connaissance de la ligne choisie pour chiffrer chaque lettre, et donc il doit y avoir un système convenu de passage de l'une à l'autre. Cet accord est obtenu grâce à un mot-clef, Pour voir comment on utilise une clef afin de crypter un bref message, chiffrons la phrase « appeler nord troupes ville », en utilisant « ROUGE » comme mot-clef.

Tout d'abord, le mot-clef est épilé bien clairement au-dessus du message, et répété en boucle de sorte que chaque lettre du message soit associée à une lettre de la clef. Le texte crypté est alors construit comme suit. Pour chiffrer la première lettre, *a*, commencez par identifier la lettre de la clef placée juste au-dessus, à savoir R, qui détermine une ligne particulière du carré de Vigenère. La ligne commençant par R est la ligne 17, et c'est elle qui va définir l'alphabet à utiliser pour substituer une lettre à la lettre originale *a*. À partir de là, on repère la colonne commençant par *a* et l'on voit qu'elle coupe la ligne 17 sur R.

Mot-clef	ROUGEROUGEROUGEROUGEROU
Clair	appeler nord troupes ville
Crypté	RDJKPVFHUVUHLUYGSMBMCZY

Pour crypter la deuxième lettre du message, on recommence. La lettre-clef placée au-dessus de *p* est le O si bien que le codage va utiliser cette fois la ligne 14 du tableau, celle qui commence par la lettre O précisément. La colonne p coupe cette ligne sur la lettre D qui est donc la lettre codée correspondant à *p* du texte en clair. Le mot-clef, par chacune de ses lettres, définit un alphabet chiffré particulier du tableau de Vigenère, et puisqu'il est formé de cinq lettres, l'expéditeur crypte son message en faisant tourner toujours les cinq mêmes lignes du tableau. Donc, pour la sixième lettre du message, on revient à la première lettre de la clef. Un mot-clef plus long ou une phrase-clef feraient intervenir un plus grand nombre de lignes dans la procédure et augmenteraient la complexité du chiffre. Le [Tableau 4](#) montre un carré de Vigenère, où les cinq alphabets cryptés définis par la clef ROUGE ont été surlignés.

Le grand avantage du chiffre de Vigenère est qu'il est inattaquable par l'analyse des fréquences décrite dans le chapitre 1. Par exemple, un cryptanalyste appliquant cette technique commencera généralement par

identifier la lettre la plus fréquente dans le texte chiffré : dans le cas présent, la lettre U qui apparaît trois fois est mise successivement pour un *o* ou un *d*, mais jamais pour un *e*. C'est un premier problème. Par ailleurs, une même lettre apparaissant à plusieurs reprises dans le texte chiffré, alors qu'elle remplace des lettres différentes du texte clair engendre une ambiguïté terrible pour le cryptanalyste. Dans l'autre sens, mais également troublantes, sont les représentations chiffrées différentes de la même lettre du texte clair. Par exemple, une lettre doublée comme *ll* dans *ville* est chiffrée CZ.

Non content d'être invulnérable à l'analyse de fréquences, le chiffre de Vigenère possède un nombre immense de clefs. L'expéditeur et le destinataire peuvent convenir d'un mot quelconque du dictionnaire, ou même forger des mots. Le cryptanalyste sera incapable de déchiffrer le message en cherchant toutes les clefs possibles, simplement parce que le nombre d'options est trop grand.

Le travail de Vigenère atteignit son apogée avec son *Traité des chiffres* publié en 1586. C'est la même année, curieusement, que Thomas Phelippes brisait le chiffre de Marie Stuart. Si le secrétaire de Marie avait pu lire ce traité et connaître le chiffre de Vigenère, les messages de Marie à Babington auraient tenu en échec Phelippes et sauvé la vie de Marie.

En raison de sa force et de sa sécurité, on aurait pu croire que tous les secrétaires du chiffre en Europe adopteraient rapidement le chiffre de Vigenère. Or, ils l'ignorèrent avec un bel ensemble. Ce système apparemment sans défaut resta négligé pendant les deux siècles suivants.

Tableau 4 Carré de Vigenère avec, surlignées, les lignes définies par le mot de code ROUGE. Pour le chiffrement, on passe d'un alphabet à l'autre parmi les cinq définis par les lettres R, O, U, G, E.

Clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

De Vigenère au Masque de fer

Les formes traditionnelles de substitution, antérieures au chiffre de Vigenère, étaient appelées chiffres de substitution monoalphabétique (ou plus simplement alphabétique), parce qu'elles n'utilisaient qu'un seul alphabet chiffré par message. À l'opposé, le chiffre de Vigenère appartient au groupe des chiffres *polyalphabétiques*, parce qu'il utilise plusieurs alphabets chiffrés par message. La nature polyalphabétique du code de Vigenère est ce qui lui donne sa force, mais aussi ce qui le rend d'un usage malaisé. L'effort requis découragea beaucoup de l'appliquer.

Pour la plupart des buts recherchés au XVII^e siècle, le chiffre monoalphabétique était parfaitement adapté. Si vous ne souhaitiez pas que votre serviteur lise votre correspondance, ou si vous vouliez protéger votre journal intime des regards inquisiteurs de votre épouse, ce chiffre classique était idéal. La substitution alphabétique était rapide, facile et sûre, face à des gens non versés dans la cryptanalyse. En fait, la simple substitution alphabétique perdura sous diverses formes pendant des siècles (voir Annexe D).

Pour des applications plus sérieuses, telles les communications gouvernementales ou militaires, le simple chiffre monoalphabétique était inadéquat. Les cryptographes professionnels en lutte avec les cryptanalystes professionnels avaient besoin d'une meilleure arme ; pourtant ils hésitaient devant le chiffre polyalphabétique en raison de sa complexité. Les communications militaires, en particulier, demandaient rapidité et simplicité, et une chancellerie diplomatique pouvait recevoir et envoyer des centaines de messages par jour, aussi le temps était-il compté. Les cryptographes cherchèrent donc un chiffre intermédiaire, qui soit plus difficile à faire céder que le chiffre monoalphabétique, mais plus simple à employer que le chiffre polyalphabétique.

Il y avait plusieurs solutions potentielles, parmi lesquelles le très efficace *chiffre de substitution homophonique*. Son principe est de remplacer chaque lettre par divers substituts, le nombre des substituts possibles étant proportionnel à la fréquence de la lettre. Par exemple, la lettre *a* en français représente environ 9 % de l'ensemble des lettres

utilisées pour écrire, aussi lui attribuerons-nous 9 symboles pour la représenter. À chaque fois *qu'un a* apparaîtra dans le texte clair, il sera remplacé par l'un des 9 symboles au hasard, en sorte qu'à la fin du chiffrement chaque symbole représente environ 1 % du texte chiffré. Comparons avec la lettre *v* qui compte pour 2 % à peu près de l'ensemble des lettres. On lui attribuera 2 symboles. Chaque fois que *v* apparaît dans le texte clair, l'un des 2 symboles sera choisi, et à la fin de la rédaction chaque symbole devra là encore représenter 1 % du texte chiffré. Ce procédé d'attribution d'un nombre variable de symboles aux lettres s'effectue tout au long de l'alphabet, jusqu'au *z*. Dans l'exemple ci-dessous, les substitués dans l'alphabet chiffré sont des nombres à 2 chiffres, et il y a de 1 à 16 substitués, en proportion de la fréquence observée en français pour chaque lettre de l'alphabet clair.

On peut considérer que chacun des nombres attribués à la lettre *a* du texte clair représente le même son dans le texte chiffré, le son de la lettre *a*. D'où l'origine du terme de substitution homophonique, *homo* signifiant semblable et *phono* signifiant son en grec. L'intérêt de proposer plusieurs options de substitution pour les lettres usuelles est de bouleverser les fréquences dans le texte chiffré. Si nous chiffons un message en utilisant l'alphabet chiffré ci-dessus, chaque nombre représentera environ 1 % du texte total. Si aucun symbole n'apparaît plus souvent que les autres comment attaquer le texte par l'analyse des fréquences ? Une sécurité parfaite, alors ? Pas tout à fait.

Tableau 5 : Exemple de chiffre de substitution homophonique

Clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Chiffré	09	81	13	01	06	31	25	39	32	15	04	26	22	18	00	38	94	29	11	17	02	34	60	28	24	01
	12		41	03	10				50			37	27	58	05	90		35	19	20	08	52				
	33		62	45	14				56			51	68	59	07	95		40	21	30	61					
	47				16				70			65		66	54			42	36	43	63					
	48				23				73			84		71	72			77	76	49	85					
	53				24				83					91				80	86	69	90					
	67				44				88					99					96	75						
	78				46				93										97							
	92				54																					
					55																					
					57																					
					74																					
					79																					
					82																					
					87																					
					98																					

En fait, le texte chiffré offre plusieurs indications au cryptanalyste attentif. Chaque lettre dans la langue française a sa propre personnalité, qui peut être définie par sa relation avec toutes les autres lettres, et cette spécificité reste discernable après le cryptage effectué selon la substitution homophonique. En français, l'exemple typique d'une lettre d'un usage particulier est la lettre *q*, toujours suivie dans le corps d'un mot par la même lettre, *u*. Si l'on déchiffre un texte, on peut établir pour commencer que la lettre *q* étant d'un usage rare elle ne sera représentée que par un seul symbole, et nous savons que le *u*, qui compte pour environ 6 % des lettres, sera probablement représenté par 6 symboles.

Donc, si nous trouvons dans le texte chiffré un symbole toujours suivi par six différents symboles, on pourra raisonnablement penser que le premier est mis pour *q* et les six autres pour *u*. D'autres lettres sont plus difficiles à repérer, mais sont aussi trahies par leurs relations entre elles. Un chiffre homophonique peut sembler peu différent d'un chiffre polyalphabétique, dans la mesure où chaque lettre du texte clair peut être chiffrée de différentes manières, mais il y a une différence majeure, et le chiffre homophonique n'est en fait qu'une variante du chiffre monoalphabétique. Dans la table des homophones montrée ci-dessus, la lettre *a* peut être représentée par 9 nombres. Plus important, ces 9 nombres ne peuvent représenter que la lettre *a*. En d'autres termes, une

lettre en clair peut être représentée par plusieurs symboles, mais chaque symbole ne représente qu'une lettre exclusivement. Dans un alphabet polyalphabétique, une lettre du texte en clair sera représentée également par différents symboles mais, et c'est ce qui prête le plus à confusion, ces symboles représenteront des lettres différentes au long du même chiffrement.

La raison fondamentale qui rapproche le chiffre homophonique du chiffre alphabétique est que, l'alphabet chiffré étant établi, il restera constant au cours de tout le processus de cryptage. Que l'alphabet chiffré offre plusieurs options pour crypter chaque lettre ne change rien. Alors qu'un cryptage utilisant un chiffre polyalphabétique doit naviguer sans cesse entre différents alphabets chiffrés au cours du cryptage.

En amendant le chiffre monoalphabétique de base de diverses manières, comme l'introduction d'homophones, il devenait pourtant possible de crypter des messages avec une grande sécurité, sans avoir recours aux complexités du chiffre polyalphabétique. L'un des exemples les plus impressionnants d'un chiffre alphabétique renforcé fut le Grand Chiffre de Louis XIV. Le Grand Chiffre était employé pour les messages les plus secrets du roi, afin de protéger les détails de ses plans, de ses intrigues et de ses machinations politiques. L'un de ces messages avait trait à un personnage qui reste une énigme dans l'histoire de France, l'homme au Masquer de fer, mais la force du Grand Chiffre était telle que le message et son contenu allaient rester indéchiffrables pendant deux siècles.

Le Grand Chiffre fut élaboré par un père et son fils, Antoine et Bonaventure Rossignol. Antoine s'était fait remarquer en 1626 lorsqu'on lui avait confié une lettre codée, saisie sur un messenger sorti de la ville assiégée de Réalmont. Le jour même, il avait déchiffré la lettre qui révélait que l'armée huguenote qui tenait la ville était sur le point de céder. Les Français, qui ignoraient jusque-là la condition désespérée des Huguenots, leur retournèrent la lettre accompagnée de sa version déchiffrée. Les Huguenots, comprenant que désormais leur ennemi ne se retirerait pas, se rendirent rapidement.

Le pouvoir des codes devenait évident et les Rossignol occupèrent des places considérables à la cour. Après avoir servi Louis XIII, ils furent les cryptanalystes de Louis XIV, qui installa leurs bureaux tout près de ses propres appartements, si bien que les Rossignol finirent par jouer un rôle

central dans l'élaboration de la diplomatie française. Mais le plus grand hommage rendu à leurs capacités est l'utilisation dans le langage courant du terme *rossignol* appliqué à un outil permettant de forcer les serrures.

Leur sens exceptionnel du déchiffrement permit aux Rossignol d'élaborer une forme de cryptage mieux défendue, et ils inventèrent le fameux Grand Chiffre. Le Grand Chiffre était si sûr qu'il tint en échec tous les cryptanalystes ennemis. Il tomba malheureusement en désuétude après la mort de ses inventeurs et ses règles précises furent rapidement perdues, ce qui rendit impossible la lecture de nombreux documents chiffrés des archives françaises. Le Grand Chiffre était si fort qu'il défia des générations de briseurs de code. On était encore incapable de le lire à la fin du XIX^e siècle.

En 1890, Victor Gendron, un historien travaillant sur les campagnes de Louis XIV, découvrit une nouvelle correspondance utilisant le Grand Chiffre. Dans l'incapacité de la comprendre, il la communiqua au commandant Etienne Bazeris, un remarquable spécialiste du service cryptographique de l'armée. Bazeris vit dans ces lettres le plus extraordinaire des défis, et il consacra les trois années suivantes à le relever.

Les pages cryptées contenaient 587 nombres différents, qui apparaissaient des milliers de fois au total. Il était clair que le Grand Chiffre était plus compliqué qu'un simple chiffre de substitution, qui n'aurait utilisé que 26 nombres, un pour chaque lettre. Bazeris tenta d'abord un déchiffrement reposant sur l'hypothèse que les nombres en surplus représentaient des homophones et que plusieurs nombres représentaient la même lettre. L'exploration de cette voie lui prit deux mois d'efforts constants, sans aucun résultat. Le Grand Chiffre n'était pas un chiffre homophonique.

Ensuite Bazeris envisagea qu'un nombre pouvait représenter une paire de lettres, un *digramme*. Si l'alphabet n'est composé que de 26 lettres, il y a 676 paires de lettres possibles, et ce nombre n'est pas éloigné de celui des nombres figurant dans les textes chiffrés. Il tenta un déchiffrement en choisissant les nombres les plus répandus dans les textes chiffrés (22, 42, 124, 125 et 341) et en supposant qu'ils étaient là à la place des digrammes français les plus courants (-es-, -en-, -ou-, -de-, -nt-). Il appliquait ainsi l'analyse de fréquences au niveau des paires de lettres. Après des mois de travail, n'étant parvenu à aucun déchiffrement porteur de sens, il renonça à cette théorie.

Bazeries hésitait à poursuivre, quand une autre idée lui vint : et si chaque nombre, plutôt qu'une paire de lettres, représentait une syllabe entière ? Bazeries essaya de rapprocher chaque nombre d'une syllabe, les nombres les plus représentés étant présumés être là pour les syllabes les plus courantes en français. Il essaya plusieurs permutations, toutes débouchaient sur du charabia, jusqu'à ce qu'il parvienne à identifier un mot particulier. Un groupe de chiffres (124-22-125-46-345) apparaissait plusieurs fois sur chaque page et Bazeries pensa qu'ils pouvaient être là pour *les-en-ne-mi-s*, les ennemis. Cette trouvaille se révéla déterminante.

Bazeries pouvait progresser en examinant d'autres parties des textes chiffrés où ces nombres apparaissaient dans plusieurs mots. Il les remplaça alors par les syllabes découlant de « les ennemis », ce qui lui donna des parties d'autres mots. Comme le sait tout amateur de mots croisés, quand des mots sont en partie remplis, il est souvent possible de deviner le reste. Au fur et à mesure que Bazeries complétait de nouveaux mots, il identifiait de nouvelles syllabes, qui à leur tour révélaient de nouveaux mots, et ainsi de suite. Il était souvent désarçonné, parfois parce que les valeurs syllabiques n'étaient pas évidentes, parfois parce que certains des nombres représentaient une lettre isolée, enfin parce que les Rossignol avaient introduit des pièges dans le chiffre. Par exemple, un nombre ne représentait ni une syllabe ni une lettre, mais signifiait qu'il fallait effacer le nombre précédent.

Quand le déchiffrement fut terminé, Bazeries devint la première personne à pouvoir pénétrer les secrets de Louis XIV. Les documents ainsi révélés fascinèrent les historiens, qui se passionnèrent en particulier pour une lettre touchant à l'une des grandes énigmes du XVII^e siècle. La lettre avait trait au Masque de fer.

L'identité du Masque de fer avait fait l'objet de maintes spéculations depuis son emprisonnement dans la forteresse de Pignerol, dans le Piémont. Lorsqu'il fut transféré à la Bastille en 1698, des paysans essayèrent de l'apercevoir, et en donnèrent des descriptions variées, certains l'avaient vu petit, d'autres grand, blond ou brun, jeune ou vieux. Il y en eut même pour prétendre qu'il s'agissait d'une femme. De Voltaire à Benjamin Franklin, chacun élaborait sa propre théorie. La plus communément répandue était la théorie de la conspiration : le Masque aurait été le frère jumeau de Louis XIV, de huit heures plus jeune, et on l'aurait emprisonné afin d'éviter toute controverse sur les droits au trône. Une des versions soutient que le Masque aurait eu des descendants, et un pamphlet publié en 1801 prétendait que Napoléon lui-même descendait

du Masque, rumeur flatteuse que l'empereur ne se crut pas obligé de démentir.

Le mythe du Masque de fer a inspiré des poèmes, des romans et des pièces de théâtre. En 1848, Victor Hugo avait commencé une pièce intitulée *Jumeaux*, mais quand il s'aperçut qu'Alexandre Dumas avait utilisé la même intrigue dans *Le Vicomte de Bragelonne*, il abandonna les deux actes déjà écrits. Depuis cette époque, on associe effectivement le nom de Dumas à l'histoire du Masque de fer. Le succès de son roman ancre l'idée que le Masque était apparenté au roi, et cette hypothèse prévaut encore aujourd'hui, en dépit des révélations dues aux déchiffrements de Bazerics.

Bazerics avait déchiffré une lettre écrite par Louvois, alors ministre de la Guerre, rapportant les fautes commises par Vivien de Bulonde, alors qu'il était chargé de mener une attaque contre la ville de Cuneo, sur la frontière franco-italienne. Bien qu'on lui ait ordonné de tenir le terrain, Bulonde prit peur devant l'arrivée des troupes ennemies venant d'Autriche ; il s'enfuit, abandonnant ses munitions et quantité de soldats blessés. D'après le ministre de la Guerre, ces actes compromirent toute la campagne du Piémont, et la lettre montrait clairement que le roi considérait le comportement de Bulonde comme un acte d'une extrême lâcheté. « Sa Majesté voit mieux que personne les conséquences de cet acte, et est consciente du préjudice qu'il a porté à notre cause en ne réussissant pas à prendre la place, un échec qu'il va falloir réparer durant l'hiver. Sa Majesté désire que vous arrêtiez immédiatement le général de Bulonde, et qu'il soit conduit à la forteresse de Pignerol, où il sera enfermé dans une cellule gardée la nuit, et où il pourra se promener sur les remparts dans la journée, en portant un masque. »

C'était là une référence explicite à un prisonnier masqué incarcéré à Pignerol, sanction justifiée par une faute extrêmement grave, et dont les dates concordaient avec l'épisode de l'homme au Masque de fer. Mais pourquoi ce masque, et le mystère était-il résolu ? Évidemment non. Les adeptes d'une version plus romanesque trouvèrent des points faibles dans l'affaire Bulonde. Par exemple, si Louis XIV avait réellement voulu tenir emprisonné secrètement son frère jumeau, il pouvait très bien avoir cherché à entraîner les curieux sur de fausses pistes. Les lettres cryptées étaient peut-être destinées à être déchiffrées. Bazerics, le briseur de code du XIX^e siècle, était peut-être tombé dans le piège posé au XVII^e.

Les cabinets noirs

Renforcer le chiffre monoalphabétique en l'appliquant aux syllabes ou en lui ajoutant des homophones avait apparemment suffi au XVII^e siècle, mais au XVIII^e la cryptanalyse devint une véritable industrie, avec des équipes de cryptanalystes travaillant de concert pour venir à bout du chiffre alphabétique le plus complexe. Chaque puissance européenne avait son *cabinet noir*, ainsi qu'on appelait les centres où l'on déchiffrait les messages et où l'on recueillait les renseignements. Le plus célèbre, le mieux organisé et le plus efficace des cabinets noirs fut le *Geheime Kabinets-Kanzlei* de Vienne.

Il opérait selon un minutage rigoureux, car il était nécessaire que ses activités ne perturbent pas le fonctionnement régulier du service postal. Le courrier destiné aux ambassades étrangères à Vienne était d'abord acheminé vers le cabinet noir, où il arrivait à sept heures du matin. Des secrétaires en faisaient fondre les sceaux, et une équipe de sténographes copiait les lettres — si nécessaire, un spécialiste de la langue utilisée se chargeait des écritures peu communes. En trois heures, les lettres avaient été scellées à nouveau dans leurs enveloppes et retournées au bureau de la poste centrale, pour être délivrées à leurs destinataires. Le courrier qui transitait seulement par Vienne arrivait au cabinet à dix heures et les lettres partant des ambassades pour des destinations extérieures à l'Autriche arrivaient à quatre heures de l'après-midi. Toutes ces lettres étaient copiées avant de poursuivre leur voyage. Une centaine de lettres passaient ainsi chaque jour par le cabinet noir viennois.

Les copies étaient communiquées aux cryptanalystes, installés dans de petites cabines où ils débrouillaient les messages. Non content de fournir aux empereurs d'Autriche des renseignements inappréciables, le cabinet noir de Vienne vendait l'information qu'il recueillait à d'autres puissances européennes. En 1774, Abbot Georgel, secrétaire de l'ambassade de France, passa un accord qui lui assurait une livraison d'informations deux fois par semaine en échange de 1 000 ducats. Il envoyait ensuite ces lettres directement à Louis XV, à Paris.

Les cabinets noirs vinrent à bout de toutes les formes de chiffres monoalphabétiques, ce qui contraignit les cryptographes à adopter le chiffre de Vigenère, plus complexe mais plus sûr. Peu à peu, les

secrétaires du chiffre passèrent au chiffre polyalphabétique. Le développement du télégraphe et la nécessité de protéger le contenu des télégrammes comptèrent également pour beaucoup dans cette évolution vers des formes de cryptage mieux défendues.

Bien que l'apparition du télégraphe et la révolution qu'il entraîna dans les communications datent du XIX^e siècle, on peut faire remonter ses origines à 1753. Cette année-là, en effet, une lettre anonyme publiée par un magazine écossais décrivait comment on pouvait envoyer un message à de grandes distances en reliant l'envoyeur et le receveur par vingt-six câbles, un pour chaque lettre de l'alphabet. L'expéditeur épèle le message en envoyant des impulsions électriques sur chaque câble. Par exemple, pour épeler *hello*, il donnera une impulsion sur le câble *h*, puis sur le câble *e* et ainsi de suite. Le destinataire ressentira le courant électrique provenant de chaque câble et lira le message. Toutefois, cette *méthode expéditive de transfert de renseignement*, comme l'appelait son inventeur, ne fut jamais construite, car il y avait plusieurs obstacles à surmonter.

Les ingénieurs avaient besoin d'un système suffisamment sensible pour la détection des signaux électriques. En Angleterre, sir Charles Wheatstone et William Fothergill Cooke construisirent des détecteurs munis d'aiguilles magnétiques qui basculeraient lorsqu'on enverrait un courant électrique. En 1839, le système Wheatstone-Cooke fut utilisé pour envoyer des messages entre les stations de chemin de fer de Drayton-ouest et de Paddington, distantes de dix-huit miles. La réputation du télégraphe se répandit vite, et rien ne fit plus pour la populariser que la naissance du second fils de la reine Victoria, le prince Alfred, le 6 août 1844. L'annonce de la naissance fut télégraphiée à Londres, et, dans l'heure, le *Times* était dans les rues avec la nouvelle. Le journal rendait hommage à l'invention qui avait permis cet exploit, et dont il était « redevable au pouvoir extraordinaire du télégraphe électromagnétique ». L'année suivante, le télégraphe accrut encore sa renommée avec l'arrestation de John Tawell, meurtrier de sa maîtresse à Slough, et qui avait tenté de s'échapper en sautant dans un train pour Londres. La police locale télégraphia le signalement de Tawell à Londres, et il fut arrêté à son arrivée à Paddington.

À la même époque, en Amérique, Samuel Morse venait de construire sa première ligne télégraphique, longue de trente-sept miles, entre Baltimore et Washington. Morse employa un électro-aimant pour

amplifier le signal, de sorte qu'en atteignant le destinataire, il soit encore assez puissant pour inscrire clairement une série de signes longs et courts, traits et points, sur une feuille de papier. Il mit au point le célèbre code Morse en traduisant chaque lettre de l'alphabet en une série de points et de traits, comme le montre le [tableau 6](#). Un vibreur, permettant au destinataire de percevoir chaque lettre sous la forme de points et de traits audibles, compléta son système.

Symbole	Code morse international
A	·—
B	...·
C	—·—·
D	—...·
E	·
F	··—·
G	—·—·
H	·····
I	··
J	·—
K	—·—
L	·—··
M	— —
N	—·
O	— — —

P	·—·
Q	—·—
R	·—·
S	...
T	—
U	··—
V	...—
W	·—
X	—·—
Y	—·—
Z	—·
1	·——
2	··——
3	...—
4	—
5	
6	—....
7	—...·
8	——··
9	——·
0	——
point	·—·—·—

,	— · —
?	· — · ·
:	— · · ·
;	— · — ·
-	— · · —
/	— · · —
.	· — · —

Tableau 6 Code Morse international

Le système de Morse prit peu à peu le dessus en Europe sur le système Wheatstone-Cooke, et en 1851 une forme européenne du morse, incluant les lettres avec accent, fut adoptée sur tout le continent. Chaque année, le morse et le télégraphe jouaient un plus grand rôle dans le monde, permettant à la police de capturer des criminels, aidant les journaux à imprimer les dernières nouvelles, et permettant à des entreprises éloignées de communiquer instantanément.

Protéger ces informations, souvent sensibles, devenait évidemment un souci majeur. Le morse n'est pas par lui-même une forme de cryptographie, puisqu'il n'a aucunement pour but de cacher le message. Les points et les traits ne sont qu'une manière simple de représenter les lettres pour l'usage du télégraphe ; le morse n'est en fait rien d'autre qu'un alphabet alternatif. Le premier problème qu'il pose pour la sécurité surgit lorsque l'expéditeur transmet son message à un opérateur de morse, qui devra le lire pour le transmettre. Les opérateurs du télégraphe avaient accès à tous les messages, ils risquaient d'être achetés par une entreprise désireuse d'avoir accès aux communications d'un concurrent. Ce problème était exposé dès 1853 dans un article publié par la revue anglaise *Quarterly Review*.

Des mesures devront être prises pour parer à une sérieuse objection que l'on soulève à propos des communications privées par télégraphe — la violation du secret — car, dans tous les cas, une demi-douzaine de personnes sont amenées à connaître chaque mot adressé par une personne à une autre. Les employés de la Compagnie anglaise du Télégraphe s'engagent au secret sous serment, mais nous écrivons souvent des choses que nous ne supporterions pas de voir lues par d'autres avant nous. C'est encore un grave défaut du télégraphe, et il faut y remédier d'une manière ou d'une autre.

La solution était de chiffrer le message confié à l'opérateur, qui traduirait en morse le message chiffré avant de le transmettre. Ce cryptage interdirait en outre la lecture du message par des espions pendant sa transmission. Le chiffre de Vigenère était le meilleur moyen d'assurer le secret : n'était-il pas qualifié d'« indéchiffrable » ? Les cryptographes, pour le moment du moins, l'emportaient sur les cryptanalystes.

M. Babbage contre le chiffre de Vigenère

La figure la plus étonnante de la cryptanalyse au XIX^e siècle est incontestablement celle de Charles Babbage, ce génie excentrique connu pour avoir posé les bases de l'ordinateur moderne. Né en 1791, il était le fils de Benjamin Babbage, un prospère banquier londonien. Quand Charles se maria sans l'autorisation paternelle, il renonça à la fortune des Babbage, mais il lui restait des moyens suffisants pour poursuivre une vie de vagabondage scientifique, appliquant son talent à toute question qui excitait son imagination. Ses inventions vont du compteur de vitesse au pare-buffle qu'on fixe à l'avant des locomotives pour écarter les bestiaux de la voie ferrée. En matière de découvertes scientifiques, il fut le premier à comprendre que, dans un tronc d'arbre, la largeur d'un anneau dépend du temps qu'il a fait dans l'année, et il en déduisit la possibilité de déterminer les climats du passé en examinant les très vieux arbres. Il s'intéressa aussi aux statistiques, au point de dresser les premières tables de mortalité, qui demeurent un outil de base pour les compagnies d'assurances aujourd'hui.

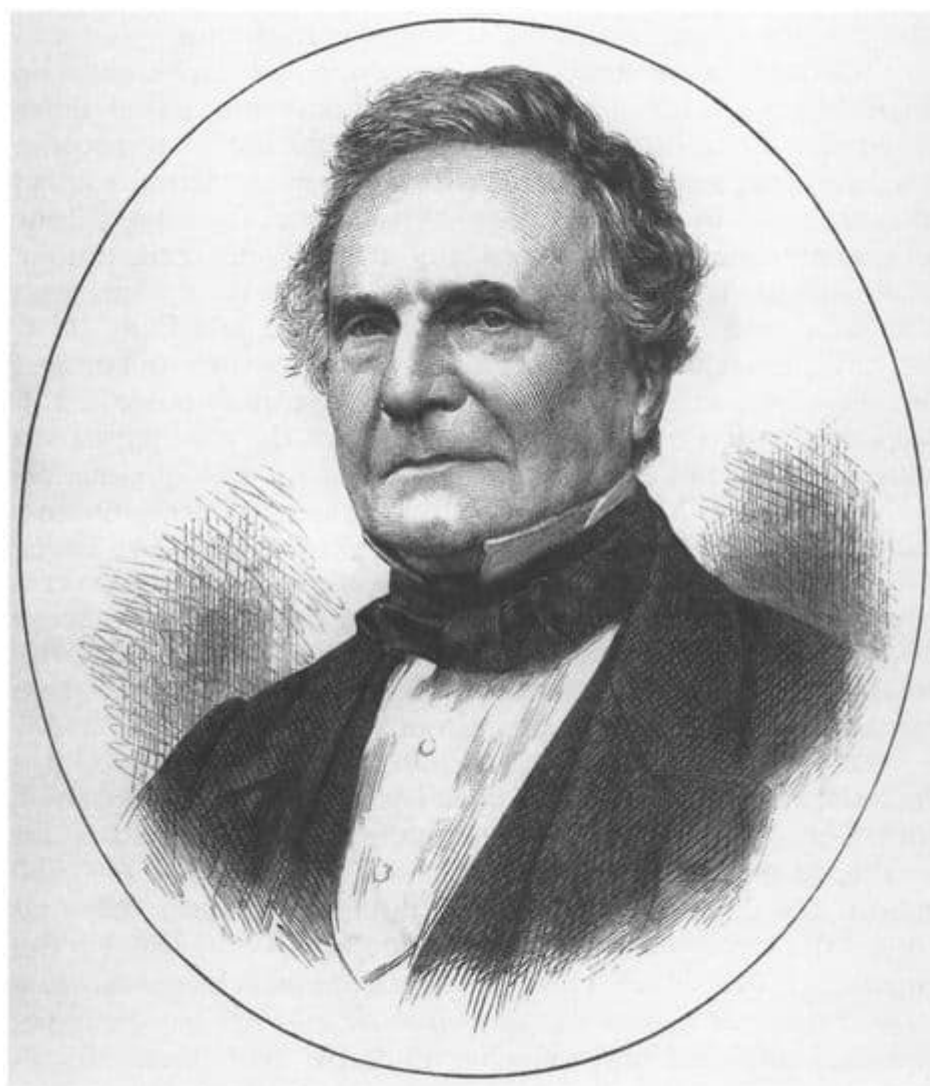


Fig. 12 Charles Babbage.

Babbage ne se limita pas aux problèmes techniques ou scientifiques. À son époque, l'affranchissement d'une lettre dépendait de la distance à parcourir. Babbage fit remarquer que le temps passé à calculer le prix pour chaque lettre revenait plus cher que le coût du transport lui-même. Il proposa donc le système que nous utilisons aujourd'hui : un prix unique indépendant de la destination de chaque lettre. Il s'intéressa aussi aux problèmes politiques et sociaux, et, vers la fin de sa vie, lança une campagne pour débarrasser les rues de Londres des organistes et autres musiciens des rues qui y traînaient. Il se plaignait de ce que « il n'était pas rare de voir danser sur cette musique des galopins en guenilles, rejoints quelquefois par des hommes à moitié ivres, qui joignaient au tumulte leurs voix discordantes (...) Une autre catégorie d'amateurs de ce genre de musique est constituée par des femmes de petite vertu et d'origines cosmopolites, qui trouvent là une bonne excuse pour exhiber

leurs charmes à la fenêtre. » Les musiciens contre-attaquèrent en se réunissant de plus en plus nombreux et en jouant aussi fort que possible autour de sa maison.

Le grand tournant de sa carrière scientifique se produisit en 1821, lorsqu'il se pencha, avec l'astronome John Herschell, sur un ensemble de tables mathématiques, du type utilisé pour les calculs appliqués à l'astronomie, à la mécanique et à la navigation. Les deux hommes furent affolés de trouver dans ces tables de nombreuses erreurs susceptibles d'entraîner des fautes dans des calculs importants. Les *Ephémérides nautiques pour trouver la latitude et la longitude en mer*, par exemple, contenaient plus de mille erreurs. Et de fait, bien des naufrages et des désastres technologiques étaient à mettre sur le compte de tables fausses.

Ces tables mathématiques étaient calculées à la main, et les fautes étaient simplement des erreurs humaines — ce qui fit dire à Babbage : « On jurerait que ces calculs ont été faits à l'emporte-pièce ! ». Cette observation marqua le début d'une tentative extraordinaire : construire une machine capable d'effectuer sans faute des calculs avec un haut degré de précision. En 1823, Babbage établit les plans d'un superbe calculateur appelé *Difference Engine N° 1*, comprenant 25 000 pièces d'une mécanique de précision, et qui devait être construit grâce à des fonds publics. Mais, brillant inventeur, Babbage était moins bon réalisateur. Après dix ans d'efforts, il abandonna *Difference Engine N° 1*, élabora un projet entièrement nouveau et se mit à construire *Difference Engine N° 2*.

Quand Babbage abandonna sa première machine, le gouvernement lui retira sa confiance et décida de limiter les pertes en renonçant au projet : 17 470 livres avaient déjà été dépensées, le prix de deux bateaux de guerre. « Proposez à un Anglais un principe, un instrument, aussi admirables soient-ils, commenta amèrement Babbage, et vous verrez que tout l'effort de l'esprit anglais visera à lui trouver une difficulté, un défaut, ou une impossibilité. Si vous lui parlez d'une machine à éplucher les pommes de terre, il vous dira que c'est impossible. Si vous en pelez une devant lui, il vous dira que cette machine est inutile puisqu'elle ne peut pas découper un ananas en tranches. »

Faute de financement, *Difference Engine N° 2* ne fut jamais achevé. Ce qui est tragique d'un point de vue scientifique, c'est que la machine de Babbage aurait été un tremplin vers la Machine Analytique. Non contente de calculer un ensemble de tables données, *Difference Engine N° 2* aurait été capable de résoudre une grande variété de problèmes

mathématiques en obéissant aux instructions qu'elle aurait reçues. La Machine Analytique était le prototype des calculateurs modernes. La maquette incluait une *mémoire* et un *moulin* (processeur) qui auraient permis de prendre des décisions et de répéter des instructions, équivalents des commandes IF, THEN et LOOP (boucle) dans la programmation moderne.

Un siècle plus tard, au cours de la Seconde Guerre mondiale, les premiers équivalents électroniques de la machine de Babbage devaient avoir des retombées importantes sur la cryptanalyse, mais Babbage lui-même apporta une autre contribution importante à la cryptanalyse. Il réussit à casser le chiffre de Vigenère, ce qui représentait le progrès le plus considérable depuis que les érudits arabes avaient brisé, au IX^e siècle, le chiffre monoalphabétique grâce à l'analyse des fréquences. Le travail de Babbage ne demandait ni calculs sur machine, ni mathématiques compliquées : rien que finesse et astuce.

Babbage s'intéressait aux chiffres depuis son plus jeune âge, à l'école. « Les plus grands faisaient des codes, se rappelait-il, mais à partir de quelques mots j'en trouvais habituellement la clef. Avec des conséquences quelquefois pénibles : les auteurs des codes détectés me tombaient dessus. » Ces coups ne le découragèrent pas, et la cryptanalyse continua à le passionner.

Dans la société londonienne, Babbage se fit rapidement la réputation d'un cryptanalyste prêt à s'attaquer à n'importe quel message, et des inconnus lui soumettaient toutes sortes de problèmes. Il aida ainsi un biographe qui tentait désespérément de déchiffrer les notes abrégées de John Flamsteed, le premier Astronome royal d'Angleterre. Il vint aussi au secours d'un écrivain, en résolvant le chiffre de la reine Henriette, femme de Charles I^{er} d'Angleterre ; puis, en 1854, il collabora avec un avocat pour apporter une preuve cryptographique dans un procès. Au fil des ans, il accumula une pile épaisse de messages cryptés, qu'il voulait utiliser comme base d'un ouvrage intitulé « *La philosophie du déchiffrement* ». Le livre proposerait deux exemples de chaque type de code, l'un dont Babbage détaillerait le déchiffrement, l'autre qui serait laissé à résoudre par le lecteur, à titre d'exercice. Malheureusement, comme beaucoup de ses projets, le livre ne fut jamais mené à son terme.

Alors que la plupart des cryptanalystes avaient définitivement renoncé à briser le chiffre de Vigenère, Babbage entreprit d'en tenter le déchiffrement à la suite d'un échange de lettres avec John Hall Brock

Thwaites, un dentiste de Bristol peu informé en matière de codes. En 1854, Thwaites annonça qu'il avait inventé un nouveau chiffre, qui se trouvait, en fait, être le chiffre de Vigenère. Il écrivit au *Journal of the Society of Arts* pour faire breveter son invention, ignorant apparemment qu'il était en retard de plusieurs siècles. Babbage, à son tour, écrivit au journal, précisant que « le code était très ancien et figurait dans de nombreux ouvrages ». Thwaites ne se démonta pas, et mit Babbage en demeure de briser son chiffrement, défi aussitôt relevé.

Faire céder un chiffre difficile ressemble à l'escalade d'une falaise. Le cryptanalyste cherche les prises et les appuis qui permettront la plus légère progression. Dans un chiffre monoalphabétique, le cryptanalyste va saisir la fréquence des lettres, car les lettres les plus répandues — *e*, *a*, et *i* — se remarqueront quelle que soit leur transformation. Dans le chiffre polyalphabétique de Vigenère, les fréquences sont beaucoup plus équilibrées, puisque le mot de code est utilisé pour passer d'un alphabet à l'autre. À première vue, le rocher semble absolument lisse.

La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières. Si le mot-clef est KILO, par exemple, chaque lettre du texte en clair peut être chiffrée de quatre façons différentes, puisque le mot-clef comporte quatre lettres. Chacune de ces lettres définit un alphabet crypté différent dans la grille de Vigenère, comme le montre le [tableau 7](#), où on a surligné la colonne *e* du carré et les lignes correspondant à KILO :

Si le K de Kilo est utilisé pour chiffrer e, la lettre chiffrée sera O
Si le I de Kilo est utilisé pour chiffrer e, la lettre chiffrée sera M
Si le L de Kilo est utilisé pour chiffrer e, la lettre chiffrée sera P
Si le O de Kilo est utilisé pour chiffrer e, la lettre chiffrée sera S

De même, des mots entiers peuvent être chiffrés de différentes manières. Le mot *thé* peut être chiffré DPP, BSS, EVO, et HRM, suivant sa position par rapport au mot-clef. Bien que cela rende la cryptanalyse difficile, elle n'est pas impossible. Le point le plus important à noter est que, s'il y a quatre façons d'écrire le mot *thé*, et que le message d'origine contient ce mot plus de quatre fois, il est certain qu'une des formes au moins du mot chiffré sera répétée dans le texte chiffré. Ceci est démontré par l'exemple suivant dans lequel la ligne « *thé russe thé jasmin thé chine* » sera chiffrée selon Vigenère avec le mot-clef KILO :

Clef	KILOKILOKILOKILOKILOKILOK
Clair	t h é r u s s e t h é j a s m i n t h é c h i n e
Chiffré	D P P F E A D S D P P X K A X W X B S S M P T B O

Le mot *thé* est chiffré DPP dans le premier et le deuxième cas, et BSS dans le troisième. La raison en est que la deuxième apparition de *thé* dans la ligne s'effectue quatre lettres plus loin que la première, ce qui est exactement la longueur du mot-clef, alors que le troisième *thé* est décalé puisqu'il commence sous le I de KILO.

Clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tableau 7 Carré de Vigenère avec le mot-clef KILO. Le mot-clef définit quatre alphabets chiffrés distincts, de sorte que la lettre *e* peut être cryptée en O, en M, en P ou en S.

Babbage comprit que des répétitions de cette sorte lui offraient la prise dont il avait besoin pour attaquer Vigenère et faire céder le *chiffre indéchiffrable*. Pour illustrer sa technique, imaginons que nous avons intercepté le texte chiffré suivant. Nous savons qu'il est chiffré à l'aide du chiffre de Vigenère, mais nous ne savons rien du message original et le mot-clef constitue pour nous un mystère.

Fig. 13 Le texte chiffré

XAUNMEESYIEDTLLFGSNBWQ
 UFXPQTYORUTYIINUMQIEUL
 SMFAFXGUTYBXXAGBHMIFII
 MUMQIDEKRIFRIRZQUHIENO
 OOIGRMLYETYOVQRYSEXOK
 IYPYOIGRFBWPIYRBQURJIY
 EMJIGRYKXYACPPQSPBVESI
 RZQRUFREDYJIGRYKXBLOPJ
 ARNPUGEFBWMILXMZSMZYXP
 NBPUMYZMEEFBUGENLRDEPB
 JXONQEZTMBWOEFIIPAHPPQ
 BFLGDEMFWFAHQ

Babbage va d'abord chercher des séquences de lettres qui apparaissent plus d'une fois dans le texte. Deux cas peuvent amener de telles répétitions. L'explication la plus évidente est que la même séquence de lettres du texte clair a été cryptée avec la même partie de la clef. L'autre possibilité, assez faible, est que deux suites de lettres différentes dans le texte clair aient été chiffrées par différentes parties de la clef qui auraient, par pure coïncidence, engendré la même suite dans le texte chiffré. Si nous nous en tenons à de longues séquences, nous rendons encore plus improbable la seconde hypothèse, et nous allons donc nous intéresser qu'aux séquences de quatre lettres ou plus. Le tableau ci-dessous est une représentation de ces répétitions, avec l'espacement entre elles.

Séquence répétée	Espace de répétition	Longueurs de clef possibles (ou facteurs)														
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	
U-M-Q-I	30	x	x		x	x				x					x	
O-I-G-R	25				x											
J-I-G-R-Y	30	x	x		x	x				x					x	

Tableau 8 Répétitions et espaces dans le texte chiffré

Aussi bien qu'à écrire le texte clair en texte chiffré, le mot-clef sert à déchiffrer le texte chiffré pour revenir au texte clair. Donc, si nous identifions le mot-clef, le déchiffrement sera facile. À ce stade nous n'avons pas assez d'indices pour trouver les lettres du mot-clef, mais le tableau nous offre quelques renseignements précieux sur sa longueur. Ayant établi le relevé des séquences qui se répètent et le nombre de caractères entre ces répétitions, nous utilisons le reste du tableau pour établir les diviseurs de ce nombre. Par exemple, la séquence U-M-Q-I- se répète après 30 lettres, et les nombres 1, 2, 3, 5, 6, 10, 15 et 30 sont appelés ses facteurs parce qu'ils divisent 30 exactement sans laisser de reste. Ces facteurs suggèrent 8 possibilités :

1 la clef est constituée de 1 lettre et se répète 30 fois entre 2 occurrences

2 la clef est constituée de 2 lettres et se répète 15 fois entre 2 occurrences

3 la clef est constituée de 3 lettres et se répète 10 fois entre 2 occurrences

4 la clef est constituée de 5 lettres et se répète 6 fois entre 2 occurrences

5 la clef est constituée de 6 lettres et se répète 5 fois entre 2 occurrences

6 la clef est constituée de 10 lettres et se répète 3 fois entre 2 occurrences

7 la clef est constituée de 15 lettres et se répète 2 fois entre 2 occurrences

8 la clef est constituée de 30 lettres et se répète 1 fois entre 2 occurrences

La dernière possibilité est à exclure, puisque la séquence O-I-G-R- se répète après 25 caractères seulement. De même, la première possibilité doit être exclue parce qu'une clef d'une seule lettre est celle d'un alphabet monoalphabétique. Pour indiquer les autres possibilités, des x sont placés sur le tableau dans les colonnes appropriées.

Pour établir si la clef est composée de 2, 3, 5, 6, 10 ou 15 facteurs, nous allons faire figurer sur le tableau les facteurs égaux ou inférieurs à 15 pour chacun des espacements. Il apparaît clairement que toutes les périodes sont divisibles par 5. La première séquence U-M-Q-I peut résulter d'un mot-clef qui tourne 6 fois entre sa première et sa deuxième occurrence. La deuxième séquence O-I-G-R peut résulter d'un mot-clef qui tourne cinq fois entre ses deux occurrences. La troisième séquence J-I-G-R-Y reviendrait après 6 cycles du mot-clef. Bref, tout se cale parfaitement sur un mot-clef de 5 lettres.

Maintenant, il va falloir découvrir les lettres en question. Pour l'instant, appelons le mot clef L_1 - L_2 - L_3 - L_4 - L_5 , L_1 représentant la première lettre du mot-clef et ainsi de suite. La lettre L_1 définit une ligne du carré de Vigenère, et procure un alphabet chiffré de substitution monoalphabétique pour la première lettre du texte clair. Toutefois, pour crypter la deuxième lettre du texte clair, le cryptographe aura utilisé L_2 pour définir une autre ligne du carré de Vigenère, procurant évidemment un autre alphabet chiffré de substitution monoalphabétique. La troisième lettre serait cryptée suivant L_3 , la quatrième suivant L_4 et la cinquième suivant L_5 . Chaque lettre du mot-clef fournit un alphabet chiffré différent. Toutefois la sixième lettre du texte clair sera à nouveau cryptée selon L_1 , la septième lettre selon L_2 et le cycle se répète jusqu'au bout. En d'autres termes, le chiffre polyalphabétique est fait, dans ce cas, de 5 chiffres monoalphabétiques, chaque chiffre monoalphabétique est responsable d'un cinquième du message, et, rappelons-nous, nous savons déjà comment cryptanalyser des chiffres monoalphabétiques.

Procédons comme suit : nous savons que l'une des lignes du carré de Vigenère, définie par L_1 , commande l'alphabet chiffré pour la 1^{re}, la 6^e, la 11^e... lettres du message. Donc si nous regardons la 1^{re}, la 6^e, la 11^e, la 16^e... lettres du texte chiffré, nous pourrions utiliser notre bonne vieille analyse de fréquences pour déterminer l'alphabet en question. Le graphique ci-dessous montre la fréquence de distribution des lettres qui apparaissent à la 1^{re}, la 6^e, la 11^e, la 16^e... places dans le texte chiffré, soit X, E, E, F...

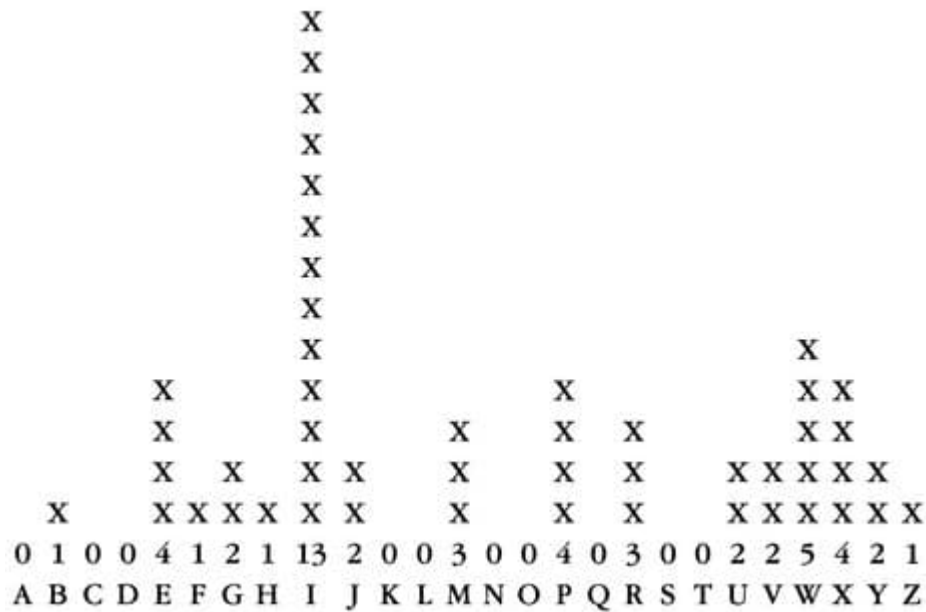


Fig. 14 Fréquences de distribution des lettres cryptées selon l’alphabet chiffré L_1 (nombre d’occurrences).

Maintenant, rappelons-nous que chaque alphabet chiffré du carré de Vigenère est un simple alphabet normal, décalé de un à vingt-six crans. Par conséquent, la répétition ci-dessus devrait présenter des traits communs avec celle d’un alphabet normal, bien que décalée d’une distance indéterminée. En comparant la répétition L_1 à la répartition banale, on devrait pouvoir repérer le décalage. Le graphique suivant illustre la répartition habituelle des lettres en français.

Le graphique de la répétition usuelle est animé de pics, de plateaux et de vallées. Son pic le plus important se trouve sous le E, précédé d’un creux sous BCD avec, pour A une présence relativement importante. Nous retrouvons dans la répartition de fréquences L_1 un schéma du même type avec un pic pour I, un creux pour FGH, et un E un peu plus long. Cela nous donne envie de superposer les alphabets en faisant coïncider le I de l’alphabet chiffré avec le E de l’alphabet normal. Dans le cas où les deux graphiques présenteraient alors à peu près la même silhouette, nous pourrions en déduire que la première lettre du mot-clef, L_1 , est probablement E.

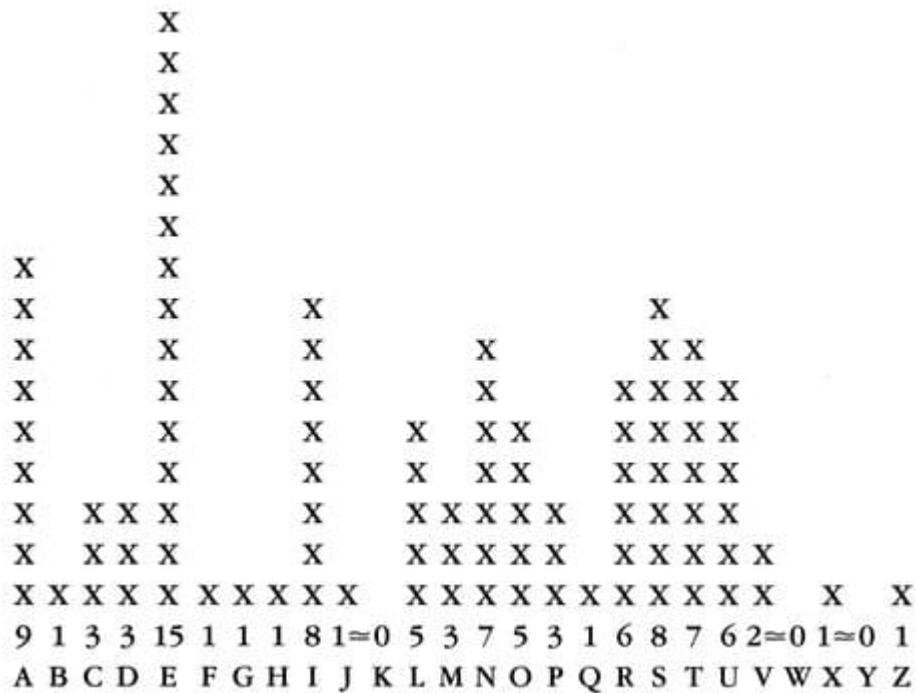


Fig. 15 Répartition des fréquences dans l'alphabet usuel.

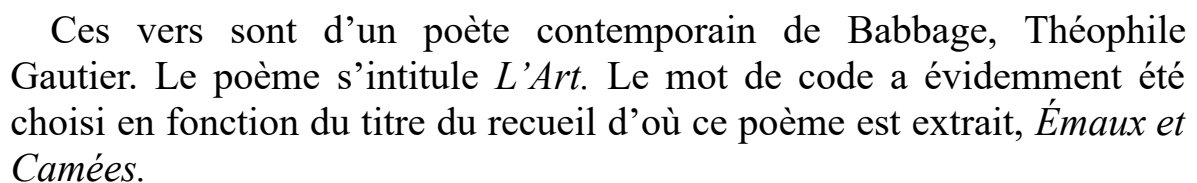
Cette superposition confirme la ressemblance entre les graphiques, nous montrant ainsi que la séquence W-X-Y-Z-A-B-C-D de l'alphabet chiffré se présente d'une manière frappante comme S-T-U-V-W-X-Y-Z dans l'alphabet usuel, ce qui confirme que L_1 est E. Nous allons recommencer la même démarche pour identifier la deuxième lettre du mot-clef. Une répartition des fréquences une fois établie pour la 2^e, la 7^e, la 12^e, la 17^e... lettres du texte chiffré, nous comparons de nouveau le graphique obtenu à celui de l'alphabet courant.

Ce graphique nous parle moins que le précédent, car nous avons avec G et Q deux pics presque aussi importants, tous deux précédés d'un schéma pour D-E-F et N-O-P qui pourrait convenir à E dans l'alphabet normal, précédé de B-C-D. Toutefois, nous pouvons trouver une autre indication dans la suite I-J-K-L. Si ces lettres absentes (0-0-0-0) correspondaient aux moins usitées couramment W-X-Y-Z, l'enchaînement amènerait à Q pour E. Cela nous donnerait, pour la deuxième lettre du mot-clef, M. Établissons ce graphique, et comparons avec l'alphabet usuel ; la [figure 18](#) nous prouve que L_2 est bien M.


```

      X
      X
      X
      X
      X
X    X          X
XX   XX        XXXX
XXX  XX        XXXX
3 2 1 2 8 0 0 0 3 0 0 4 3 2 2 1 0 6 4 3 7 0 0 0 0 0
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L

```



La cryptanalyse du chiffre de Vigenère par Babbage fut probablement achevée en 1854, peu après sa querelle avec Thwaites, mais sa découverte resta ignorée, car il ne la publia jamais. Ce travail ne fut mis en lumière qu'au XX^e siècle, lors de recherches effectuées sur l'ensemble des papiers de Babbage. Pendant ce temps, Friedrich Wilhelm Kasiski, un officier prussien à la retraite, était parvenu au même résultat. Depuis 1863, date de la publication de son livre *Die Geheimschriftren und die Dechiffir-kunst* (« Écriture secrète, et art du déchiffrement »), cette technique a porté son nom, et Babbage est resté inconnu.

Mais pourquoi Babbage se montra-t-il aussi discret ? Certes, il avait l'habitude de ne pas mener à bien ses projets et de ne pas publier ses découvertes, et il ne faut peut-être pas chercher plus loin la raison de cette négligence. Il y a toutefois une autre explication. Sa découverte intervint au début de la guerre de Crimée, et l'on peut penser qu'elle donnait aux Anglais un avantage considérable sur leur ennemi russe. Il est tout à fait possible que le renseignement britannique ait demandé à Babbage de garder son travail secret, ce qui lui aurait conféré pour un temps le monopole de cette méthode. Si c'est le cas, cette anecdote trouverait sa place dans la longue tradition du silence sur les victoires remportées par les décrypteurs, dans l'intérêt de la sécurité nationale — pratique qui se perpétue aujourd'hui.

Du courrier du cœur au trésor caché

Le chiffre de Vigenère ayant été cassé, les cryptographes ne pouvaient plus garantir le secret. Malgré tous leurs efforts pour créer de nouveaux codes, il n'apparut rien de significatif pendant la seconde moitié du XIX^e siècle, et la cryptographie professionnelle était en détresse. Or, la même période vit croître dans le public un engouement considérable pour les chiffres.

Le développement du télégraphe, qui avait suscité dans les milieux d'affaires un vif intérêt pour la cryptographie, provoqua le même phénomène dans le grand public. Celui-ci souhaitait protéger ses messages d'ordre privé et, lorsque c'était nécessaire, avait recours au cryptage, même si cela augmentait le coût du télégramme. Les opérateurs de morse pouvaient par exemple envoyer du texte clair en anglais à une vitesse atteignant trente-cinq mots/minute, parce qu'ils mémorisaient certaines phrases et les transmettaient d'un jet, alors que le fouillis de lettres formant un texte chiffré était beaucoup plus long à transmettre, obligeant l'opérateur à se reporter à la page continuellement pour vérifier la suite des lettres. Les chiffres utilisés par le grand public n'auraient pas résisté à l'attaque d'un cryptanalyste professionnel, mais ils suffisaient à mettre le texte à l'abri des indiscrets.

Lorsque le public se fut accoutumé au chiffrement, il commença à déployer ses talents cryptographiques dans divers domaines. Dans l'Angleterre victorienne, les jeunes gens amoureux n'étaient pas autorisés à manifester leurs sentiments. Sachant que leurs lettres seraient saisies et lues par les parents, ils trouvèrent comme ressource de s'envoyer des messages cryptés dans les colonnes des journaux. Ces rubriques d'annonces personnelles (baptisées en Angleterre *agony columns*) provoquèrent la curiosité des cryptanalystes, qui s'amusèrent à déchiffrer leur excitant contenu. Charles Babbage était friand de cette activité, ainsi que ses amis sir Charles Wheatstone et le baron Lyon Playfair, qui élaborèrent ensemble l'adroit chiffre de Playfair (décrit dans l'Annexe E). Un jour, Wheatstone déchiffra dans le *Times* une annonce émise par un étudiant d'Oxford qui proposait à l'objet de sa passion de s'enfuir avec lui. Quelques jours plus tard, Wheatstone fit paraître son propre message, crypté grâce au même chiffre, mettant en garde le

couple contre cet acte de rébellion irréfléchi. Peu après paraissait un troisième message, cette fois non crypté, et de la dame en question : « Cher Charlie, n'écrivez plus. Notre chiffre est découvert. »

Bientôt les journaux présentèrent d'autres sortes de textes cryptés. Les cryptographes commencèrent à faire insérer des pavés de texte chiffré, pour le seul plaisir de provoquer leurs collègues. À d'autres occasions, des notes cryptées furent utilisées pour critiquer des personnages publics ou des institutions. Dans un cas, le *Times* répandit sans le vouloir la nouvelle cryptée suivante : « Le *Times* est le Jeffreys de la presse », annonce qui stigmatisait le *Times* en donnant à entendre que, à l'image du célèbre juge du XVII^e siècle, le journal jouait de l'intimidation et se faisait le porte-parole du gouvernement.

Un autre exemple de cryptographie familière était l'usage répandu du cryptage par piquûres d'épingle. L'historien de la Grèce antique Énée le Tacticien imagina d'envoyer un message secret en piquant de minuscules trous sous certaines lettres dans une page apparemment anodine, tout comme vous voyez des points sous certaines lettres de ce paragraphe. Les lettres pointées livreront un message, aisément lu par le destinataire. Si un intermédiaire voit la page, il y a peu de chances qu'il remarque les points imperceptibles, et le message secret lui échappera. Deux mille ans plus tard, les épistoliers anglais employèrent la même méthode, non pour assurer le secret à leurs envois, mais pour éviter de payer des taxes postales excessives. Avant la réforme du service postal, dans les années 1850, envoyer une lettre coûtait environ un shilling tous les cent miles, ce qui était hors de portée pour la plupart des gens, mais les journaux ne payaient pas de taxe. Ceci laissait une brèche pour les contemporains astucieux. Au lieu d'envoyer des lettres, ils se mirent à utiliser les pointes d'épingles pour épeler leurs messages, sur la première page d'un journal. Ils n'avaient plus qu'à envoyer le journal par la poste, sans payer un penny.

La fascination grandissante exercée par les techniques de la cryptographie amena codes et chiffres à figurer en bonne place dans la littérature du XIX^e siècle. Dans le *Voyage au centre de la terre* de Jules Verne, le déchiffrement d'un parchemin couvert de caractères runiques constitue le premier pas de ce voyage épique. Les caractères proviennent d'un chiffre de substitution qui engendre un texte en latin, qui ne prend lui-même son sens que lorsqu'on inverse les lettres : « Descends dans le cratère du Yocul de Sneffels que l'ombre du Scartoris vient caresser avant les calendes de juillet, voyageur intrépide, et tu atteindras le centre

de la terre. » En 1885, Verne utilisa à nouveau un chiffre comme pivot de son roman *Mathias Sandorf*, et fit référence au *Handbuch der Kryptographie* (« Manuel de cryptographie ») de Wostrowitz. En Angleterre, l'un des écrivains les plus versés dans la cryptographie de fiction fut sir Arthur Conan Doyle. Évidemment, Sherlock Holmes était un expert en cryptographie et, comme il l'explique au docteur Watson, il était l'auteur d'une monographie sur le sujet, dans laquelle il analyse cent soixante chiffres différents. Le plus célèbre déchiffrement de Holmes est raconté dans *Les hommes dansants*, qui met en scène un chiffre composé de personnages en bâtonnets, chacune de leurs poses représentant une lettre distincte.



Fig. 19. Extrait du texte chiffré figurant dans *Les hommes dansants*, de sir Arthur Conan Doyle.

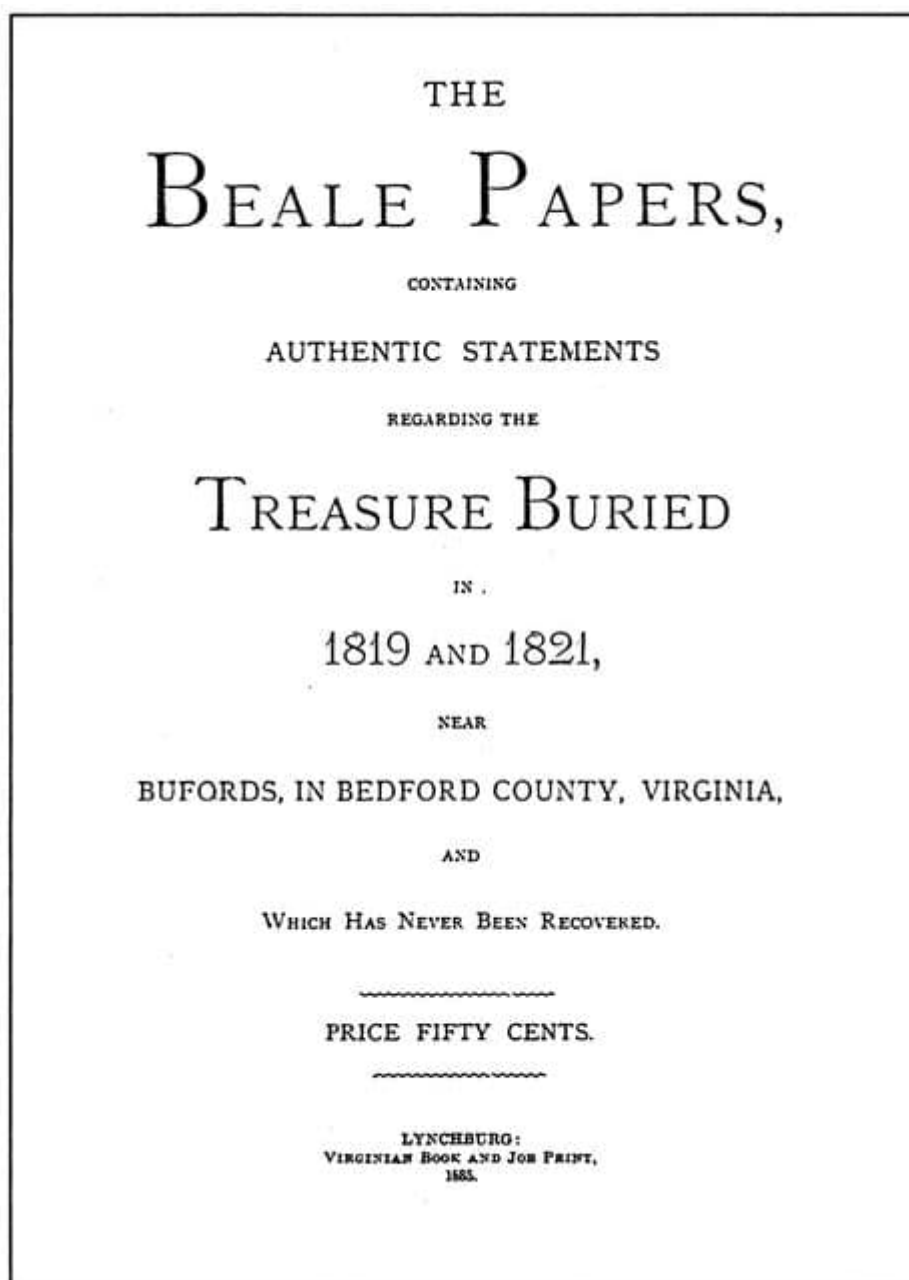
De l'autre côté de l'Atlantique, Edgar Allan Poe s'intéressait lui aussi à la cryptanalyse. Collaborant au journal de Philadelphie, *l'Alexander Weekly Messenger*, il lança un défi aux lecteurs, prétendant qu'il se faisait fort de venir à bout de n'importe quel chiffre de substitution monoalphabétique. Des centaines de lecteurs envoyèrent leurs cryptogrammes, qu'il déchiffrâ tous brillamment. Cela demande beaucoup plus que l'analyse des fréquences, et les lecteurs de Poe furent étonnés par ses prouesses. Un lecteur enthousiaste le proclama « le plus profond et le plus habile cryptographe qui ait jamais existé ».

En 1843, prompt à exploiter l'intérêt qu'il avait soulevé, Poe écrivit une nouvelle, *Le Scarabée d'or*, mettant en scène des chiffres, que les cryptographes professionnels s'accordent à juger le meilleur texte de littérature romanesque sur le sujet. William Legrand découvre un scarabée rare, le scarabée d'or, et le ramasse en se servant d'une feuille de papier. Le soir il dessine le scarabée sur cette même feuille, et regarde ensuite son dessin en le tenant devant la lueur du feu, pour vérifier son exactitude. Apparaît alors sous son dessin un texte, sans doute écrit à l'encre invisible, et révélé par la chaleur des flammes. Legrand examine les lettres qu'il découvre et se persuade qu'il a entre les mains les directives codées permettant de retrouver le trésor du capitaine Kidd. Le reste du livre est une démonstration classique d'analyse de fréquences,

qui permet le déchiffrement des indications du capitaine et la découverte de son trésor.

Le Scarabée d'or est une œuvre de pure fiction, même si une histoire réellement arrivée au XIX^e siècle offre avec cette nouvelle de nombreuses similitudes. L'affaire des chiffres de Beale réunit des cavalcades dans l'Ouest sauvage, un cow-boy qui amassa une immense fortune, un trésor enterré de vingt millions de dollars et un ensemble mystérieux de textes cryptés expliquant comment le trouver. Ce que nous connaissons de cette histoire, y compris les papiers cryptés, est contenu dans une brochure publiée en 1885 dans la ville de Lynchburg, en Virginie. Malgré sa brièveté — vingt-trois pages —, ce texte a dérouté des générations de cryptanalystes et captivé des centaines de chasseurs de trésor.

L'histoire commence en 1820, soixante-cinq ans avant la publication du fascicule, à l'hôtel Washington de Lynchburg. D'après le texte de Beale, l'hôtel et son propriétaire, Robert Morriss, jouissaient d'une grande considération : son amabilité, son honnêteté, la tenue parfaite de sa maison, faisaient de lui un hôte réputé jusque dans les États voisins. C'était la maison *par excellence* de la ville, et aucune réunion élégante ne se serait tenue ailleurs. En janvier 1820, un étranger du nom de Thomas J. Beale arriva à cheval à Lynchburg et se présenta à l'hôtel Washington. « Il mesurait environ six pieds, devait se rappeler Morriss. Il avait des yeux d'un noir de jais, les cheveux également, qu'il portait plus longs qu'on ne le faisait à l'époque. Il était bien bâti, et son allure dénotait une force et une agilité peu banales ; mais son trait le plus notable était un teint à la fois très sombre et bistré, comme si une exposition constante à l'air et au soleil l'avait tanné et décoloré ; ceci, toutefois, ne portait pas préjudice à son aspect, et j'ai trouvé qu'il était le plus bel homme que j'aie jamais vu. » Bien que Beale passât le reste de l'hiver chez Morriss et fût « extrêmement populaire, en particulier chez les dames », il n'évoqua jamais son passé, sa famille, ni les raisons de sa présence. Puis, fin mars, il partit comme il était venu.



[Fig. 20](#) Page de titre de *The Beale Papers*, la brochure qui racontait tout ce que l'on sait du mystérieux trésor de Beale.

Deux années plus tard, en janvier 1822, Beale réapparaissait à l'hôtel Washington, « plus sombre et plus tanné que jamais ». À nouveau, il passa l'hiver à Lynchburg et disparut au printemps, mais auparavant il confia à Morriss une boîte en fer fermée à clef, qui, dit-il, contenait « des papiers sans valeur ni importance ». Morriss plaça la boîte dans un coffre et l'oublia, jusqu'à qu'il reçoive une lettre de Beale, datée du 9 mai 1822, et expédiée de Saint Louis. Après quelques plaisanteries et un paragraphe à propos d'un projet d'aller « chasser le buffle et rencontrer

les sauvages grizzlis », la lettre de Beale en venait au contenu de la boîte :

Elle renferme des papiers d'une importance capitale pour ma fortune et celle de beaucoup d'autres qui sont en affaires avec moi et, si je mourais, sa perte serait irréparable. Vous pouvez juger de la nécessité de la garder avec soin, et de tout faire pour éviter une terrible catastrophe (...) Si aucun de nous ne se manifeste, gardez la boîte à l'abri pendant dix ans à compter de cette lettre, et si à l'issue de cette période ni moi ni aucune personne envoyée par moi n'en a demandé la restitution, vous l'ouvrirez, ce qui peut être fait en démontant la serrure. Vous découvrirez, en plus de papiers à vous adressés, d'autres papiers incompréhensibles sans l'aide d'une clef. J'ai confié cette clef à un ami ici, dans une enveloppe scellée à votre adresse, et en mentionnant qu'elle ne soit pas acheminée avant juin 1832. Vous apprendrez alors tout ce que vous aurez à faire.

Morriss remplit son devoir et garda la boîte, attendant que Beale vienne la chercher, mais le mystérieux voyageur ne revint pas à Lynchburg. On ne le revit plus jamais, ni là ni ailleurs. Dix ans plus tard, Morriss aurait pu suivre les instructions données par la lettre et ouvrir la boîte, mais il semble avoir hésité à briser la serrure. La lettre de Beale mentionnait qu'une note censée expliquer comment déchiffrer le contenu de la boîte serait envoyée à Morriss en juin 1832. Mais la note n'arriva jamais, et Morriss pensa peut-être qu'il ne lui servirait à rien d'ouvrir la boîte, s'il ne pouvait déchiffrer ce qu'elle recélait. Pourtant, en 1845, la curiosité l'emporta, et il força la serrure. La boîte contenait trois feuillets chiffrés et une note écrite par Beale en anglais normal.

La note révélait la vérité sur Beale, la boîte et les chiffres. Elle expliquait qu'en avril 1817, presque trois ans avant sa première rencontre avec Morriss, Beale et vingt-neuf autres hommes avaient entamé un voyage à travers l'Amérique. Après avoir parcouru les riches terrains de chasse des plaines de l'Ouest, ils atteignirent Santa Fe et passèrent l'hiver dans la « petite ville mexicaine ». En mars, ils se dirigèrent vers le nord et commencèrent à poursuivre un « immense

troupeau de buffles », en abattant autant qu'il était possible tout au long du trajet. C'est alors, selon Beale, qu'ils eurent un coup de chance.

Un jour où nous les suivions, notre groupe installa son camp dans un petit ravin, à 250 ou 300 miles au nord de Santa Fe et, ayant attaché les chevaux, se préparait pour le repas du soir, quand l'un des hommes découvrit dans une fente des rochers quelque chose qui avait l'apparence de l'or. Il le montra aux autres qui tombèrent d'accord : c'était bien de l'or, et cette découverte suscita une grande excitation.

La lettre continuait en expliquant que Beale et ses hommes, aidés par la tribu locale, creusèrent le site durant les dix-huit mois suivants, pendant lesquels ils accumulèrent une grande quantité d'or, et un peu d'argent trouvé à côté. Ils jugèrent alors que leur richesse toute neuve devait être mise en lieu sûr, et ils décidèrent de la rapporter en Virginie, où ils la garderaient dans une cachette secrète. En 1830, Beale se rendit à Lynchburg avec l'or et l'argent, trouva un endroit adéquat, et enterra le trésor. C'est à cette occasion qu'il logea à l'hôtel Washington et fit la connaissance de Morriss. Quand il repartit, à la fin de l'hiver, il alla rejoindre ses hommes qui avaient continué à travailler à la mine pendant son absence. Dix-huit mois s'écoulèrent encore, et Beale retourna à Lynchburg avec de quoi augmenter son dépôt caché. Cette fois-ci, il y avait une raison supplémentaire à son voyage :

Avant que je laisse mes compagnons dans les plaines, l'idée leur est venue que, au cas où un accident nous arriverait, le trésor caché serait perdu pour leurs familles, si des dispositions n'étaient pas prises. Je fus donc chargé de trouver une personne de confiance qui pourrait, le cas échéant, être chargée d'exécuter leurs volontés concernant leurs parts respectives.

Beale avait estimé que Morriss était cet homme intègre qu'il cherchait, ce qui justifiait de lui confier la boîte contenant les feuillets cryptés qu'on appelle aujourd'hui les chiffres de Beale. Chaque feuillet chiffré était composé d'une suite de nombres (voir [figures 21-23](#)), et déchiffrer ces nombres livrerait toutes les indications utiles. La première feuille

portait la description de l'emplacement du trésor, la deuxième énumérait son contenu, et la troisième établissait la liste des personnes à qui était attribuée une part du trésor. Quand Morriss lut cette lettre, vingt-trois ans s'étaient écoulés depuis sa dernière rencontre avec Beale. Supposant que Beale et ses hommes étaient morts, Morriss se mit en devoir de trouver l'or et de le partager entre les ayants droit désignés. Mais sans la clef il partait de zéro, et le déchiffrement des textes devint la principale occupation des vingt années qui lui restaient à vivre. Il n'y parvint jamais.

En 1862, âgé de quatre-vingt-quatre ans, Morriss sentit que ses jours étaient comptés, et il jugea qu'il devait transmettre le secret des chiffres de Beale, afin que tout espoir d'exécuter les volontés de celui-ci ne meure pas avec lui. Morriss se confia à un ami, dont l'identité demeure un mystère. Tout ce que nous savons à son propos, c'est que c'est lui qui écrivit la brochure publiée en 1885, aussi l'appellerai-je simplement « l'auteur ». L'auteur expliquait son anonymat dans le livret : « Je pense que ces papiers vont connaître une large diffusion, et, pour éviter d'être assailli par une multitude de lettres venant de tous les coins du pays, me posant toutes sortes de questions, et demandant des réponses qui, si je m'y prêtais, occuperaient tout mon temps et changeraient le caractère de mon travail, j'ai décidé de retirer mon nom de cette publication, après avoir assuré à toutes les personnes intéressées que j'ai livré tout ce que je sais sur le sujet, et que je n'ai pas un mot à ajouter à l'énoncé des faits ici formulé. » Pour protéger son identité, l'auteur demanda à un inspecteur de la voirie, James B. Ward, respecté dans le comté, d'être son agent et son éditeur.

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975,
 14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485,
 604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370,
 11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500,
 538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283,
 118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21,
 24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131,
 160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62,
 116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568,
 614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4,
 30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461,
 44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216,
 728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5,
 81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86,
 36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985,
 233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62,
 194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895,
 10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62,
 31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31,
 86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216,
 548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56,
 216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617,
 84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18,
 212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88,
 612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132,
 40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936,
 447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216,
 814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84,
 221, 736, 820, 214, 11, 60, 760.

[Fig. 21](#) Premier chiffre de Beale.

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56,
 239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122,
 106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140,
 287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41,
 78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196,
 81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 6, 191, 122, 43,
 234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46,
 10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28,
 248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113,
 140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107,
 603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8,
 14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53,
 79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515,
 125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115,
 48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121,
 12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
 85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49,
 47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2,
 270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31,
 10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250,
 557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106,
 160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353,
 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27,
 8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25,
 44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51,
 50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140,
 112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150,
 112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811,
 30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205,
 185, 112, 125, 540, 65, 106, 807, 188, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50,
 154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205,
 38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37,
 38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84,
 125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30,
 150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140,
 485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811,
 125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26, 353, 302,
 246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51,
 63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.

Fig. 22 Deuxième chiffre de Beale.

317, 8, 92, 73, 112, 89, 67, 318, 28, 96, 107, 41, 631, 78, 146, 397, 118, 98, 114, 246, 348, 116, 74, 88, 12, 65, 32, 14, 81, 19, 76, 121, 216, 85, 33, 66, 15, 108, 68, 77, 43, 24, 122, 96, 117, 36, 211, 301, 15, 44, 11, 46, 89, 18, 136, 68, 317, 28, 90, 82, 304, 71, 43, 221, 198, 176, 310, 319, 81, 99, 264, 380, 56, 37, 319, 2, 44, 53, 28, 44, 75, 98, 102, 37, 85, 107, 117, 64, 88, 136, 48, 154, 99, 175, 89, 315, 326, 78, 96, 214, 218, 311, 43, 89, 51, 90, 75, 128, 96, 33, 28, 103, 84, 65, 26, 41, 246, 84, 270, 98, 116, 32, 59, 74, 66, 69, 240, 15, 8, 121, 20, 77, 89, 31, 11, 106, 81, 191, 224, 328, 18, 75, 52, 82, 117, 201, 39, 23, 217, 27, 21, 84, 35, 54, 109, 128, 49, 77, 88, 1, 81, 217, 64, 55, 83, 116, 251, 269, 311, 96, 54, 32, 120, 18, 132, 102, 219, 211, 84, 150, 219, 275, 312, 64, 10, 106, 87, 75, 47, 21, 29, 37, 81, 44, 18, 126, 115, 132, 160, 181, 203, 76, 81, 299, 314, 337, 351, 96, 11, 28, 97, 318, 238, 106, 24, 93, 3, 19, 17, 26, 60, 73, 88, 14, 126, 138, 234, 286, 297, 321, 365, 264, 19, 22, 84, 56, 107, 98, 123, 111, 214, 136, 7, 33, 45, 40, 13, 28, 46, 42, 107, 196, 227, 344, 198, 203, 247, 116, 19, 8, 212, 230, 31, 6, 328, 65, 48, 52, 59, 41, 122, 33, 117, 11, 18, 25, 71, 36, 45, 83, 76, 89, 92, 31, 65, 70, 83, 96, 27, 33, 44, 50, 61, 24, 112, 136, 149, 176, 180, 194, 143, 171, 205, 296, 87, 12, 44, 51, 89, 98, 34, 41, 208, 173, 66, 9, 35, 16, 95, 8, 113, 175, 90, 56, 203, 19, 177, 183, 206, 157, 200, 218, 260, 291, 305, 618, 951, 320, 18, 124, 78, 65, 19, 32, 124, 48, 53, 57, 84, 96, 207, 244, 66, 82, 119, 71, 11, 86, 77, 213, 54, 82, 316, 245, 303, 86, 97, 106, 212, 18, 37, 15, 81, 89, 16, 7, 81, 39, 96, 14, 43, 216, 118, 29, 55, 109, 136, 172, 213, 64, 8, 227, 304, 611, 221, 364, 819, 375, 128, 296, 1, 18, 53, 76, 10, 15, 23, 19, 71, 84, 120, 134, 66, 73, 89, 96, 230, 48, 77, 26, 101, 127, 936, 218, 439, 178, 171, 61, 226, 313, 215, 102, 18, 167, 262, 114, 218, 66, 59, 48, 27, 19, 13, 82, 48, 162, 119, 34, 127, 139, 34, 128, 129, 74, 63, 120, 11, 54, 61, 73, 92, 180, 66, 75, 101, 124, 265, 89, 96, 126, 274, 896, 917, 434, 461, 235, 890, 312, 413, 328, 381, 96, 105, 217, 66, 118, 22, 77, 64, 42, 12, 7, 55, 24, 83, 67, 97, 109, 121, 135, 181, 203, 219, 228, 256, 21, 34, 77, 319, 374, 382, 675, 684, 717, 864, 203, 4, 18, 92, 16, 63, 82, 22, 46, 55, 69, 74, 112, 134, 186, 175, 119, 213, 416, 312, 343, 264, 119, 186, 218, 343, 417, 845, 951, 124, 209, 49, 617, 856, 924, 936, 72, 19, 28, 11, 35, 42, 40, 66, 85, 94, 112, 65, 82, 115, 119, 236, 244, 186, 172, 112, 85, 6, 56, 38, 44, 85, 72, 32, 47, 73, 96, 124, 217, 314, 319, 221, 644, 817, 821, 934, 922, 416, 975, 10, 22, 18, 46, 137, 181, 101, 39, 86, 103, 116, 138, 164, 212, 218, 296, 815, 380, 412, 460, 495, 675, 820, 952.

[Fig. 23](#) Troisième chiffre de Beale

Tout ce que nous savons de l'étrange histoire de Beale est rapporté dans cet ouvrage, et c'est grâce à son auteur que nous avons les chiffres et le récit des faits conté par Morriss. L'auteur réussit en outre à déchiffrer le deuxième chiffre de Beale. Comme le premier et le troisième, le deuxième est constitué par une page de nombres, et l'auteur supposa que chaque nombre représentait une lettre. Toutefois, la quantité de nombres était bien plus grande que celle des lettres de l'alphabet, et l'auteur pensa qu'il se trouvait en face d'un chiffre qui utilisait plusieurs nombres pour représenter la même lettre. Un chiffre qui correspond à cette définition est celui appelé *chiffre du livre*, dans lequel un livre, ou n'importe quel autre texte, est choisi comme clef.

Pour commencer, le cryptographe numérote séquentielle-ment chaque mot du texte-clef. Ensuite, chaque numéro agit comme substitut pour la lettre initiale du mot auquel il est associé. ¹Par ²exemple, ³si ⁴expéditeur ⁵et ⁶destinataire ⁷avaient ⁸décidé ⁹que ¹⁰cette “phrase ¹²serait ¹³le ¹⁴texte-clef, ¹⁵alors ¹⁶chaque ¹⁷mot ¹⁸serait ¹⁹flanqué ²⁰d’²¹un ²²nombre, ²³comme ²⁴montré ²⁵plus ²⁶bas. Après quoi, une liste serait établie, affectant à la première lettre de chaque mot le nombre qui lui est associé.

1 = p
2 = e
3 = s
4 = e
5 = e
6 = d
7 = a
8 = d
9 = q
10 = c
11 = p
12 = s
13 = l
14 = t
15 = a
16 = c
17 = m
18 = s
19 = f
20 = d
21 = u
22 = n
23 = c
24 = m
25 = p
26 = b

Dès lors, le message peut être crypté en substituant aux lettres du texte clair les nombres qui leur sont affectés sur la liste : la lettre f serait remplacée par 19, et la lettre e du texte clair serait remplacé par 2, 4 ou

5. Notre texte clair étant court, nous n'avons pas établi de nombres pour remplacer des lettres rares comme x ou z, mais nous avons assez de substituts pour écrire le mot « Beale », qui devient (26.2.7.13.5). Si le destinataire a une copie du texte-clef, le déchiffrement du message est enfantin. Toutefois, si le message chiffré est intercepté par un tiers, alors la cryptanalyse reposera sur l'identification du texte-clef. L'auteur écrit : « Me fondant sur cette idée, je fis des essais avec tous les livres que je pus me procurer, en affectant un nombre aux lettres et en comparant ces nombres à ceux du manuscrit ; tous sans succès, jusqu'à ce que la Déclaration d'Indépendance apporte la solution à l'un des papiers, et ranime tous mes espoirs. »

La Déclaration d'Indépendance se révélait être le texte-clef du deuxième chiffre de Beale et, en numérotant les mots de la déclaration, il est possible de le dévoiler. La [figure 24](#) montre le début de la Déclaration d'Indépendance, avec les mots numérotés toutes les dizaines pour aider le lecteur à comprendre comment fonctionne le déchiffrement. Le premier nombre est 115, le 115^e mot de la déclaration est *instituted*, donc le premier nombre est mis pour un i. Le deuxième nombre du texte chiffré est 73, le 73^e mot de la déclaration est *hold*, donc il représente h. En continuant ce procédé, on peut retrouver le texte clair derrière le deuxième chiffre de Beale. Son déchiffrement est imprimé dans la brochure. Voici la version française de ces révélations :

J'ai déposé dans le comté de Bedford, à quatre miles environ de Buford, dans une excavation ou caverne à six pieds au-dessous du sol, les choses suivantes, appartenant aux personnes dont les noms figurent sur la page ci jointe :

Le premier dépôt, de novembre 1819, consiste en mille quatorze livres d'or, et trois mille huit cent douze livres d'argent. Le second fut fait en décembre 1821 et consiste en mille neuf cents livres d'or, et mille deux cent quatre-vingt-huit livres d'argent ; ainsi que des bijoux, échangés à Saint Louis contre l'argent pour simplifier le transport, et estimés à 13 000 dollars.

Les biens ci-dessus sont enfermés à l'abri dans des récipients de fer, munis de couvercles de fer. La caverne est grossièrement tapissée de pierres, et les récipients sont posés sur un bloc de pierre, et couverts par d'autres. La

feuille n° 1 décrit l'emplacement exact de la caverne, afin qu'elle puisse être trouvée sans difficulté.

Il est intéressant de noter qu'il y a des erreurs dans le texte chiffré. Par exemple, le déchiffrement inclut les mots « four miles », le u découlant du 95^e mot de la Déclaration d'Indépendance, comme si celui-ci débutait par la lettre « u ». Or, le 95^e mot est « inalienable ». Cela pourrait être une erreur de transcription de Beale, mais plus probablement Beale s'appuyait sur une copie de la déclaration qui portait « unalienable », forme qu'on peut trouver dans certaines versions datant du début du XIX^e siècle. En tout cas, le déchiffrement permettait d'évaluer précisément le trésor : au moins 120 millions de francs actuels.

Declaration of Independence

¹When, ²in ³the ⁴course ⁵of ⁶human ⁷events, ⁸it ⁹becomes ¹⁰necessary for people to dissolve the political bands which ²⁰have connected them with another, and to assume among the ³⁰powers of the earth, the separate and equal station to ⁴⁰which the laws of nature and of nature's God entitle ⁵⁰them, a decent respect to the opinions of mankind requires ⁶⁰that they should declare the causes which impel them ⁷⁰to the separation.

We hold these truths to be self-evident, ⁸⁰that all men are created equal, that they are endowed ⁹⁰by their Creator with certain inalienable rights, that among these ¹⁰⁰are life, liberty and the pursuit of happiness ; That to ¹¹⁰secure these rights, governments are instituted among men, deriving their ¹²⁰just powers from the consent of the governed ; That whenever ¹³⁰any form of government becomes destructive of these ends, it ¹⁴⁰is the right of the people to alter or to ¹⁵⁰abolish it, and to institute a new government, laying its ¹⁶⁰foundation on such principles and organizing its power in such ¹⁷⁰form, as to them shall seem most likely to effect ¹⁸⁰their safety and happiness. Prudence, indeed, will dictate that governments ¹⁹⁰long established should not be changed for light and transient ²⁰⁰causes ; and accordingly all experience hath shewn, that mankind are ²¹⁰more disposed to suffer, while evils are sufferable, than to ²²⁰right themselves by abolishing the forms to which they are ²³⁰accustomed.

But when a long train of abuses and usurpations, ²⁴⁰pursuing invariably the same object evinces a design to reduce them ²⁵⁰under absolute despotism, it is their right, it is their ²⁶⁰duty, to throw off such government, and to provide new ²⁷⁰Guards for their future security. Such has been the patient ²⁸⁰sufferance of these Colonies ; and such is now the necessity ²⁹⁰which constrains them to alter their former systems of government.

Fig. 24 Les premiers paragraphes de la Déclaration d'Indépendance, avec les numérotations tous les dix mots. Ceci constitue la clef du deuxième chiffre de Beale.

Comme on l'imagine, dès qu'il sut la valeur du trésor, l'auteur fit tout son possible pour analyser les deux autres textes chiffrés, en particulier le premier qui décrit l'emplacement de la cachette. En dépit de tous ses efforts, il n'y parvint jamais, et les chiffres ne lui apportèrent que des malheurs. « En raison du temps que j'ai perdu en investigations, j'ai vu mes moyens se réduire d'une aisance convenable à une gêne absolue, entraînant des souffrances pour ceux qu'il aurait été de mon devoir de protéger, et cela, en dépit de leurs remontrances. Mes yeux se sont enfin ouverts, et j'ai décidé de rompre immédiatement, et pour toujours, tout rapport avec l'affaire, et de racheter, si c'est possible, mes erreurs. J'ai donc décidé que le meilleur moyen pour moi d'en finir avec cette tentation serait de rendre toute l'histoire publique, et de décharger mes épaules de ma responsabilité envers M. Morriss. »

Voilà comment les chiffres, et tout ce que savait l'auteur, furent publiés en 1885. Bien que l'incendie d'un hangar ait détruit la plupart des brochures, celles qui restèrent suffirent à bouleverser Lynchburg. Au nombre des plus ardents chasseurs de trésor qui se passionnèrent pour les chiffres de Beale, étaient les frères George et Clayton Hart. Pendant des années, ils se plongèrent dans les deux textes restants, tentant des attaques cryptanalytiques variées, ayant parfois l'impression qu'ils tenaient une solution. Une fausse ligne d'attaque peut engendrer quelques mots compréhensibles dans un océan de charabia, entraînant le cryptanalyste à construire une série d'arguments pour expliquer la confusion. Les frères Hart se crurent un jour si près du but qu'ils eurent recours à la dynamite pour creuser un certain site ; malheureusement, ce n'était pas le bon. Clayton Hart renonça en 1912, mais George continua à travailler sur les chiffres de Beale jusqu'en 1952. Un fanatique encore plus persévérant fut Hiram Herbert Jr., qui commença ses recherches en 1923 et qui poursuivait sa quête dans les années 70. Lui non plus ne vit pas ses efforts récompensés.

Il va sans dire que des cryptanalystes professionnels se sont également engagés sur la piste du trésor. Herbert O. Yardley, qui fonda le Bureau du chiffre américain (le cabinet noir américain) à la fin de la Première Guerre mondiale, fut intrigué par les chiffres de Beale, de même que l'éminent colonel William Friedman, le plus grand cryptanalyste américain de la première moitié du siècle. Alors qu'il dirigeait les transmissions du Service de renseignements, ce dernier inscrivit au programme de formation les codes de Beale, qu'il estimait « d'une

ingéniosité diabolique, élaborés spécialement pour leurrer le lecteur non averti ». Les archives Friedman, conservées au Centre de recherches George C. Marshall, sont fréquemment consultées par des historiens militaires, mais beaucoup plus souvent encore par des visiteurs engagés dans l'étude de Beale, et tentant de marcher dans les pas du grand homme. Plus récemment, une des figures de proue de cette chasse au trésor fut Carl Hammer, directeur retraité du département ordinateurs de Sperry Univac et l'un des pionniers de la cryptanalyse sur ordinateurs. D'après Hammer, les chiffres de Beale ont mobilisé « au moins 10 % des meilleurs cerveaux de la cryptanalyse dans ce pays. Et pas un sou dépensé pour cette quête ne l'a été en vain. Ce travail — même si les voies suivies se sont terminées en impasses — a plus que justifié les investissements par les avancées et les perfectionnements qu'il a apportés à la recherche sur les ordinateurs ». Hammer fut un membre éminent de l'*Association pour le chiffre et le trésor de Beale*, fondée dans les années 60. Au départ, l'association demanda à chaque membre de s'engager, s'il trouvait le trésor, à le partager avec les autres, mais cette obligation sembla détourner bien des prospecteurs d'y adhérer ; l'association préféra vite laisser tomber cette exigence.

En dépit des efforts combinés de l'association, des chasseurs de trésor amateurs, et des cryptanalystes professionnels, le premier et le troisième chiffres de Beale sont demeurés un mystère depuis plus d'un siècle, et son or, son argent et ses bijoux restent à trouver. De nombreuses tentatives de déchiffrement ont été faites autour de la Déclaration d'Indépendance, qui était la clef du deuxième chiffre. Une numérotation directe de la déclaration ne menant à rien pour le premier et le troisième chiffres, les cryptanalystes ont essayé divers autres schémas, comme numéroter à l'envers ou numéroter un mot sur deux, mais rien n'a marché. L'un des problèmes réside dans le fait qu'on trouve dans le premier texte chiffré des nombres allant jusqu'à 2 906, alors que la déclaration ne compte que 1 322 mots. On a donc pensé que les clefs potentielles provenaient d'autres textes, et de nombreux cryptanalystes ont penché pour la possibilité d'un système de cryptage entièrement différent.

Comment Beale parvint-il à mettre au point un système si formidable ? La réponse est que les chiffres de Beale furent inventés dans des circonstances qui donnaient au cryptographe un grand avantage. Les messages étaient émis dans le cadre d'une correspondance à sens unique, et, en raison de l'importance du trésor, Beale est peut-être allé

jusqu'à préparer un texte-clef spécial pour le premier et le troisième chiffres. Il est possible que le texte-clef ait été écrit par Beale lui-même, auquel cas les cryptanalystes n'ont effectivement aucun moyen de le retrouver, même en explorant tout ce qui a été publié. Imaginons que Beale ait écrit un récit personnel de 2 000 mots sur le sujet de la chasse aux buffles, dont il n'y aurait qu'un exemplaire. Seul le possesseur de ce manuscrit pourrait déchiffrer le premier et le troisième chiffres. Beale mentionnait qu'il avait laissé la clef « dans la main d'un ami » à Saint Louis, mais si cet ami a perdu ou détruit la clef, alors les cryptanalystes ne parviendront jamais à faire craquer les chiffres de Beale.

Créer un texte-clef unique pour un message est beaucoup plus sûr qu'utiliser une clef basée sur un livre publié, mais ce n'est faisable que si l'expéditeur dispose du temps nécessaire pour le créer et a les moyens de le transmettre au destinataire, conditions difficiles à remplir pour des transactions quotidiennes. Beale, lui, avait tout loisir pour composer son texte, le remettre à son ami à Saint Louis et pour le faire ensuite poster à la date qu'il souhaitait dans le futur.

Une autre théorie avancée pour expliquer l'inviolabilité des codes de Beale est que l'auteur de la brochure les ait délibérément falsifiés avant de les publier. Peut-être voulait-il faire sortir la clef, qui était apparemment dans les mains de l'ami de Beale à Saint Louis. S'il publiait les chiffres exacts, l'ami pourrait déchiffrer les messages et aller chercher l'or, et l'auteur ne serait pas récompensé de ses efforts. Alors que si les chiffres étaient déformés d'une certaine manière, l'ami comprendrait qu'il avait besoin de l'aide de l'auteur, contacterait l'éditeur, lequel, à son tour, contacterait l'auteur. L'auteur pourrait alors échanger les textes chiffrés exacts contre une part du trésor.

Il est encore possible que le trésor ait été trouvé depuis de nombreuses années, et que son inventeur l'ait subtilisé sans être repéré par les habitants du lieu. Certains chercheurs acharnés penchent pour la théorie de la conspiration, et prétendent que la National Security Agency (NSA) a déjà trouvé le trésor. Le service du chiffre du gouvernement américain dispose des ordinateurs les plus puissants et de quelques-uns des plus brillants cerveaux du monde, et ils peuvent très bien avoir découvert quelque chose qui aurait échappé à tous les autres. Aucune annonce n'en aurait été faite, conformément à la réputation de la NSA. N'affirme-t-on pas que NSA ne veut pas dire National Security Agency, mais *Never Say Anything*, « Ne jamais rien dire ».

Enfin, nous ne pouvons exclure que les chiffres de Beale n'aient été qu'un savant canular, et que Beale lui-même n'ait jamais existé. Des sceptiques ont suggéré qu'un inconnu, inspiré par *Le Scarabée d'or* de Poe, avait inventé toute l'histoire et écrit le fascicule pour se moquer de l'avidité des gens. Pour étayer leur théorie, ils sont allés chercher dans l'histoire de Beale des invraisemblances et des erreurs. Par exemple, si l'on en croit le fascicule, la lettre de Beale qui était dans la boîte, et théoriquement écrite en 1822, contient le mot *stampede*, mot qui apparaît pour la première fois dans un texte imprimé en 1844. Il est possible, pourtant, que ce mot ait été d'usage courant dans l'Ouest à une date plus éloignée.

Au premier rang des sceptiques figure le cryptographe Louis Kruh, qui prétend avoir trouvé la preuve que l'auteur de la brochure avait aussi écrit les lettres de Beale, celle supposée envoyée de Saint Louis et celle de la boîte. Il opéra une analyse des textes afin de détecter des similarités entre les mots attribués à l'auteur et les mots attribués à Beale. Kruh compara tous les aspects : le pourcentage de phases commençant par Le, De, ou Et, la moyenne des virgules et des points-virgules dans chaque phrase, et le style même, c'est-à-dire l'usage des négations, les passifs négatifs, les infinitifs et les relatifs. En plus des lettres de Beale et de l'ouvrage de l'auteur, l'analyse portait également sur l'écriture de trois Virginiens du XIX^e siècle. De ces cinq écritures, c'étaient celles de Beale et de l'auteur qui offraient le plus de ressemblances, ce qui permettait de les supposer de la même main. Bref, l'auteur aurait forgé les lettres attribuées à Beale, et inventé toute l'histoire.

Mais les éléments en faveur de l'authenticité des chiffres de Beale ne manquent pas non plus. En premier lieu, si les chiffres non déchiffrés étaient des canulars, on pourrait s'attendre à ce que leur créateur ait choisi les nombres plus ou moins distraitemment. Or, ces nombres suscitent divers groupements enchevêtrés. L'un de ces modèles peut être détecté en appliquant la Déclaration d'Indépendance comme clef au premier texte chiffré, ce qui ne permet pas d'obtenir des mots intelligibles, mais donne des suites comme « abfdefghiiijklmmnohpp ». Si ce n'est pas là un alphabet en ordre parfait, ce n'est certainement pas non plus un enchaînement dû au hasard. Bien que James Gillogly, le président de l'Association américaine de Cryptographie, ne fût pas convaincu de l'authenticité des chiffres de Beale, il estimait que la probabilité pour qu'une telle suite apparaisse par hasard est inférieure à une sur cent millions, suggérant ainsi que le premier texte repose bien

sur un principe cryptographique. Une autre théorie avance que la Déclaration d'Indépendance est bien la clef, mais que le texte obtenu doit être soumis à une deuxième épreuve de déchiffrement, ce qui revient à dire que le chiffre de Beale serait crypté selon un procédé en deux étapes, appelé *surchiffrement*. Dans ce cas, la suite alphabétique pourrait avoir été placée là en signe d'encouragement, comme un signal indiquant que le premier niveau du déchiffrement a été réussi.

Diverses recherches historiques plaident également en faveur de l'authenticité des chiffres. Peter Viemeister, un historien local, a rassemblé le résultat de ses travaux dans son livre *Le Trésor de Beale, Histoire d'un mystère*. Viemeister commença par se demander si Thomas Beale avait seulement existé. À l'aide du recrutement de 1790 et de divers autres documents, Viemeister identifia plusieurs Thomas Beale, nés en Virginie et dont le profil correspondait aux quelques détails que nous connaissons. Viemeister a aussi tenté de corroborer certains épisodes du livre, comme le voyage de Beale à Santa Fe et sa découverte de l'or. Une légende cheyenne datant des années 1820 raconte que de l'or et de l'argent qui avaient été trouvés dans l'Ouest furent enterrés dans des montagnes de l'Est. En 1820 également, le maître de postes de Saint Louis faisait état sur une liste d'un « Thomas Beall » (sic), ce qui correspond à la date du passage de Beale dans cette ville au cours de sa route vers l'Ouest, après son départ de Lynchburg. La plaquette faisait aussi référence à une lettre envoyée par Beale de Saint Louis en 1822.

Il semble donc bien y avoir un fondement historique à l'affaire des chiffres de Beale, et c'est cette certitude qui continue à animer les cryptanalystes passionnés et les chasseurs de trésor, tels Joseph Jancik, Marilyn Parsons et leur chien Muffin. En février 1983, ceux-ci furent inculpés de « violation de sépulture », après qu'on les eut surpris en train de creuser un trou dans le cimetière de l'église de Mountain View, en pleine nuit. Ils passèrent deux jours en prison et furent condamnés à une amende de 500 dollars. Ces amateurs peuvent se consoler avec l'idée qu'ils avaient été à peine moins chanceux que Mel Fisher, le chasseur de trésor professionnel qui récupéra pour environ quarante millions de dollars d'or provenant du galion espagnol *Nuestra Señora de Atocha*, qu'il découvrit au large de Key West en 1985. En 1989, Fisher reçut de Floride une information envoyée par un spécialiste de Beale, qui pensait que le stock de Beale était enterré au Moulin de Graham, dans le comté de Bedford, en Virginie. Épaulé par un groupe de riches investisseurs, Fisher acheta l'endroit au nom de M. Voda (pour éloigner tout soupçon),

mais malgré d'interminables travaux d'excavation, il ne trouva rien. Certains chasseurs de trésor avaient abandonné l'espoir d'éclaircir les deux chiffres insolubles et s'efforcèrent plutôt de tirer des indications de celui qui avait été déchiffré. Ainsi, tout en détaillant le contenu du trésor, le chiffre dit qu'il était déposé « à environ quatre miles de Buford », ce qui faisait probablement référence à la commune de Buford et, plus spécialement, à *Buford's Tavern*. Le chiffre mentionne aussi que « la caverne est grossièrement tapissée de pierres », et de nombreux chasseurs de trésor ont porté leurs pas vers Goose Creek, qui est riche en grandes pierres. Chaque été, la région attire des gens pleins d'espoir, certains armés de détecteurs, d'autres accompagnés de médiums ou de devins. La ville voisine de Buford offre un certain nombre d'entreprises ravies de louer de l'équipement, jusqu'à des excavateurs professionnels. Les fermiers locaux sont moins enchantés par le débarquement de ces étrangers qui piétinent leurs terres, abîment leurs haies, et forent des trous gigantesques.

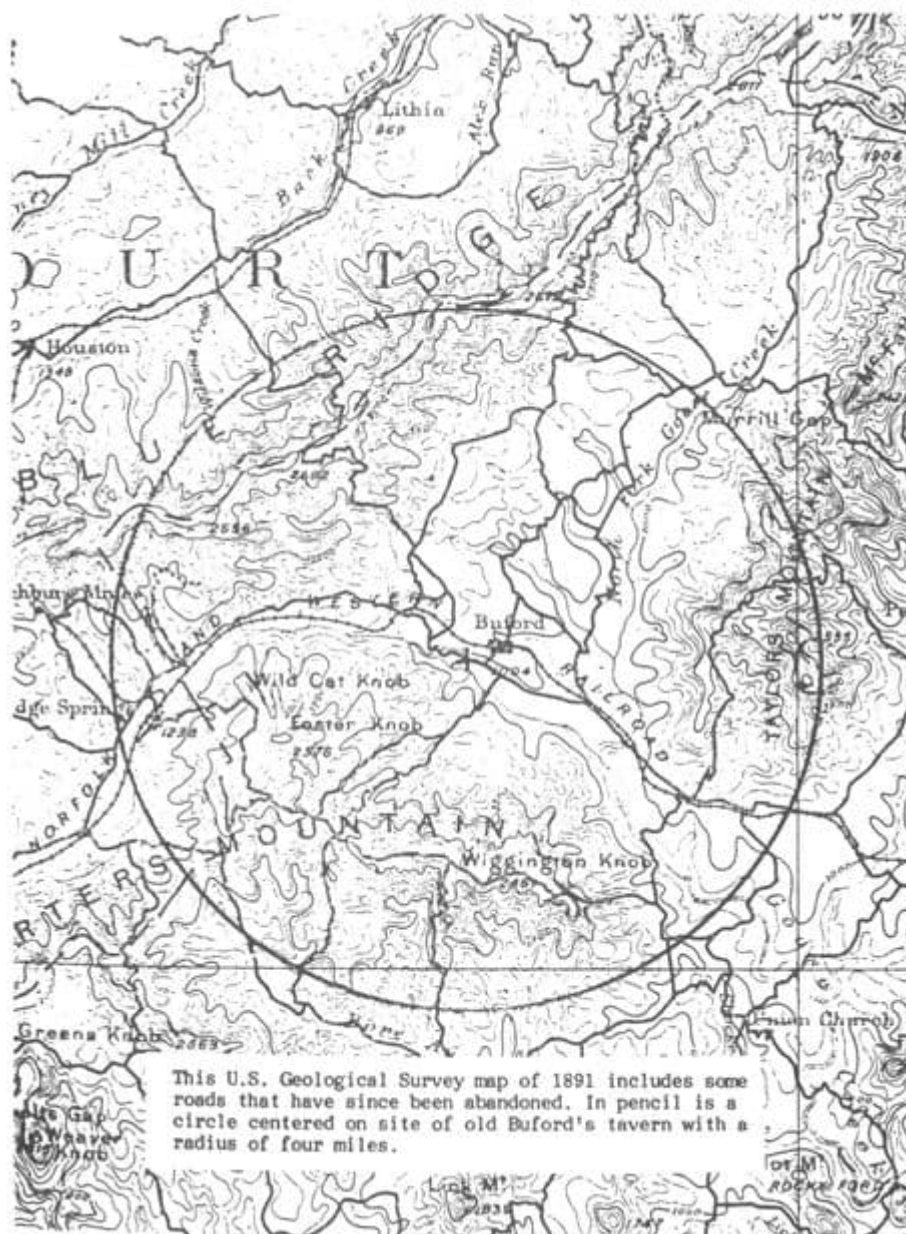


Fig. 25 Détail d'une carte des services géologiques américains de 1891. Le cercle a un rayon de 4 miles et il est centré sur *Buford's Tavern*, lieu auquel il est fait allusion dans le deuxième chiffre de Beale.

3

La mécanisation du codage

Vers la fin du XIX^e siècle, la cryptographie était dans une situation désastreuse. Depuis que Babbage et Kasiski avaient percé le secret du chiffre de Vigenère, les cryptographes étaient à la recherche d'un nouveau chiffre, qui rétablirait le secret des communications et permettrait, entre autres, aux hommes d'affaires d'exploiter sans risque l'instantanéité du télégraphe. C'est alors qu'intervint, au tournant du siècle, l'invention par le physicien italien Guglielmo Marconi d'une forme encore plus performante de télécommunication, qui rendait plus pressant le besoin d'un cryptage totalement sûr.

En 1894, Marconi entama de curieuses expériences sur les circuits électriques. Sous certaines conditions, un courant passant dans une boucle induisait un courant dans une autre boucle située à distance. En perfectionnant les deux circuits, en augmentant leur puissance et en ajoutant des antennes, Marconi put bientôt transmettre et recevoir des impulsions sur des distances de plus de deux kilomètres. Il avait inventé la TSF (Télégraphie sans fil) ou radiotélégraphie. Le télégraphe était déjà en service depuis un demi-siècle, mais il fallait un câble pour transporter le message entre l'émetteur et le récepteur, tandis que le gros avantage du système de Marconi était de n'exiger aucune liaison matérielle — le signal voyageait, comme par miracle, à travers l'éther.

En 1896, Marconi émigra en Grande-Bretagne, où il déposa son premier brevet, et se mit en quête d'un soutien financier. Il poursuivit ses expériences pour accroître la portée de ses communications radio, et transmit d'abord un message sur une distance de quinze kilomètres à travers le détroit de Bristol, puis sur cinquante kilomètres au-dessus de la Manche, vers la France. Dans le même temps, il commençait à chercher des applications commerciales de son invention. Il réussit un magnifique coup publicitaire en 1899, en équipant deux bateaux pour permettre aux journalistes qui couvraient la Coupe de l'America, la plus importante

course de voile au monde, d'envoyer leurs reportages par radio jusqu'à New York.

Plus encore, Marconi détruisit le mythe selon lequel toute communication radio était limitée par la ligne d'horizon. Les critiques avaient avancé que les ondes radio ne pouvaient se plier à la courbure de la Terre, et donc que les communications seraient limitées à une centaine de kilomètres environ. Marconi tenta de leur donner tort en envoyant un message de Poldhu, en Cornouailles, à Saint-Jean, sur Terre-Neuve, à 3 500 kilomètres. En décembre 1901, chaque jour, pendant trois heures, l'émetteur de Poldhu envoya la lettre « S » (point point point), sans arrêt, tandis que Marconi se tenait sur les falaises ventées de Terre-Neuve pour essayer de les détecter. Chaque jour, il luttait pour faire s'élever un cerf-volant géant, qui lui-même soulevait une antenne très haut dans les airs. Un peu après midi le 12 décembre, Marconi détecta enfin trois faibles points — le premier message radio transatlantique. Sa réussite resta un mystère sans explication jusqu'à ce qu'en 1924 les physiciens découvrent l'ionosphère, une couche ionisée de l'atmosphère qui commence à partir de 60 km d'altitude, et qui agit comme un miroir pour les ondes radio. Celles-ci sont réfléchies aussi à la surface de la Terre, si bien que les messages radio peuvent effectivement atteindre n'importe quel point du globe après une série de réflexions entre la Terre et l'ionosphère.

Fatalement, la découverte de Marconi fascina les militaires, qui en virent tout de suite les avantages. Avant elle, par exemple, l'autorité navale basée dans un port n'avait aucun moyen de communiquer avec ses navires, qui pouvaient disparaître pendant des mois entiers. Avec la TSF, il devenait possible de coordonner la flotte où qu'elle soit. De même, les généraux pouvaient garder continuellement le contact avec leurs bataillons, indépendamment de leurs mouvements. Cependant, cette aptitude des ondes à se propager partout est aussi leur plus grande faiblesse sur le plan militaire, puisque les messages atteindront aussi bien l'ennemi que le destinataire choisi. D'où la nécessité d'un chiffrement sûr. Et du même coup, si l'ennemi était en mesure d'intercepter tout message, alors les cryptographes se devaient de trouver le moyen d'en empêcher le déchiffrement.

Le déclenchement de la Première Guerre mondiale mit particulièrement en lumière les avantages et les risques de la radio : facilité de communication et facilité d'interception. Les belligérants

furent prompts à l'exploiter ; en même temps, ils s'interrogeaient sur sa sécurité. La concomitance de la Grande Guerre et de l'arrivée de la radio augmenta le besoin d'un cryptage efficace. On avait l'espoir de quelque nouveau chiffre qui procurerait la confidentialité pour les liaisons militaires, et pourtant, on n'enregistre aucune découverte d'importance entre 1914 et 1918, seulement un catalogue des échecs de la cryptographie. Plusieurs chiffres nouveaux apparurent, qui ne vécurent que le temps d'être déchiffrés.

L'un des plus fameux fut le code allemand ADFGVX introduit le 5 mars 1918, juste avant la grande offensive allemande qui débuta le 21 mars. Comme toute attaque, la poussée allemande devait bénéficier de l'élément de surprise, et un comité de cryptanalystes avait sélectionné l'ADFGVX parmi plusieurs options, en pensant qu'il offrait la meilleure sécurité. Sa force résidait dans sa nature convoluée, un mélange de substitution et de transposition (voir Annexe F).

Début juin 1918, l'artillerie allemande n'était qu'à 100 km de Paris, et préparait l'assaut final. Les Alliés devaient absolument briser le chiffre ADFGVX pour savoir où les Allemands avaient l'intention d'enfoncer leurs défenses. Par chance, ils avaient une arme secrète, un Français brun et fluet du nom de Georges Painvin. Doué d'une intelligence pénétrante, le lieutenant Painvin n'avait découvert ses capacités à résoudre les énigmes cryptographiques qu'à l'occasion d'une rencontre avec un membre du Bureau du Chiffre, peu après le début de la guerre. Depuis, il avait appliqué son talent à relever les faiblesses des chiffres allemands. Il se battit nuit et jour avec le chiffre ADFGVX, perdant plus de quinze kilos dans l'affaire.

La nuit du 2 juin, enfin, il put décrypter un message en code ADFGVX. La découverte de Painvin entraîna une avalanche d'autres déchiffrements, y compris celui d'un message qui comportait l'ordre suivant : « Acheminez munitions. Urgence. Même de jour si camouflés. » L'ordre signifiait un bombardement imminent et, de plus, le préambule du message en indiquait la source, c'est-à-dire le lieu de l'attaque, entre Montdidier et Compiègne, à 80 km au nord de Paris. Une reconnaissance aérienne confirma que ce devait être le centre de l'assaut allemand. Des troupes furent envoyées en renfort sur cette portion du front où, une semaine plus tard, l'attaque allemande se déclencha en effet. Ayant perdu l'avantage de la surprise, l'armée allemande fut repoussée au terme d'une terrible bataille de cinq jours.

Le déchiffrement du code ADFGVX est typique de la cryptographie au temps de la Première Guerre mondiale. Le déferlement de nouveaux codes ne recouvrait que des variantes ou des combinaisons des codes du XIX^e siècle déjà déchiffrés. Même si certains offraient, à leur apparition, une certaine sécurité, il ne fallut jamais bien longtemps pour que les cryptanalystes en viennent à bout. Le plus dur pour eux était de faire face au volume du trafic. Avant la TSF, les messages interceptés étaient des denrées rares et précieuses, et les cryptanalystes soignaient chacun d'entre eux. Mais pendant la guerre, alors même que la quantité de communications était énorme, les messages étaient tous interceptables, ce qui engendrait un flot continu de texte codé. On estime ainsi que les Français ont intercepté cent millions de mots dans les transmissions allemandes au cours de la guerre.

De tous les cryptanalystes du temps de guerre, les Français furent les plus efficaces. Au début du conflit, ils avaient déjà la plus forte équipe en Europe, et c'était là une conséquence heureuse de leur défaite humiliante dans la guerre franco-prussienne de 1870, qui semble avoir donné aux cryptanalystes français une motivation nouvelle pour s'acharner à connaître les plans de leurs ennemis.

C'est dans ce climat qu'Auguste Kerckhoffs écrivit son traité *La Cryptographie militaire*. Bien que hollandais, Kerckhoffs passa la plus grande partie de sa vie en France. Au moment où commença la Première Guerre mondiale, trois décennies plus tard, les militaires français avaient développé les idées de Kerckhoffs à l'échelle industrielle. Tandis que des génies solitaires comme Painvin cherchaient à casser les nouveaux codes, des équipes d'experts, chacune spécialisée dans un chiffre particulier, se concentraient sur les déchiffrements au jour le jour. Le facteur temps était primordial, et le tapis roulant de la cryptanalyse parvenait à alimenter les renseignements avec rapidité et efficacité.



Fig. 26 Le lieutenant Georges Painvin.

Les Français surent aussi développer plusieurs techniques parallèles pour tirer du renseignement de la radio. Ainsi, leurs postes d'écoute apprirent-ils à reconnaître le coup de patte d'un opérateur. Une fois codé, un message est envoyé en morse, série de points et de traits, et chaque opérateur peut être identifié d'après ses pauses, sa vitesse de transmission et les durées relatives de ses points et de ses tirets. La manipulation de l'opérateur est l'équivalent d'une forme d'écriture manuscrite, et donc reconnaissable. En même temps que des stations

d'écoute, les Français établirent six stations de recherche directionnelle, capables de détecter d'où provenait chaque message. Chaque station orientait son antenne de façon à obtenir un signal maximum, afin d'identifier la direction de la source. Ensuite, en croisant l'information directionnelle de plusieurs stations, on pouvait localiser exactement la source de transmission ennemie. En combinant la *signature* de l'opérateur télégraphiste et l'information directionnelle, on pouvait obtenir à la fois l'identité et la position, par exemple, d'un bataillon donné. Le renseignement français pouvait ainsi suivre ses déplacements sur plusieurs jours, et éventuellement en déduire sa destination et ses intentions. Cette forme de renseignement, appelée *analyse de trafic*, se montra particulièrement utile dans les périodes où, les clefs de chiffrement ayant été changées, la cryptanalyse était temporairement impuissante. En somme, même indéchiffrable, un message pouvait donner des informations.

La vigilance et la réussite des Français font contraste avec l'imprévoyance des Allemands, qui entrèrent en guerre dépourvus d'un bureau de renseignement militaire. Ce n'est qu'en 1916 qu'ils mirent en place l'*Abhorchdienst*, ou Service des écoutes, destiné à intercepter les messages alliés. Ce retard est dû pour partie à l'avance de l'armée allemande en territoire français durant la première période de la guerre. En se repliant, les Français détruisaient les lignes terrestres, ce qui obligeait les Allemands à utiliser la radio pour leurs communications. Cela offrait aux Français une moisson continue de messages allemands, tandis que l'inverse n'était pas vrai. Les Français qui se repliaient sur leur propre territoire pouvaient utiliser leurs lignes terrestres, privant les Allemands de leurs possibilités d'interception. C'est ce qui explique que, pendant les deux premières années de la guerre, les Allemands ne se soucièrent pas de développer leur département de cryptanalyse.

Britanniques et Américains apportèrent également d'importantes contributions à la cryptanalyse alliée. La suprématie des perceurs de code alliés est magnifiquement illustrée par le déchiffrement d'un télégramme allemand intercepté le 17 janvier 1917 par les Anglais. Cette histoire montre combien la cryptanalyse peut affecter le cours d'une guerre au plus haut niveau et montre les répercussions dévastatrices d'un cryptage inadéquat. En quelques semaines, le télégramme dévoilé força l'Amérique à repenser sa politique de neutralité, renversant ainsi l'équilibre des forces en Europe.

Pendant les deux premières années de guerre, et malgré les appels répétés d'hommes politiques de Grande-Bretagne et d'Amérique, le président Woodrow Wilson avait refusé avec constance l'envoi de troupes américaines en renfort des Alliés, autant pour éviter de sacrifier la jeunesse de son pays sur les champs de bataille d'Europe que pour rester neutre et se présenter le jour venu en position de médiateur. Convaincu qu'on ne pourrait mettre fin à la guerre que par un règlement négocié, il se réservait pour ce rôle. En novembre 1916, Wilson vit un espoir d'arrangement quand l'Allemagne nomma un nouveau ministre des Affaires étrangères, Arthur Zimmermann, une sorte de géant jovial qui semblait initier une ère nouvelle pour la diplomatie allemande. Les journaux américains titraient : « Notre ami Zimmermann » ou « Libéralisation de l'Allemagne ». Un article le proclamait « l'un des plus heureux augures pour l'avenir des relations germano-américaines ». Cependant, à l'insu des Américains, Zimmermann, qui n'avait aucune intention de chercher la paix, travaillait au contraire à étendre l'agression militaire allemande.

En 1915, un sous-marin allemand avait pris la responsabilité de couler le paquebot *Lusitania*, noyant 1 198 passagers, dont 128 citoyens américains. La perte du *Lusitania* aurait pu amener l'Amérique à entrer en guerre, n'étaient les assurances répétées des Allemands que, désormais, les sous-marins feraient surface avant d'attaquer, pour éviter de s'en prendre accidentellement à des bâtiments civils. Cependant, le 9 janvier 1917, Zimmermann participait à une réunion au château de Pless en Allemagne, où le Commandement suprême essayait de persuader le Kaiser qu'il était temps de revenir sur cette promesse, et de se lancer dans une guerre sous-marine totale. Les chefs allemands savaient que leurs sous-marins étaient quasi invulnérables lorsqu'ils expédiaient leurs torpilles en plongée, et cela pouvait bien être un facteur décisif pour l'issue de la guerre. L'Allemagne avait mis à l'eau une flotte de deux cents sous-marins, et le Commandement suprême arguait qu'en coupant les approvisionnements de la Grande-Bretagne et en l'affamant, on obtiendrait sa soumission dans les six mois.



[Fig. 27](#) Arthur Zimmermann.

Le risque était qu'une guerre sous-marine totale, avec pour conséquence inévitable la destruction de bateaux civils américains, inciterait presque à coup sûr les États-Unis à déclarer la guerre à l'Allemagne. Dans cette perspective, l'Allemagne se devait d'obtenir une capitulation des Alliés avant que l'Amérique puisse mobiliser ses troupes et peser de tout son poids sur le champ de bataille européen. À la fin de la rencontre de Pless, le Kaiser était convaincu qu'une victoire rapide

était possible, et il signa un ordre de passer à la guerre sous-marine sans restriction, à dater du 1^{er} février 1917, trois semaines plus tard.

Pendant ces trois semaines, Zimmermann mit au point une politique de sauvegarde. Si la guerre totale renforçait l'éventualité d'une entrée en guerre des États-Unis, il avait un plan pour réduire ou retarder l'engagement américain, voire l'empêcher tout à fait. Son idée était de proposer une alliance au Mexique et d'encourager son président à envahir les États-Unis et à réclamer des territoires comme le Texas, le Nouveau-Mexique et l'Arizona. L'Allemagne soutiendrait le Mexique financièrement et militairement.

De plus, Zimmermann souhaitait que le président mexicain agisse comme intermédiaire et persuade le Japon qu'il devait lui aussi attaquer l'Amérique. L'Allemagne menacerait la côte Est des États-Unis, le Japon attaquerait à l'ouest et le Mexique envahirait le sud. L'ambition de Zimmermann était de causer aux États-Unis de tels problèmes sur leur territoire qu'ils ne pourraient se permettre d'envoyer des troupes en Europe. Ainsi, l'Allemagne pourrait gagner la bataille sur mer, gagner la guerre en Europe, avant de mettre fin à la campagne américaine. Le 16 janvier, Zimmermann formula sa proposition dans un télégramme à l'ambassadeur d'Allemagne à Washington, à charge pour lui de le retransmettre à l'ambassadeur d'Allemagne à Mexico, qui devait le faire parvenir au président du Mexique :

Nous avons le projet de lancer une guerre sous-marine totale le 1^{er} février, en nous efforçant malgré tout de préserver la neutralité américaine. Pour le cas où nous ne pourrions y parvenir, nous faisons au Mexique une proposition d'alliance sur la base suivante : faire la guerre ensemble, faire la paix ensemble, un soutien financier généreux, étant entendu de notre part que le Mexique doit reconquérir ses territoires perdus au Texas, au Nouveau-Mexique et en Arizona. À vous de prendre les dispositions appropriées.

Vous informerez le Président de cela dans le secret le plus absolu, dès que le déclenchement de la guerre avec les États-Unis sera certain, et ajouterez la suggestion qu'il devra alors, de sa propre initiative, solliciter l'adhésion immédiate du Japon et, en même temps, être le médiateur entre le Japon et nous-mêmes.

Veillez bien attirer l'attention du Président sur le fait que l'emploi sans restriction de nos sous-marins offre maintenant la perspective de contraindre l'Angleterre à signer la paix dans les six mois. Accusez réception.

Zimmermann devait crypter son télégramme, car l'Allemagne savait que les Alliés interceptaient toutes les communications transatlantiques, conséquence du premier geste offensif britannique de la guerre. Un peu avant l'aube du premier jour du conflit, le bateau anglais *Telconia* s'était approché de la côte allemande et, profitant de l'obscurité, avait jeté l'ancre et halé un nœud de câbles sous-marins. Il s'agissait des câbles du réseau transatlantique allemand, son lien de communication avec le reste du monde. Au lever du jour, ce lien était rompu. Cet acte de sabotage avait pour but de détruire les moyens de transmission les plus sûrs, obligeant ainsi les Allemands à communiquer par des liaisons radio moins protégées, ou par les réseaux câblés appartenant à d'autres nations. Zimmermann fut donc contraint d'envoyer son télégramme crypté *via* la Suède, et, en appui, par le câble américain, plus direct. Les deux voies passaient par l'Angleterre, ce qui veut dire que le télégramme de Zimmermann, comme on s'en aperçut bientôt, tomba rapidement entre des mains britanniques.

Il fut immédiatement envoyé au Bureau 40, le bureau du chiffre de l'Amirauté, ainsi nommé d'après la pièce qu'il avait initialement occupée. Le Bureau 40 offrait un curieux mélange de linguistes, d'érudits classiques et de cruciverbistes forcenés, capables des exploits les plus ingénieux en cryptanalyse. L'un d'eux, le révérend Montgomery, un brillant traducteur d'ouvrages de théologie allemande, avait déchiffré un message secret caché dans une carte postale adressée à sir Henry Jones, 184 King's Road, Tighnabruaich, Écosse. La carte avait été envoyée de Turquie et sir Henry pensait qu'elle venait de son fils, alors prisonnier des Turcs. Il fut déconcerté devant l'absence totale de texte, et l'adresse était étrange : le village de Tighnabruaich était, en effet, si petit qu'aucune maison n'y portait de numéro, et il n'y avait pas de King's Road. Le révérend Montgomery comprit le message crypté de la carte. L'adresse était une allusion à la Bible, premier Livre des Rois, chapitre 18, verset 4 : « Obdyahu prit cent prophètes et les cacha, cinquante à la fois, dans une grotte où il les ravitaillait en pain et en eau. » Le fils de sir Henry avait voulu rassurer sa famille et faire savoir qu'il était bien traité dans sa captivité.

Lorsque le télégramme crypté de Zimmermann arriva au service du chiffre, c'est Montgomery qui fut chargé de le déchiffrer, avec l'aide de Nigel de Grey, un éditeur de chez William Heinemann. Ils virent immédiatement qu'ils avaient affaire à une forme de cryptage utilisée uniquement pour des communications diplomatiques au plus haut niveau, aussi s'attaquèrent-ils au télégramme en priorité absolue. Le déchiffrement était loin d'être aisé, mais ils pouvaient se fonder sur des analyses précédentes de télégrammes cryptés de la même façon. En quelques heures, le duo réussit à reconstituer quelques fragments du texte, suffisamment pour voir qu'ils travaillaient sur un message de la plus grande importance. Montgomery et de Grey persévérèrent et, en fin de journée, ils pouvaient cerner les contours du terrible plan de Zimmermann.

Montgomery et de Grey portèrent le télégramme partiellement déchiffré à l'amiral sir William Hall, directeur des renseignements de la Marine, s'attendant à ce qu'il communique l'information aux Américains, les entraînant ainsi dans le conflit. Mais l'amiral Hall plaça simplement le message dans son coffre-fort, et invita les cryptanalystes à finir d'en remplir les blancs. Hall hésitait à donner aux Américains un déchiffrement incomplet, pour le cas où une information vitale n'aurait pas encore été décryptée. Il avait aussi une autre idée derrière la tête. Si les Britanniques donnaient aux Américains le télégramme de Zimmermann déchiffré, et si les Américains réagissaient publiquement en condamnant le projet d'agression de l'Allemagne, les Allemands comprendraient que leur méthode de chiffrement avait été découverte, ce qui les conduirait à mettre au point un système plus résistant, fermant ainsi un canal majeur de renseignements. De plus, Hall savait que l'attaque des sous-marins commencerait deux semaines plus tard, et suffirait seule à obliger le président Wilson à déclarer la guerre à l'Allemagne. Il n'y avait pas de raison pour compromettre une source de renseignements aussi précieuse, alors que le but souhaité serait atteint de toute façon.

WESTERN UNION TELEGRAM

SEND THE FOLLOWING TELEGRAM, SUBJECT TO THE TERMS ON BACK HEREOF, WHICH ARE HEREBY AGREED TO

via Galveston

**GERMAN LEGATION
MEXICO CITY**

130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21580	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5101	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
23284	22200	19452	21589	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17106	13851	4458	17149	14471	6706
13850	12224	6929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21001	17388	7446	23638	18222	6719	14331	15021	23845	
3116	23552	22096	21604	4797	9497	22401	20855	4377	
23610	18140	22260	5905	13347	20420	39689	13732	20667	
6929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7632	7357	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2185	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17926	11347	17142	11264	7667	7762	15099	9110
10462	97556	3569	3670						

BEPNSTOPFF.

Charge German Embassy.

JAN 29 1917

862.2012/724

Fig. 28 Le télégramme de Zimmermann, tel qu'il fut envoyé de Washington par Bernstorff à Eckhardt, à Mexico.

Le 1^{er} février, comme le Kaiser l'avait ordonné, l'Allemagne se lança dans une guerre navale à outrance. Le 2 février, Woodrow Wilson réunit son cabinet pour décider de la réponse américaine. Le 3 février, il parla au Congrès et annonça que l'Amérique œuvrerait pour la paix, tout en maintenant sa neutralité. Cela était contraire à l'attente des Alliés comme à celle des Allemands. Le peu d'empressement des Américains à entrer dans la guerre ne laissait pas à l'amiral Hall d'autre choix que d'exploiter le télégramme de Zimmermann.

Entre-temps, Montgomery et de Grey avaient terminé le déchiffrement. Par ailleurs, Hall avait trouvé un moyen pour que les

Allemands ne soupçonnent pas la découverte de leur cryptage. Il pensa que von Bernstorff, l'ambassadeur d'Allemagne à Washington, avait dû effectuer de légères modifications au télégramme avant de le transmettre à von Eckardt, l'ambassadeur d'Allemagne à Mexico. Von Bernstorff avait notamment dû supprimer les instructions qui lui étaient personnellement destinées, et évidemment modifier l'adresse. Von Eckardt avait sans doute ensuite transmis cette version revue du télégramme, en clair, au président mexicain. Si Hall pouvait d'une manière ou d'une autre se procurer cette version mexicaine, on pourrait la publier dans la presse, et les Allemands seraient convaincus que la fuite provenait du gouvernement mexicain, et non d'une interception et d'un déchiffrement anglais réalisés au cours de la liaison vers l'Amérique. Hall contacta donc un agent à Mexico, connu comme M.H., qui infiltra le bureau du télégraphe mexicain. M.H. réussit à obtenir exactement ce qu'il voulait, à savoir la version mexicaine du télégramme de Zimmermann.

C'est cette version que Hall remit à Arthur Balfour, le ministre anglais des Affaires étrangères. Le 23 février, Balfour convoqua l'ambassadeur américain, Walter Page, et lui présenta le télégramme de Zimmermann. Balfour parla plus tard de cet entretien comme du « plus dramatique moment de sa vie ». Quatre jours plus tard, le président Wilson eut sous ses propres yeux « la preuve éloquente » — ainsi qu'il la qualifia — que les Allemands encourageaient une agression directe contre l'Amérique.

Le télégramme fut diffusé dans la presse et la nation américaine se trouva enfin confrontée aux intentions véritables de l'Allemagne. Bien que le peuple américain n'eût que peu de doutes sur la nécessité de représailles, l'administration des États-Unis tenait à s'assurer qu'il ne s'agissait pas d'un faux, forgé par les Anglais pour forcer les Américains à entrer en guerre. La question de l'authenticité fut toutefois bientôt résolue, car Zimmermann reconnut publiquement être l'auteur du télégramme. « C'est vrai. Je ne peux le nier », déclara-t-il spontanément lors d'une conférence de presse tenue à Berlin.

Le ministère allemand des Affaires étrangères chercha naturellement à savoir comment les Américains s'étaient procuré le télégramme. Dupés par le stratagème de l'amiral Hall, ils conclurent que la trahison avait bien sa source à Mexico. Hall, pendant ce temps, continuait à détourner l'attention générale du travail des cryptanalystes anglais en initiant dans la presse anglaise une campagne contre sa propre organisation, coupable,

selon les journaux, de ne pas avoir intercepté le télégramme de Zimmermann. L'opération donna lieu à une avalanche d'articles fustigeant les services secrets anglais et tressant des couronnes aux Américains.

Au début de l'année, Woodrow Wilson avait déclaré que ce serait « un crime contre la civilisation » de laisser entraîner son pays dans la guerre, mais le 2 avril 1917, il avait changé d'avis : « Je recommande que le Congrès déclare que le geste récent du gouvernement impérial ne constitue rien de moins qu'un acte de guerre à l'encontre des États-Unis, et qu'il accepte formellement le statut de belligérant qui nous a été ainsi imposé. » Une unique percée faite par les cryptanalystes du Bureau 40 avait réussi là où trois années de diplomatie intense avaient échoué. Barbara Tuchman, l'historienne américaine auteur de l'ouvrage *Le télégramme de Zimmermann*, écrit :

Si le télégramme n'avait été ni intercepté, ni publié, inévitablement les Allemands auraient fait quelque chose d'autre qui nous aurait précipités dans la guerre. Mais c'était déjà tard, et si nous avions encore tardé, les Alliés auraient peut-être été conduits à négocier. Dans cette mesure, le télégramme de Zimmermann a modifié le cours de l'histoire (...) En lui-même, le télégramme de Zimmermann n'était qu'un caillou sur la longue route de l'histoire. Mais un caillou peut tuer Goliath, et celui-ci tua l'illusion américaine que nous pouvions nous consacrer tranquillement à nos propres affaires, à l'écart des autres nations. À l'échelle des événements mondiaux, ce n'était qu'une misérable intrigue d'un ministre allemand. Dans la vie du peuple américain, c'était la fin de l'innocence.



Fig. 29 « Ça lui explose dans les mains ! » Dessin humoristique de Rollin Kirby publié le 3 mars 1917 dans *The World*.

Le Graal de la cryptographie

On pourrait établir un catalogue des victoires des cryptanalystes pendant la Première Guerre mondiale, culminant avec le déchiffrement du télégramme de Zimmermann. Depuis la résolution du chiffre de Vigenère au XIX^e siècle, les briseurs de codes avaient nettement pris le dessus sur les concepteurs de codes, mais à la fin de la guerre, alors que la cryptographie semblait en bien mauvaise posture, des scientifiques américains firent une étonnante avancée. Ils découvrirent que le chiffre de Vigenère pouvait être utilisé comme base pour une nouvelle forme de cryptage, formidablement efficace. En fait, ce nouveau chiffre offrirait une sécurité totale.

Le point faible du chiffre de Vigenère réside dans sa nature cyclique : si le mot-clef a cinq lettres, toutes les cinq lettres du texte en clair, on chiffrera avec le même alphabet. Si le cryptanalyste réussit à définir la longueur du mot-clef, le texte chiffré pourra être traité comme une série de cinq chiffres monoalphabétiques, et chacun d'eux pourra être résolu par l'analyse des fréquences. Mais voyons ce qui se passe lorsque le mot-clef est plus long.

Imaginons un texte en clair de 1 000 lettres crypté selon le chiffre de Vigenère, et essayons d'analyser le texte chiffré en résultant. Si le mot-clef utilisé n'était que de 5 lettres, alors sa cryptanalyse consisterait à appliquer l'analyse des fréquences à 5 ensembles de 200 lettres, ce qui est facile. Si le mot-clef était de 50 lettres, le cryptanalyste devrait étudier les fréquences sur 20 ensembles de 50 lettres, ce qui est déjà plus pénible. Mais si le mot-clef comportait 1 000 lettres, il faudrait alors analyser les fréquences sur 1 000 fois une lettre, ce qui est quasi impossible. En d'autres termes, si le mot-clef (ou la phrase-clef) est aussi long que le message, la technique de cryptanalyse mise au point par Babbage et Kasiski ne fonctionne plus.

Utiliser une clef aussi longue que le message nécessite évidemment que le cryptographe crée cette longue clef. Si le message fait plusieurs centaines de lettres, la clef doit être de la même longueur. Plutôt que d'établir une longue clef en partant de zéro, on peut être tenté de la faire reposer, par exemple, sur les paroles d'une chanson. Ou bien le cryptographe peut s'emparer d'un livre sur la nidification des oiseaux, et

choisir au hasard des listes de noms d'oiseaux. Et pourtant, toutes ces clefs sont défectueuses.

Dans l'exemple suivant, j'ai chiffré un texte en utilisant le chiffre de Vigenère, avec une phrase-clef de la même longueur que le message. Toutes les techniques que j'ai préalablement décrites n'en réussiront pas la cryptanalyse. Pourtant, le message peut être déchiffré.

Clef	????????????????????
Texte clair	????????????????????
Texte chiffré	NEFTRNOVEMFDYXJTLUWUJS

Ce nouveau système de cryptanalyse commence par un postulat : on suppose que le texte chiffré doit contenir certains mots courants, comme l'article *les*. Nous allons donc placer au hasard les à divers endroits du texte, et en déduire quelles lettres-clefs seraient propres à traduire les dans le mot chiffré approprié.

Par exemple, si nous estimons que *les* peut être le premier mot du texte clair, qu'en découlera-t-il pour les trois premières lettres de la clef ? La première crypterait *l* en *N*. Nous prendrons donc un carré de Vigenère, nous descendrons la colonne commençant par *l* jusqu'au *N* et identifierons la lettre qui est en tête de cette ligne et qui se trouve être le *C*.

On répète ce procédé avec le *e* et le *s* qui seraient cryptés respectivement *E* et *F*, et dans ce cas nous aurions comme trois premières lettres possibles de la clef, *CAN*. Tout ceci repose sur la supposition que *les* est le premier mot du texte clair. Nous plaçons maintenant *les* dans quelques autres situations et, à nouveau en déduisons les lettres-clefs correspondantes :

Clef	CAN???DRM????YPT?????
Texte Clair	les???les????les?????
Texte chiffré	NEFTRNOVEMFDYXJTLUWUJS

Nous avons essayé trois *les* en face de trois morceaux du texte chiffré choisis arbitrairement, et avons ainsi engendré trois possibilités qui pourraient être des parties de la clef. Comment savoir si ces *les* sont à la bonne place ? Nous supposons que la clef est formée de mots normaux, et nous pouvons utiliser ce point à notre avantage. Si *les* n'est pas à sa juste place, il en résultera probablement une étrange suite de lettres-clefs. Par contre, si ces *les* sont bien placés, les lettres-clefs devraient avoir un

début de sens. Par exemple, le premier *les* produits les lettres-clefs *CAN*, ce qui est une syllabe parfaitement vraisemblable en français. Il est possible que ce premier *les* soit à sa place. Le second engendre la suite *DRM*, combinaison de consonnes étrange et probablement une erreur. Le troisième *les* produit le segment *YPT*, syllabe peu fréquente, mais qui mérite qu'on y regarde de plus près. Si *YPT* fait réellement partie de la clef, ce serait à l'intérieur d'un mot plus long, comme *APOCALYPTIQUE*, *CRYPTE*, ou *ÉGYPTE* ou des dérivés de ces mots. Comment pouvons-nous savoir si l'un de ces mots figure dans la clef ? Nous pouvons tester les trois hypothèses en intégrant successivement les trois mots au-dessus de la section correspondante du texte chiffré et en déduisant le texte clair correspondant :

Clef	CAN?????APOCALYPTIQUE?
Texte clair	les?????exrbyml esmgaf?
Texte chiffré	NEFTRNOVEMFDYXJTLUWUJS
Clef	CAN?????CRYPTE?????????
Texte clair	les?????wglesq?????????
Texte chiffré	NEFTRNOVEMFDYXJTLUWUJS
Clef	CAN?????EGYPTE?????????
Texte clair	les?????urlesq?????????
Texte chiffré	NEFTRNOVEMFDYXJTLUWUJS

Si le mot-clef testé ne fait pas partie de la clef, il va probablement en résulter une bizarre suite de lettres dans le texte clair. S'il en fait partie, le résultat en clair devrait avoir un peu de sens. Avec *APOCALYPTIQUE*, le résultat est un mélange de lettres impossible. Avec *CRYPTE*, le texte clair devient... *wglesq...*, ce qui est en partie possible, mais *wg* serait une terminaison, ce qui n'existe dans aucun mot. Par contre, *ÉGYPTE* engendre *urlesq* qui peut provenir par exemple du mot burlesque ou être là pour... : *ur les q...*

Pour l'instant, considérons donc qu'*ÉGYPTE* fait partie de la clef. Si c'est le cas, peut-être la clef est-elle une liste de pays ? Ce qui voudrait dire que *CAN*, correspondant au premier *les*, serait là pour *CANADA*. On peut tester cette hypothèse en supposant que *CANADA* fait partie de la clef, tout comme *ÉGYPTE*.

Clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tableau 9 Carré de Vigenère.

Clef	CANADA?????ÉGYPTE????
Texte clair	l e s t o n?????u r l e s q????
Texte chiffré	N E F T R N O V E M F D Y X J T L U W U J S

Notre tentative semble avoir un sens. *CANADA* entraîne que le texte clair commencerait par *les ton...*, ce qui peut être le début de *les tons* ou *les tonnes* ou *les tonneaux*. Si l'on essaie successivement ces trois possibilités, il apparaît que *les tonneaux* nous livre le mot-clef *BRÉSIL*.

Nous avons donc une grande part de la clef *CANADABRÉSIL*, et le déchiffrement nous donne : les tonneaux sur les *q ? ? ? ?*

Pour trouver le mot qui termine le texte clair, dont nous connaissons la première lettre *q*, la meilleure stratégie serait d'essayer l'un après l'autre tous les noms de pays formés de quatre lettres et d'en déduire le texte clair. Le seul mot ayant un sens découle du mot final *CUBA*

Clef	CANADABRÉSILÉGYPTECUBA
Texte clair	les tonneaux sur les quais
Texte chiffré	NEFTRNOVEMFDYXJTLUWUJS

En conclusion, une clef de la longueur du message n'assure pas à elle seule la sécurité. La fragilité de l'exemple ci-dessus tient à l'usage, dans la clef, de mots porteurs de sens. Nous commençons par insérer *les* au hasard dans le texte et nous en tirons les lettres-clefs correspondantes. Nous pouvons savoir si nous avons mis *les* aux bonnes places, parce que les lettres-clefs ont un aspect qui les rend vraisemblables dans des mots français. Puis, nous nous servons de ces petits morceaux de clef pour en déduire des mots entiers de la clef. Cela nous fournira ensuite quelques bribes supplémentaires du message, que nous pourrions développer en mots complets et ainsi de suite.

Les allées et venues entre le message et la clef n'étaient possibles que parce que la clef avait un agencement propre, fait de mots reconnaissables. Dès 1918, les cryptographes commencèrent à tester des clefs dépourvues de toute organisation logique. Le résultat était un chiffre impossible à briser.

Alors que la Grande Guerre touchait à son terme, le major Joseph Mauborgne, qui était à la tête de la recherche cryptographique de l'armée américaine, introduisit le concept d'une *clef aléatoire*, c'est-à-dire une clef non constituée d'une suite de mots identifiables, mais plutôt d'une suite de lettres prises au hasard. Il préconisait d'appliquer l'emploi de ces clefs aléatoires au chiffre de Vigenère, pour lui apporter un niveau jamais atteint de sécurité. Le système de Mauborgne était fondé sur la compilation d'un épais bloc de papier, dont chacune des centaines de pages portait une seule clef sous la forme de lettres alignées au hasard. Deux exemplaires du bloc sont nécessaires, un pour l'expéditeur et un pour le récepteur. Pour crypter le message, l'expéditeur appliquera le chiffre de Vigenère en utilisant le premier feuillet du bloc comme clef.

Ci-dessous, nous avons trois feuilles d'un bloc (dans la réalité, chaque feuille portait des centaines de lettres), suivies par un message crypté à l'aide de la clef désordonnée de la première feuille.

	Feuille 1	Feuille 2	Feuille 3
	P L M O E	O I W V H	J A B P R
	Z Q K J Z	P I Q Z E	M F E C F
	L R T E A	T S E B L	L G U X D
	V C R C B	C Y R U P	D A G M R
	Y N N R B	D U V N M	Z K W Y I
Clef	P L M O E Z Q K J Z L R T E A V C R C B Y		
Texte clair	a t t a q u e z l a r o u t e a l a u b e		
Texte chiffré	P E F O U T U J U Z C F N X E V N R W C C		

Fig. 30 Trois clefs potentielles pour un chiffre à usage unique. Le message est chiffré selon la feuille 1.

Le destinataire pourra déchiffrer aisément le texte chiffré en utilisant la même clef, et le chiffre de Vigenère à l'envers. Une fois que le message a bien été transmis, expéditeur et destinataire détruisent le feuillet portant la clef, qui ne devra plus jamais être utilisée. Quand le message suivant est crypté, c'est avec la clef figurant sur la feuille suivante, qui sera elle aussi détruite, et ainsi de suite. Comme chaque clef ne sert qu'une seule fois, on appelle ce système : *chiffre à usage unique*, ou *clef une-fois*.

Ce chiffre supprime toutes les faiblesses des précédents. Imaginez que le message « Attaquez la route à l'aube » soit chiffré comme ci-dessus, envoyé par radio, et intercepté par l'ennemi. Il confie le texte à un cryptanalyste pour qu'il le déchiffre. Le premier obstacle est que, par définition, il n'y a pas de répétition notable dans une clef aléatoire, et la méthode de Babbage et Kasiski ne peut venir à bout de ce chiffre. Le cryptanalyste peut alors essayer de placer le mot *la* en divers endroits, et déduire la partie de la clef correspondante, comme nous l'avons fait pour le précédent message. Si le cryptanalyste essaie de placer *la* en tête du message, ce qui est une erreur, sa séquence correspondante de la clef serait AE, suite de lettres au hasard. Mais si le cryptanalyste cherche à placer *la* sur la neuvième et la dixième lettres, ce qui est juste, le résultat sera JZ, qui n'a pas plus de sens. Le cryptanalyste ne peut donc savoir si le mot qu'il essaie est, ou non, à sa juste place.

En désespoir de cause, le cryptanalyste peut tenter une recherche exhaustive de toutes les clefs. Le texte chiffré est composé de 21 lettres, le cryptanalyste sait donc que la clef est longue de 21 lettres. Ce qui offre plus de 500 000 000 000 000 000 000 000 000 000 clefs possibles, et excède toutes les possibilités humaines ou mécaniques. D'ailleurs, même si les cryptanalystes pouvaient tester toutes ces clefs, il resterait un obstacle encore plus gênant à surmonter : en vérifiant toutes les clefs, on trouverait certainement le bon message, mais on en trouverait aussi de faux. Appliquons la clef suivante au même texte chiffré : nous obtenons un message bien différent.

Clef	L J F M A P V O D L I O J F B R S I L R Y
Texte Clair	e v a c u e z t r o u p e s d e v i l l e
Texte Chiffré	P E F O U T U J U Z C F N X E V N R W C C

En essayant différentes clefs, on peut générer tous les messages de 21 lettres possibles, et le cryptanalyste ne peut distinguer le bon des autres. Cette difficulté ne se présenterait pas si la clef avait été une suite de mots ou une phrase, car les messages incorrects auraient presque certainement été engendrés par une clef dépourvue de sens, tandis que le message exact aurait été associé à une clef intelligible.

La sécurité du chiffre à usage unique tient à la rédaction aléatoire de la clef. La clef introduit une part de hasard qui empêche le cryptanalyste de saisir le texte chiffré. On peut prouver mathématiquement qu'il est impossible pour un cryptanalyste de venir à bout d'un message traité avec un chiffre à usage unique. Ce chiffre n'est pas seulement jugé infrangible, comme celui de Vigenère au XIX^e siècle, *il est réellement d'une sûreté absolue*. C'est le Graal de la cryptographie.

Les cryptographes ont donc fini par trouver ce système de cryptage parfait. On pourrait supposer que cette découverte marque la fin de toute quête du secret. En vérité, le bloc de chiffres une-fois fut à peine utilisé. Bien que parfait en théorie, il est défectueux dans la pratique, car il souffre de deux inconvénients fondamentaux. D'abord, il faut établir une quantité importante de clefs aléatoires. En une seule journée, on peut échanger dans une armée des centaines de messages, composés chacun de milliers de caractères ; ce qui entraîne la nécessité pour les soldats de disposer de clefs pour plusieurs millions de lettres quotidiennement.

Fournir autant de séquences aléatoires de lettres est une tâche insurmontable.

Quelques cryptographes pensèrent qu'ils pouvaient créer une quantité importante de clefs en tapant simplement au hasard sur une machine à écrire. Mais à chaque fois que l'on a essayé, on s'est aperçu que la dactylo était entraînée à utiliser la main droite pour taper un caractère, la gauche pour le suivant, et à alterner ainsi entre les deux côtés. C'est peut-être un moyen rapide d'établir des clefs aléatoires, mais ce n'est plus tout à fait aléatoire : si l'on frappe la lettre D sur la gauche du clavier, il est probable que la lettre suivante proviendra de la droite. Pour que la clef soit réellement aléatoire, il faudrait qu'un caractère tapé sur la partie gauche du clavier soit, en moyenne une fois sur deux, suivi par un caractère tapé sur le même côté.

Les cryptographes s'aperçurent vite qu'il fallait consacrer beaucoup de temps, d'efforts et d'argent, pour établir une clef aléatoire. Les meilleures clefs de ce type sont établies en mesurant des processus physiques naturels, comme la radioactivité qui est réputée pour son comportement vraiment aléatoire. Le cryptographe pourrait placer sur un banc un morceau d'une matière radioactive, et détecter ses radiations avec un compteur Geiger. Parfois ces émissions se succèdent rapidement, parfois elles laissent place entre elles à de longs intervalles. En somme, la durée des intervalles entre les émissions est imprévisible et aléatoire. Si le compteur Geiger était relié à un dispositif qui afficherait les lettres de l'alphabet en les faisant se succéder rapidement, mais qui se figerait lors d'une détection, la lettre apparaissant à cet instant sur l'écran serait retenue pour l'alphabet chiffré. Le dispositif fait à nouveau tourner l'alphabet, et s'arrête au hasard au moment de l'émission suivante ; la lettre qui apparaît alors sera la suivante dans la clef et on continue ainsi. Cette clef serait réellement aléatoire, mais ce système est impraticable pour une cryptographie quotidienne.

Même si vous pouvez fabriquer suffisamment de clefs, il se pose un second problème : comment allez-vous les distribuer ? Imaginez un champ de bataille où des centaines d'opérateurs radio appartiennent au même réseau de transmissions. Pour commencer, chacun doit avoir un exemplaire identique du bloc portant les codes à usage unique. Ensuite, lorsque de nouveaux blocs sont préparés, ils doivent être remis simultanément à tous. Enfin, les opérateurs doivent rester synchronisés, et bien utiliser la bonne page en même temps. Un usage répandu de ces blocs couvrirait le champ de bataille de rédacteurs et de courriers. Et si

l'ennemi s'empare d'un seul exemplaire des clefs, c'est tout le système de communication qui est compromis.

On peut être tenté de simplifier la fabrication et la distribution des clefs en réutilisant plusieurs fois la même, mais ce serait un péché cryptographique mortel. Réutiliser un chiffre permettrait à l'ennemi de déchiffrer les messages assez facilement. La technique utilisée pour forcer des textes chiffrés avec la même clef est expliquée dans l'Annexe G. Pour l'instant, il nous suffit de savoir qu'il n'y a pas de simplification possible pour ce bloc de chiffres à usage unique. Expéditeur et destinataire doivent changer de clef à chaque message. On ne peut donc recommander ce système que pour des personnes dont les communications demandent une sécurité exceptionnelle, et qui peuvent faire les frais nécessaires à l'établissement et à la répartition des clefs. La ligne directe entre les présidents russe et américain est protégée par un chiffre de ce type.

L'idée de Mauborgne ne pouvait être exploitée au cœur d'une bataille. À l'issue de la Première Guerre mondiale et de son cortège d'échecs en matière de cryptanalyse, on cherchait donc toujours un système utilisable pour le conflit suivant. Heureusement pour les cryptographes, ils ne furent pas longs à trouver une solution pour rétablir le secret des communications sur le théâtre des opérations. Bien obligés d'abandonner leur méthode avec crayon et papier, ils s'adaptèrent aux technologies les plus récentes pour brouiller leurs messages et renforcer leurs chiffres.

Développement des machines : des disques à chiffrer jusqu'à l'Enigma.

La première machine cryptographique fut le disque à chiffrer, inventé au XV^e siècle par l'architecte italien Léon Alberti, l'un des pères du chiffre polyalphabétique. Il prit deux disques de cuivre, l'un légèrement plus large que l'autre, et inscrivit l'alphabet autour de chacun d'eux. En plaçant le plus petit sur le plus grand, et en les fixant avec une aiguille faisant fonction de pivot, il construisit quelque chose qui ressemblait au disque chiffré montré sur la [figure 31](#). Les deux disques peuvent être tournés indépendamment, afin que les alphabets occupent des positions différentes l'un par rapport à l'autre, ce qui veut dire qu'ils peuvent aider à crypter un message selon le chiffre de César. Pour décaler d'une lettre, on place le A du disque intérieur sur le B du disque extérieur, le disque intérieur portant l'alphabet clair et le disque extérieur l'alphabet chiffré. Chaque lettre du texte clair se trouve en face de la lettre chiffrée qu'on utilisera pour crypter le message. Pour envoyer un message avec un décalage de cinq places, il suffit de faire tourner les disques pour que le A intérieur se trouve en face du F extérieur et le reste en découlera.

Même si le cadran d'Alberti est une machine très élémentaire, il facilite le chiffrement, et il fut utilisé pendant cinq siècles. La version qui en figure sur l'illustration 31 fut utilisée pendant la guerre de Sécession et la [figure 32](#) montre un *Codographe*, ensemble de disques utilisés par le héros éponyme de *Captain Midnight*, l'une des premières séries dramatiques diffusées par la radio américaine à ses débuts. Les auditeurs pouvaient se procurer leur codographe personnel en écrivant à Ovomaltine, la marque qui patronnait l'émission, et en envoyant l'étiquette prélevée sur une de ses boîtes. De temps en temps, le programme se terminait par un message secret du Capitaine Midnight, qui pouvait être déchiffré par les fidèles auditeurs armés de leur codographe.



[Fig. 31](#) Disque à chiffrer des Confédérés utilisé pendant la guerre de Sécession.

Le disque chiffant peut être considéré comme un *brouilleur*, qui prend chaque lettre du texte clair pour la transformer en une autre. Son mode d'opération est direct, et le chiffre qui en résulte est assez facile à briser, mais on peut aussi l'employer d'une manière plus sophistiquée. Son inventeur, Alberti, suggéra de changer la position des disques au cours du message, ce qui engendre un chiffre polyalphabétique au lieu d'un chiffre monoalphabétique.



[Fig. 32](#) Codographe du *Captain Midnight*.

Imaginons qu'Alberti ait utilisé son disque pour chiffrer le mot *gondole* avec le mot-clef LEON. Il commencerait par orienter son disque d'après la première lettre du mot-clef, tournant la lettre A intérieure en face de la lettre L extérieure. Il cryptera la première lettre du message, g, en la relevant sur le disque intérieur et en transcrivant la lettre correspondante sur le disque extérieur, qui est R. Pour la deuxième lettre, il tournera le disque pour placer le A intérieur face au E extérieur. Il chiffrera alors o en le repérant sur le disque intérieur et en notant la lettre correspondante sur le disque extérieur, qui est S. Le processus continue avec la position du disque fixée successivement en fonction de la lettre-clef O, puis de la lettre-clef N et à nouveau L, et ainsi de suite. Alberti avait effectivement crypté un message selon le chiffre de Vigenère, avec son prénom comme mot-clef. Le disque à chiffrer accélère le cryptage et réduit les erreurs par rapport à un chiffrement réalisé avec le carré de Vigenère.

Le trait le plus intéressant de cet usage du disque à chiffrer est qu'il change le mode de brouillage au cours du cryptage. Bien que cette complication supplémentaire rende le chiffre plus difficile à briser, elle ne le rend pas invulnérable, puisque nous ne faisons qu'appliquer une version mécanisée du chiffre de Vigenère, qui avait été brisé par Babbage et Kasiski. Toutefois, cinq cents ans après Alberti, une version plus complexe de son disque à chiffrer devait conduire à une nouvelle génération de chiffres, plus difficiles à résoudre qu'aucun autre auparavant.

En 1918, l'inventeur allemand Arthur Scherbius et son ami Richard Ritter fondèrent la société Scherbius et Ritter, une entreprise qui cherchait à apporter des innovations techniques dans tous les domaines, depuis les turbines jusqu'aux oreillers chauffants. Scherbius dirigeait la recherche et le développement, et courait sans cesse après de nouvelles idées. L'un de ses projets favoris était de remplacer les systèmes dépassés de cryptographie en usage pendant la Première Guerre mondiale en balayant crayons et papiers au profit d'une nouvelle forme de cryptage qui exploiterait la technologie du XX^e siècle. Il avait étudié les applications techniques de l'électricité à Hanovre et Munich, et il mit au point une machine cryptographique qui était une version électrifiée du disque d'Alberti. Appelée *Enigma*, l'invention de Scherbius allait se révéler le plus redoutable système de cryptage de l'histoire.

La machine Enigma de Scherbius était faite de composants ingénieux, qu'il combina dans une formidable machine à chiffrer. Toutefois, si nous démontons la machine et que nous la reconstruisons progressivement, ses principes de base deviennent évidents. Dans sa forme élémentaire, elle consiste en trois éléments reliés par des câbles : un clavier pour entrer chaque lettre du texte clair, un brouilleur qui crypte chaque lettre du texte clair en une lettre chiffrée, et un tableau lumineux fait d'un certain nombre de lampes pour afficher la lettre du texte crypté. La [figure 33](#) montre un schéma stylisé de la machine, limité à un alphabet de 6 lettres pour simplifier. Pour crypter une lettre du texte clair, on envoie une impulsion électrique qui passe à travers l'unité centrale de brouillage, et sort de l'autre côté, en allumant une lampe du tableau, qui indique la lettre correspondante du texte chiffré. La partie la plus importante de la machine, le brouilleur, est un tambour en matériau isolant portant sur chaque face des contacts électriques. Venant du clavier, les fils pénètrent dans le tambour en 6 points (6 dans notre exemple, 26 pour l'alphabet

complet), font à l'intérieur un parcours animé de boucles et de virages, et ressortent sur l'autre face en 6 points. Les montages internes déterminent comment les lettres du texte clair seront cryptées. Par exemple sur la [figure 33](#), les montages des fils entraînent que :

taper *a* allumera la lettre *B*, ce qui signifie que *a* est cryptée *B*
 taper *b* allumera la lettre *A*, ce qui signifie que *b* est cryptée *A*
 taper *c* allumera la lettre *D*, ce qui signifie que *c* est cryptée *D*
 taper *d* allumera la lettre *F*, ce qui signifie que *d* est cryptée *F*
 taper *e* allumera la lettre *E*, ce qui signifie que *e* est cryptée *E*
 taper *f* allumera la lettre *C*, ce qui signifie que *f* est cryptée *C*

Le message *café* sera crypté DBCE. Dans ce montage basique, le brouilleur ne fait que définir un alphabet chiffré, et la machine met simplement en œuvre un chiffre de substitution monoalphabétique.

L'idée suivante de Scherbius est de faire pivoter le tambour automatiquement de $1/6^e$ de tour à chaque fois qu'une lettre est cryptée ($1/6^e$ dans notre exemple, mais $1/26^e$ dans le cas de l'alphabet complet). Sur la figure 34(a), nous avons la même disposition que sur la [figure 33](#) et, à nouveau, taper la lettre *b* commande l'éclairage de la lettre *A*. Mais cette fois, après cette lettre, le brouilleur effectue une rotation d' $1/6^e$ jusqu'à la position montrée sur la figure 34(b). Taper maintenant la lettre *b* allumera une autre lettre, ici *C*. Tout de suite après, le rotor avance d' $1/6^e$ à nouveau jusqu'à la position de la figure 34(c). Cette fois taper *b* allumera *E*

Taper la lettre *b* six fois de suite produira le texte chiffré suivant : ACEBDC. En d'autres termes, l'alphabet chiffré change après chaque lettre cryptée. Avec ce rotor sont définis six alphabets chiffrés et la machine peut être utilisée pour appliquer un chiffre polyalphabétique.

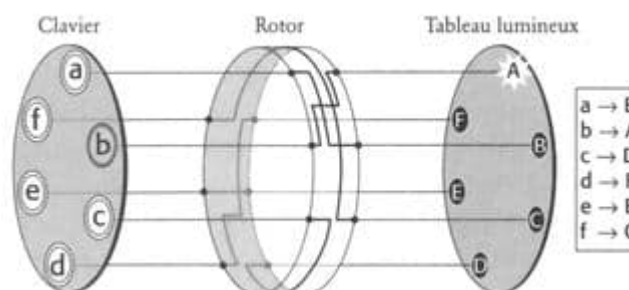


Fig. 33 Version simplifiée de la machine Enigma avec un alphabet réduit à 6 lettres. L'élément le plus important de la machine est le rotor central. Lorsqu'on tape *b* sur le clavier, à gauche, le courant est envoyé dans le rotor, où il suit le dessin de son câblage interne et ressort ensuite de

façon à allumer la lampe A : b est crypté A. L'encadré de droite montre comment sont cryptées les 6 lettres.

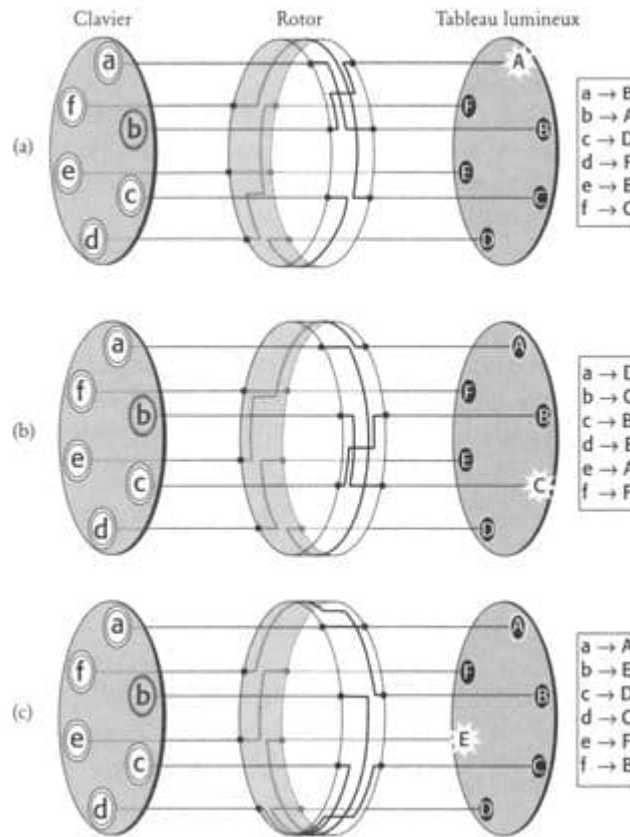


Fig. 34 À chaque fois qu'une lettre a été tapée sur le clavier, puis cryptée, le rotor tourne d'un cran, changeant ainsi le cryptage de la lettre suivante. Sur (a) le rotor crypte b en A, mais sur (b) la nouvelle orientation du rotor crypte b en C. En (c), après une autre rotation, le rotor crypte b en E. Lorsqu'il aura crypté 4 lettres de plus et aura tourné encore de 4 places, le rotor retrouvera son orientation d'origine.

La rotation du brouilleur est le principal atout du concept de Scherbius. Pourtant, telle qu'elle se présente, la machine souffre d'une évidente faiblesse. Après avoir crypté *b* six fois différemment, le tambour retrouve sa position initiale et le même schéma se répète. En général, les cryptographes sont soucieux d'éviter la répétition, qui produit dans le texte chiffré une structure et une régularité symptomatiques d'un chiffre faible. Ce défaut peut être pallié par l'adjonction d'un deuxième tambour.

La [figure 35](#) présente le schéma d'une machine à chiffrer à deux brouilleurs, ou rotors. Vu la difficulté de dessiner un brouilleur en trois dimensions, avec les fils intérieurs eux aussi en trois dimensions, la [figure 35](#) n'offre qu'une représentation en deux dimensions. Chaque fois qu'une lettre est cryptée, le premier rotor tourne d'un cran ; le deuxième rotor reste immobile pendant cette opération, il ne bouge que lorsque le

premier rotor a effectué un tour complet. Le premier rotor comporte une dent, et ce n'est que lorsque cette dent atteint un certain point qu'elle fait tourner le deuxième rotor d'un cran.

Sur la figure 35(a), le premier rotor est sur le point de déclencher le mouvement du deuxième. Après la frappe et le cryptage d'une lettre, sur la figure 35 (b), le premier rotor a tourné d'un cran et le deuxième également. Sur la figure 35(c), le premier brouilleur a bougé à nouveau d'une place et le deuxième est resté immobile. Ce dernier ne bougera à nouveau qu'après un cycle complet du premier, ce qui demande encore cinq opérations. On peut rapprocher ce système d'un compteur kilométrique : le rotor qui porte la représentation des kilomètres tourne vite et lorsque après des révolutions successives il atteint le 9, il entraîne le rotor portant les dizaines à avancer d'une unité.

L'avantage apporté par le deuxième rotor est que le processus de cryptage ne sera pas répétitif avant que le deuxième rotor ait accompli une révolution complète, soit le cryptage de $6 \times 6 = 36$ lettres au total. Autrement dit, il y a 36 positions différentes des rotors, ce qui équivalent à 36 alphabets chiffrés. Avec un alphabet complet, la machine à chiffrer jouerait sur $26 \times 26 = 676$ alphabets chiffrés.

Nous commençons maintenant à voir que, en multipliant les brouilleurs, on peut construire une machine à crypter qui passera sans cesse à des alphabets différents. L'opérateur tape une certaine lettre et, suivant la position du rotor, elle sera cryptée selon un alphabet chiffré pris parmi des centaines. Ensuite la position du rotor change en sorte que, lorsque la lettre suivante est tapée, un alphabet différent la crypte. De plus, ceci se fait avec précision et rapidité, grâce au mouvement automatique des rotors mus par l'électricité.

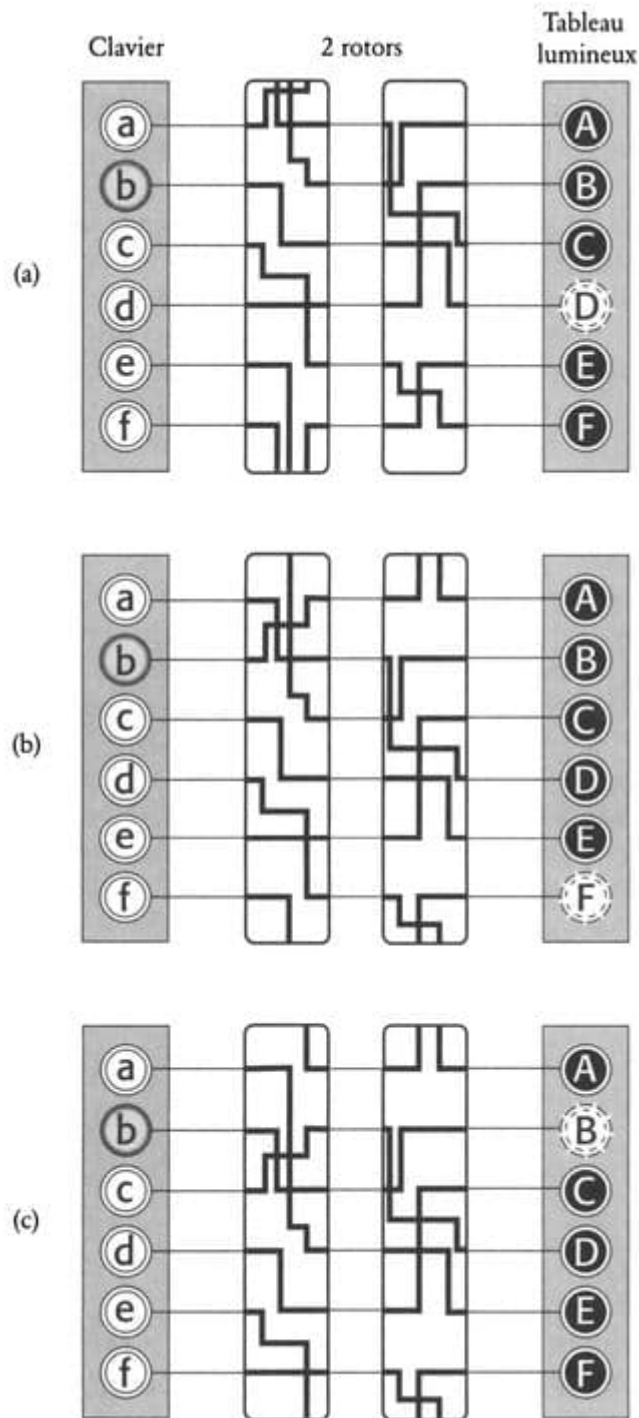


Fig. 35 En ajoutant un second rotor, le mode de cryptage ne se répète pas avant que 36 lettres aient été chiffrées ; à ce stade les deux rotors ont regagné leurs positions initiales. Pour simplifier le diagramme, les rotors sont représentés en deux dimensions : au lieu de tourner d'un cran, les câblages descendent d'un cran. Si un fil semble sortir par le haut ou par le bas d'un rotor, on continue à suivre son parcours en le reprenant en bas ou en haut du même rotor. Sur (a), b est crypté D. Après le cryptage, le premier rotor tourne d'une place, entraînant le deuxième rotor à tourner aussi d'une place. Ceci ne se produit qu'après une complète révolution du premier rotor. La nouvelle position est montrée sur (b), où b est crypté F. Après cryptage, le premier rotor tourne d'une place, mais cette fois le deuxième ne bouge pas. La nouvelle position est sur (c) où b est crypté B.

Avant de voir en détail comment Scherbius concevait l'usage de sa machine, il faut décrire deux éléments supplémentaires de la machine Enigma, qui sont montrés sur la [figure 36](#). D'abord, la machine à crypter de Scherbius était dotée d'un troisième rotor, afin d'ajouter à sa complexité : pour un alphabet de 26 lettres, ces trois rotors procurent $26 \times 26 \times 26 = 17\,576$ positions différentes de brouillage. Ensuite Scherbius ajouta un *réflecteur*. Le réflecteur est fait un peu comme un brouilleur, puisque c'est un tambour avec des câblages internes, mais il ne tourne pas et, de plus, les fils qui entrent d'un côté ressortent du même. Avec le réflecteur, lorsque l'opérateur tape une lettre qui envoie un signal électrique à travers les trois rotors, le réflecteur reçoit le signal entrant et le renvoie à travers les trois mêmes rotors, mais suivant un autre circuit. Avec un schéma conforme à la [figure 36](#), taper la lettre *b* envoie à travers les trois rotors et le réflecteur un signal qui revient par d'autres circuits et arrive à la lettre D. En réalité, le signal ne ressort pas sur le clavier, mais sur le tableau lumineux. À première vue, le réflecteur peut sembler une addition sans intérêt, puisque sa nature statique n'augmente pas le nombre des chiffres possibles. Mais les avantages qu'il apporte deviennent évidents lorsqu'on examine comment un message est crypté, puis décrypté.

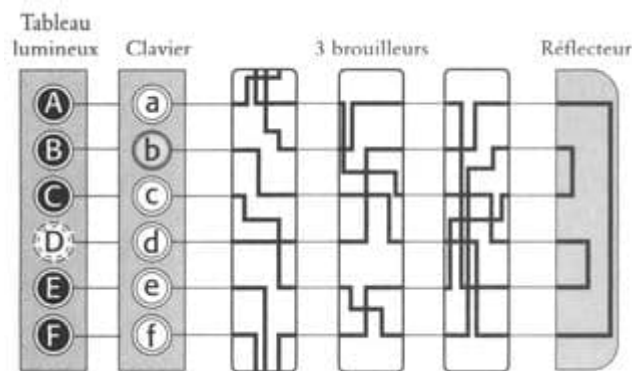


Fig. 36 Le projet de Scherbius incluait un troisième rotor dans l'Enigma, et un réflecteur qui faisait repasser le courant à travers les rotors. Dans la position montrée ici, taper *b* allume D sur le tableau lumineux, montré ici à côté du clavier.

Imaginons qu'un opérateur souhaite envoyer un message secret. Avant de commencer le cryptage, l'opérateur doit d'abord faire tourner les rotors jusqu'à la position de départ voulue. Il y a 17 576 dispositions possibles au départ. Le positionnement initial des rotors déterminera le cryptage du message. Nous pouvons regarder la machine Enigma comme un système à chiffrer global, dont les réglages initiaux déterminent les modalités précises du cryptage. Autrement dit, ce sont eux qui

fournissent la clef. Ils sont souvent choisis suivant un carnet de codes, qui définit une clef par jour, et dont disposent toutes les personnes impliquées dans le réseau de communications.

Une fois les brouilleurs réglés conformément aux directives du carnet concernant cette journée, l'expéditeur peut commencer à crypter. Il tape la première lettre du message, regarde quelle lettre s'allume sur le tableau lumineux et note cette première lettre du texte chiffré. Ensuite, le premier rotor ayant avancé d'une place, il recommence pour la deuxième, et ainsi de suite. Lorsqu'il a obtenu le texte chiffré complet, il le passe à un opérateur radio qui le transmet au destinataire.

Pour déchiffrer le message, le destinataire a besoin d'une autre machine Enigma et d'un exemplaire du carnet de codes, qui porte les positions initiales des rotors pour ce jour-là. Il règle la machine conformément au carnet, tape le texte chiffré lettre après lettre, et l'écran lumineux indique la lettre claire qui correspond. En résumé, l'expéditeur tape le texte clair pour engendrer le texte chiffré et le destinataire tape le texte chiffré pour retrouver le texte clair : chiffrement et déchiffrement sont des processus identiques. La facilité du déchiffrement est due au réflecteur. Sur la [figure 36](#), nous voyons que si nous tapons *b* et suivons le circuit électrique nous revenons à D. De même, si nous tapons *d* et suivons le circuit, nous revenons à B. La machine crypte une lettre claire en une lettre chiffrée et, à condition qu'elle soit sur la même position, elle décrypte la même lettre chiffrée en la même lettre claire.

Ayant vu à quoi sert la clef d'Enigma, il est évident que la clef et le carnet de codes ne doivent pas tomber dans des mains ennemies. Même si l'ennemi s'emparait d'une machine Enigma, sans connaître la position initiale des réglages, il aurait bien du mal à décrypter un message intercepté. Sans le carnet de codes le cryptanalyste ennemi doit vérifier toutes les clefs possibles, soit 17 576. En désespoir de cause, le cryptanalyste mettra la machine dans une certaine position, essaiera de transcrire un bout de texte crypté, et regardera si le résultat a un sens. Probablement non, et il devra alors placer les rotors différemment et recommencer. S'il peut essayer une position par minute et travailler nuit et jour, il lui faudra environ deux semaines pour essayer toutes les possibilités. Ce n'est qu'un niveau moyen de sécurité, car si l'ennemi met une douzaine de personnes au travail, il ne lui faudra qu'une journée. Aussi Scherbius décida-t-il d'améliorer son invention en accroissant le nombre de positions initiales et, par conséquent, le nombre de clefs possibles.

Il aurait pu, pour ce faire, ajouter encore des rotors, puisque chaque rotor supplémentaire accroît le nombre de clefs d'un facteur 26. Il préféra apporter deux autres aménagements. D'abord, il rendit simplement les rotors mobiles et interchangeables. On pouvait ainsi passer le premier rotor en troisième position et le troisième en première. Il y a six différentes façons de placer les trois rotors, ce qui multiplie par six le nombre des clefs possibles.

La seconde innovation fut l'insertion d'un tableau de connexions à fiches entre le clavier et le premier brouilleur. Ce tableau permet à l'expéditeur de brancher des fils qui auront pour effet d'échanger certaines des lettres avant qu'elles pénètrent dans le rotor. Par exemple, un fil peut être branché pour connecter les prises *a* et *b* du tableau afin que, lorsque le cryptographe veut crypter la lettre *b*, le signal électrique suive en fait le circuit prévu pour la lettre *a* et vice-versa. L'opérateur de l'Enigma disposait de six fils, ce qui signifiait que six fois deux lettres pouvaient être appariées, laissant quatorze lettres sans branchement. La [figure 37](#) montre l'agencement de la machine avec son tableau de connexions. Comme le diagramme n'est établi que pour un alphabet de six lettres, deux lettres seulement, *a* et *b*, sont appariées.

Il y a un autre élément dans le système de Scherbius, appelé la bague, que nous n'avons pas encore mentionné. La bague joue un certain rôle dans le cryptage, mais c'est le moins important dans la machine Enigma, et j'ai décidé de l'oublier pour simplifier les explications. (Pour les lecteurs qui voudraient connaître son rôle exact, je les renvoie à certains des livres figurant dans la liste de lectures annexes, notamment *Seizing the Enigma* de David Kahn.)

Maintenant que nous connaissons les principaux éléments d'Enigma, nous pouvons calculer le nombre de ses clefs potentielles, qui dépend des raccordements au tableau de connexions et des placements et dispositions des brouilleurs. La liste ci-dessous établit les variables pour la machine, et le nombre correspondant de possibilités pour chaque élément.

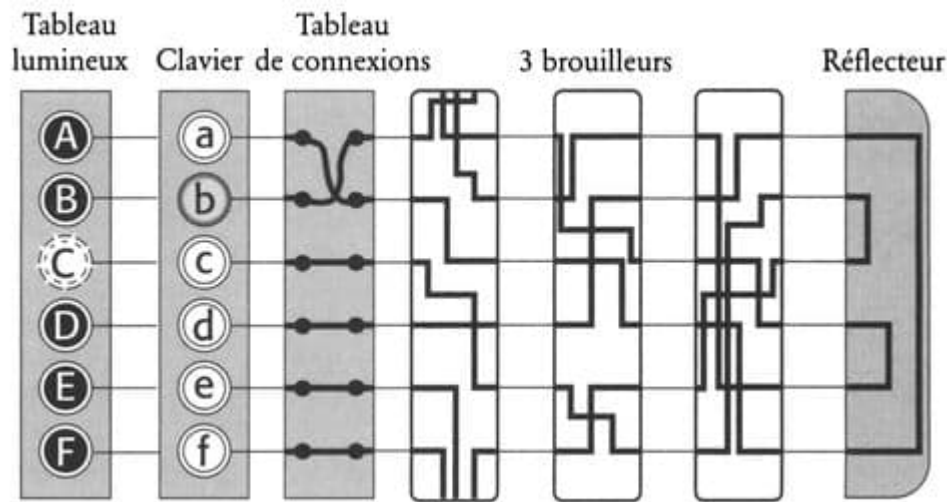


Fig.37 Le tableau de connexions est placé entre le clavier et le premier rotor. En y insérant des fiches, on peut lier deux lettres entre elles comme, dans ce cas-ci, b avec a. Maintenant, le courant qui crypte b suit le parcours prévu pour crypter a. Dans la véritable Enigma de 26 lettres, l'utilisateur disposait d'au moins 6 câbles pour relier au moins 6 paires de lettres.

Orientation des brouilleurs

Chacun des rotors peut être réglé sur 1 des 26 positions.

Il y a donc $26 \times 26 \times 26$ dispositions :

17 576

Disposition des brouilleurs

Les trois rotors (1,2,3) peuvent être placés selon les 6 dispositions suivantes : 123, 132, 213, 231, 312, 321 :

6

Tableau de connexions à fiches

Le nombre de branchements possibles en appariant 6 fois 2 lettres prises parmi les 26 de l'alphabet est énorme : $\simeq$

100 391 791 500

D'où le nombre total de clefs, produit de ces trois facteurs :

Nombre de clefs = $17\,576 \times 6 \times 100\,391\,791\,500$

$\simeq 10\,000\,000\,000\,000\,000$

Pour autant que l'expéditeur et le destinataire se soient entendus sur tous les éléments de la clef, c'est-à-dire les connexions, l'orientation de départ des rotors et l'ordre de leur disposition, ils peuvent crypter et décrypter les messages facilement. On a vu ci-dessus le nombre de clefs possibles parmi lesquelles un intercepteur ennemi devrait chercher celle pour déchiffrer le texte. Et j'ai ignoré dans ces calculs l'effet de la bague, qui augmente encore le nombre et donc le temps de déchiffrement.

Ce sont de loin les connexions du tableau qui ont la plus forte incidence sur le nombre possible de clefs, aussi peut-on se demander pourquoi Scherbius se donna tant de peine sur les rotors. Par lui-même, le tableau de connexions ne constituerait qu'un chiffre banal, puisqu'il n'effectue qu'une simple substitution de lettres, portant sur 12 lettres. Les appariements de lettres ne changent pas au cours du chiffrement, et le texte chiffré engendré serait facile à briser par l'analyse de fréquence. La manipulation des brouilleurs apporte un plus petit facteur multiplicatif mais, en tournant continuellement, elle rend le texte chiffré sans prises pour l'analyse de fréquences. En combinant le tableau et les rotors, Scherbius décourageait toute tentative d'analyse de fréquences et, en même temps, donnait à la machine un nombre considérable de clefs potentielles.

Scherbius fit breveter son invention en 1918. Sa machine à chiffrer se présentait comme une boîte mesurant seulement 34 cm x 28 cm x 15 cm, mais pesait une bonne douzaine de kilos. La [figure 39](#) montre une machine Enigma prête à l'emploi. On voit le clavier sur lequel sont tapées les lettres du texte clair et, au-dessus, l'écran qui affiche les lettres du texte chiffré qui en découle. Au-dessous de l'écran est le tableau de connexions. Il y a plus de douze lettres appariées, parce que la machine Enigma représentée ici est une version plus tardive que celle décrite plus haut. Sur la [figure 40](#), le couvercle est enlevé pour montrer l'intérieur, en particulier les trois rotors.

Scherbius pensait qu'Enigma était imprenable, et qu'on aurait de plus en plus recours à ses qualités cryptographiques. Il essaya de commercialiser sa machine auprès de l'armée comme des milieux d'affaires, leur proposant différentes versions. Il offrait ainsi une version basique aux commerciaux, alors qu'il réservait une version diplomatique de luxe pour les Affaires étrangères, avec une imprimante à la place du

tableau lumineux. Le prix d'un exemplaire s'élevait à 20 000 livres en valeur actuelle, mais Scherbius consentait un rabais de 3 000 livres si on en commandait mille exemplaires.



Fig. 38 Arthur Scherbius.



[Fig. 39](#) Machine Enigma de l'armée prête à servir.



Fig. 40 Machine Enigma de l'armée avec son couvercle intérieur relevé, découvrant les trois rotors.

Le prix de la machine sembla décourager les acheteurs potentiels. Les industriels affirmaient qu'ils n'avaient pas les moyens de s'offrir la sécurité d'Enigma, quand Scherbius prétendait, lui, qu'ils n'avaient pas les moyens de s'en passer, faisant valoir qu'un message vital intercepté par une entreprise concurrente pouvait coûter une fortune à une société, mais il ne rencontra pas beaucoup d'écho. L'armée allemande n'était pas plus motivée, ayant apparemment oublié les dommages causés par la faiblesse de son chiffre pendant la Grande Guerre. Ils préféraient croire que le télégramme de Zimmermann avait été dérobé par des agents

américains à Mexico, pour faire porter à la sécurité mexicaine la responsabilité de cette fuite. Ils n'avaient toujours pas admis l'interception du télégramme par les Britanniques, ni la responsabilité de la cryptographie allemande dans cette catastrophe.

Pour Scherbius, la déception était grande, et il n'était pas seul dans son cas. Trois autres inventeurs, dans trois autres pays, avaient, chacun de son côté et presque simultanément, eu l'idée d'une machine basée sur les rotors. Aux Pays-Bas, en 1919, Alexander Koch prit le brevet n° 10 700, mais ne réussit pas à commercialiser sa machine, dont il finit par vendre les droits en 1927. En Suède, Arvid Damm prit un brevet similaire, mais à sa mort en 1927 il n'avait toujours pas trouvé de marché. En Amérique, Edward Hebern avait une foi totale dans son invention, baptisée *Le Sphinx du sans-fil*, mais son échec fut le plus cuisant de tous.

Hebern construisit une usine de 380 000 dollars, juste au moment où la mentalité changeait en Amérique. Immédiatement après la Première Guerre mondiale, les Américains avaient créé le cabinet noir américain, un bureau du chiffre redoutablement efficace, rassemblant une vingtaine de cryptanalystes sous la houlette du flamboyant Herbert Yardley. « Le cabinet noir verrouillé, caché, gardé, voit tout, entend tout, écrivait Yardley. Même si les volets sont clos et si de lourds rideaux protègent les fenêtres, ses yeux perçants pénètrent au loin dans les salles de conférences secrètes de Washington, Tokyo, Londres, Paris, Genève, Rome. Ses oreilles particulièrement fines saisissent les murmures les plus faibles dans toutes les capitales du monde. » Le cabinet noir américain résolut 45 000 cryptogrammes en dix ans, mais au moment où Hebern construisait son usine, Herbert Hoover avait été élu président, et il souhaitait faire entrer le pays dans une ère nouvelle de clarté et de confiance. Il fit dissoudre le cabinet noir et son secrétaire d'État, Henry Stimson, déclara que des « gentlemen ne devaient pas lire le courrier les uns des autres ». Si un pays croit que c'est mal de lire les messages d'autrui, c'est qu'il s' imagine que les autres ne liront pas non plus ses propres messages. Il ne voit donc pas la nécessité d'inventer des machines à chiffrer. Hebern ne vendit que douze machines pour un prix total de 1 200 dollars, et en 1926 il fut poursuivi en justice par des actionnaires insatisfaits, et jugé coupable aux termes du *California's Corporate Securities Act*.

La chance tourna pour Scherbius le jour où l'armée allemande se vit contrainte de reconnaître la valeur de son Enigma, grâce à deux

documents britanniques. Le premier était un ouvrage de Winston Churchill, *The World Crisis*, publié en 1923, qui comportait un récit sur la manière dont les Anglais avaient eu accès à du matériel cryptographique allemand de première importance.

Au début de septembre 1914, le croiseur léger allemand Magdeburg fit naufrage dans la Baltique. Le corps de l'un des sous-officiers allemands fut repêché par les Russes quelques heures plus tard et, serrés contre sa poitrine par des bras rendus rigides par la mort, étaient le chiffre et le livre des signaux de l'armée allemande, et des cartes minutieusement quadrillées de la mer du Nord et de la baie d'Heligoland. Le 6 septembre, l'attaché naval russe vint me voir. Il avait reçu un message de Petrograd lui racontant ces faits, et que l'amirauté russe avait été capable, à l'aide du chiffre et du livre des signaux, de décoder au moins certaines parties des messages de la Kriegsmarine. Les Russes jugèrent que, en tant que première puissance navale, l'Amirauté britannique se devait d'avoir ces livres et ces relevés. Si nous pouvions envoyer un bateau à Alexandrov, les officiers russes responsables de ces documents les apporteraient en Angleterre.

Ces éléments avaient aidé les cryptanalystes du Bureau 40 à faire céder régulièrement les messages cryptés allemands. Les Allemands, eux, apprenaient cette faille dans la sécurité de leurs communications avec presque dix ans de retard. Toujours en 1923, la Royal Navy publia son histoire officielle de la Première Guerre mondiale, qui rappelait les avantages décisifs apportés aux Alliés par l'interception (et la cryptanalyse) des messages allemands. Ces prouesses du renseignement britannique constituaient une condamnation implicite pour la sécurité allemande, qui admit enfin que « le commandement de la flotte allemande, dont les messages radio étaient interceptés et déchiffrés par les Anglais, jouait pour ainsi dire cartes sur table, face au commandement anglais ».

Pour éviter la répétition d'un tel fiasco cryptographique, l'armée allemande mena une enquête qui conclut à la nécessité de s'équiper en Enigma. Dès 1925, Scherbius entreprit donc la production en série des

Enigma, qui entrèrent en service chez les militaires l'année suivante, et furent ensuite utilisées soit par le gouvernement, soit par des entreprises d'État, comme les chemins de fer. Ces Enigma différaient des quelques machines déjà vendues à des entreprises commerciales par des rotors équipés de câblages intérieurs renouvelés. Les propriétaires d'une machine Enigma commerciale ne pouvaient donc pas savoir comment étaient exactement conçues les versions militaires et gouvernementales.

Pendant les dix années qui suivirent, l'armée allemande se dota de plus de 30 000 machines Enigma. L'invention de Scherbius fournit à l'Allemagne le plus sûr système de cryptographie au monde, et au début de la Seconde Guerre mondiale, ses communications avaient atteint un niveau de cryptage sans concurrence. Il semblait alors que la machine Enigma jouerait un rôle déterminant dans la victoire nazie ; or, elle contribua à la chute d'Hitler. Scherbius ne vécut pas assez longtemps pour voir les succès et les échecs de son système de chiffrement. En 1929, alors qu'il menait un attelage de chevaux, il s'écrasa contre un mur, et mourut le 13 mai des suites de lésions internes.

À l'attaque d'Enigma

Dans les années qui suivirent la Première Guerre mondiale, les cryptanalystes britanniques continuèrent à contrôler les communications allemandes, mais en 1926 ils commencèrent à intercepter des messages qui les déroutèrent tout à fait. Enigma était entrée en action, et plus le nombre de machines Enigma augmentait, plus il devenait difficile pour le Bureau 40 de rassembler des renseignements. Les Américains et les Français essayèrent également de saisir le chiffre d'Enigma, mais leurs tentatives furent vaines, et ils abandonnèrent bientôt tout espoir d'y parvenir. L'Allemagne avait désormais le réseau de communications le plus sûr du monde.

La rapidité avec laquelle les cryptanalystes alliés renoncèrent à briser Enigma contrastait avec la persévérance qu'ils avaient déployée pendant la Première Guerre mondiale. Devant la perspective d'une défaite, les cryptanalystes alliés avaient travaillé nuit et jour pour percer les chiffres allemands. À croire que la peur est la meilleure motivation, et que l'adversité est une base nécessaire pour attaquer les codes avec succès. C'était déjà la peur qui avait galvanisé la cryptanalyse française à la fin du XIX^e siècle, lorsqu'elle était confrontée à la puissance de la Prusse. Quoi qu'il en soit, à l'issue de la Première Guerre mondiale, les Alliés ne craignaient plus personne. L'Allemagne avait été mise hors d'état de nuire, les Alliés étaient en position de domination, et leur zèle cryptanalytique s'en ressentait. Les cryptanalystes alliés voyaient fondre leurs effectifs, par ailleurs de moins en moins brillants.

Une nation, pourtant, ne pouvait se permettre pareil relâchement. Après la guerre, la Pologne était devenue un État indépendant, mais elle savait que ses voisins menaçaient sa souveraineté toute neuve. À l'est, la Russie souhaitait y instaurer un régime communiste, et à l'ouest l'Allemagne rêvait de reconquérir la Pologne qui avait fait partie de son territoire. Cernée de la sorte, la Pologne avait un besoin vital de renseignements, et elle créa un nouveau bureau du chiffre, le Biuro

Szyfrów. Si la nécessité est la mère de l'invention, peut-être l'angoisse est-elle la mère de la cryptanalyse. Le succès du Biuro Szyfrów est démontré par ses performances au cours de la guerre russo-polonaise de 1919-1920. Dans la seule année 1920, alors que les Soviétiques étaient aux portes de Varsovie, le Biuro déchiffra 400 messages ennemis. Son contrôle des communications allemandes resta à ce niveau d'efficacité jusqu'en 1926, date à laquelle il se trouva face aux messages Enigma.

Le capitaine Maksymilian Ciezki était responsable du déchiffrement des messages allemands. Ciezki était un patriote qui avait grandi dans la ville de Szamotuty, un des foyers du nationalisme polonais. Il avait eu accès à une version commerciale de la machine Enigma, ce qui lui permit de connaître les principes de l'invention de Scherbius. Mais la version commerciale différait de la version militaire par l'agencement des fils à l'intérieur de chaque tambour. Ciezki n'avait aucune chance de déchiffrer les messages envoyés par l'armée allemande sans connaître ces circuits. Il en était si conscient qu'en désespoir de cause, il alla jusqu'à employer un voyant extra-lucide pour découvrir le sens des cryptages interceptés. Il n'y eut pas de miracle, et le voyant n'effectua pas la percée dont le Biuro Szyfrów avait besoin. C'est un Allemand aigri et déçu, Hans-Thilo Schmidt, qui permit les premiers pas vers la résolution du chiffre d'Enigma.

Deuxième fils d'un professeur distingué et de son aristocratique épouse, Hans-Thilo Schmidt était né à Berlin en 1888. Il commença une carrière dans l'armée et combattit pendant la Première Guerre mondiale, mais il ne fut pas considéré comme suffisamment valable pour être maintenu dans les effectifs, après les réductions drastiques imposées par le traité de Versailles. Il tenta alors de se faire un nom dans les affaires, mais son usine de savon ayant été contrainte à la fermeture par la dépression de l'après-guerre et l'inflation, Schmidt se retrouva absolument démuní, avec une famille à charge.

Ses échecs lui étaient rendus encore plus pénibles par les succès de son frère aîné, Rudolph, lui aussi combattant de la Première Guerre, mais qui avait été gardé dans l'armée. Dans les années 20, Rudolph progressa et finit par être promu à la tête du Corps des signaux. Responsable de la sécurité des communications, ce fut lui qui imposa officiellement l'usage du chiffre Enigma dans l'armée.



[Fig. 41](#) Hans-Thilo Schmidt.

Après sa faillite, Hans-Thilo dut demander de l'aide à son frère, et Rudolf lui trouva un emploi à Berlin dans le *Chiffrierstelle*, le bureau chargé de gérer les communications cryptées allemandes. C'était le poste de commande d'Enigma, un établissement ultra-secret où l'on manipulait une information hautement sensible. Quand Hans-Thilo déménagea pour prendre ce nouveau poste, il laissa sa famille en Bavière, où le coût de la vie restait abordable. Lui-même vécut donc seul à Berlin, pauvre et isolé, jaloux de son frère, et animé d'un profond ressentiment envers une nation par laquelle il se sentait rejeté. Le résultat était prévisible. En vendant des informations secrètes sur Enigma à des puissances étrangères, Hans-Thilo Schmidt pouvait à la fois gagner de l'argent et se venger, en portant préjudice à la sécurité de son pays et en minant l'organisation dirigée par son frère.

Le 8 novembre 1931, Schmidt arriva au Grand Hôtel de Verviers, en Belgique, pour y rencontrer un agent secret français, dont le nom de code était Rex. En échange de 10 000 marks, Schmidt permit à Rex de photographier deux documents : *Gebruuchsanweisung für die Chiffriermaschine Enigma* et *Schlüsselanleitung für die Chiffriermaschine Enigma*. Ces documents portaient des instructions pour l'usage de la machine Enigma, et s'ils ne fournissaient pas une description explicite des branchements dans chaque rotor, ils contenaient suffisamment de précisions pour les déduire.

Grâce à la trahison de Schmidt, les Alliés pouvaient maintenant fabriquer une réplique exacte de la machine militaire Enigma. Cela ne suffisait pas, toutefois, pour déchiffrer les messages cryptés par Enigma. La force du chiffre ne dépendait pas tant du secret autour de la machine que du secret autour de sa disposition initiale (la clef). Si un cryptanalyste veut déchiffrer un message intercepté, il doit non seulement avoir une réplique de la machine Enigma, mais il lui reste encore à trouver, parmi les milliards de clefs possibles, celle qui a été utilisée pour le chiffrement. Un mémoire allemand résumait le génie d'Enigma : « Il est prévu que la sécurité du système de cryptage soit préservée même si l'ennemi a une machine à sa disposition. »

Les services secrets français étaient maintenant en position pour progresser, mais leurs cryptanalystes ne se montrèrent pas à la hauteur, et se révélèrent incapables d'exploiter les récentes informations. Le Bureau du chiffre ne se donna même pas la peine d'essayer de construire une machine Enigma, persuadé qu'il était de ne jamais réussir à trouver la clef.

Dix ans auparavant, les Français avaient signé un accord de coopération militaire avec les Polonais. Les Polonais avaient insisté pour être informés de tout ce qui concernait Enigma, et les Français communiquèrent donc simplement la photographie des documents de Schmidt à leur alliés, abandonnant au Biuro Szyfrów le soin de poursuivre la tâche jugée sans espoir. Le Biuro comprit que les documents ne lui donnaient qu'un point de départ mais, à l'inverse des Français, les Polonais sentaient sur eux la menace d'une invasion. Ils se persuadèrent qu'il devait y avoir un raccourci pour trouver la clef d'un message crypté par Enigma, et que, s'ils y apportaient suffisamment d'efforts, d'ingéniosité et de finesse, ils trouveraient ce raccourci.

En plus des câblages internes des rotors, les documents de Schmidt permettaient de saisir le fonctionnement des carnets de codes allemands.

Chaque mois, les opérateurs d'Enigma recevaient un nouveau carnet de codes, qui spécifiait lequel devait être utilisé pour chaque jour. Par exemple, le 1^{er} du mois, le carnet pouvait spécifier de suivre cette clef du jour :

1. *Branchements des connexions* : A/L-P/R-T/D-B/W-K/F-O/Y
2. *Réglage du brouilleur* : 2. 3. 1
3. *Orientation du brouilleur* : Q-C-W

Le réglage et l'orientation du brouilleur définissent ensemble son positionnement. Pour appliquer la clef en question, l'opérateur Enigma va positionner sa machine Enigma comme suit :

1. *Branchements des connexions* : Permuter les lettres A et L en les connectant par un câble sur le tableau, de même pour P et R, T et D, B et W, K et F, et enfin O et Y.

2. *Réglage du brouilleur* : Placer le deuxième rotor dans la première encoche de la machine, le troisième dans la deuxième encoche et le premier dans la troisième.

3. *Orientation du brouilleur* : Chaque rotor a un alphabet gravé sur son bord externe, qui permet à l'opérateur de l'orienter précisément. Ici l'opérateur tourne le rotor placé dans la première encoche de façon à faire apparaître la lettre Q au-dessus, tourne le rotor suivant pour que C soit au-dessus, et le dernier pour que W apparaisse au-dessus.

Une méthode serait que l'expéditeur crypte tous les envois d'une même journée selon le code du jour. Dans ce cas, au matin de chaque journée tous les opérateurs Enigma régleraient leurs machines en accord avec la clef du jour. Ensuite, chaque fois qu'on aurait à envoyer un message, on l'entrerait dans la machine et le résultat crypté qui en sortirait serait noté et remis à un opérateur radio pour la transmission. À l'autre bout, un autre opérateur radio recevrait le message, le passerait à un opérateur Enigma qui l'entrerait dans sa machine, déjà réglée sur le code du jour. Le message original en ressortirait.

Le procédé est à peu près sûr, mais il est affaibli par l'usage du même code pour crypter les centaines de messages envoyés un même jour. On peut admettre en général qu'une même clef utilisée pour crypter une grande quantité de texte offre au cryptanalyste plus de munitions pour identifier la clef. Si nous revenons aux chiffres simples, il est beaucoup plus facile de briser un chiffre monoalphabétique grâce à l'analyse des

fréquences si l'on dispose de plusieurs pages cryptées, plutôt que seulement de deux phrases.

Aussi les Allemands, par une précaution supplémentaire, prirent l'intelligente décision d'utiliser les réglages du jour pour transmettre un nouveau *message-clef* spécial pour chaque message. Les branchements des connexions et les réglages du brouilleur restaient conformes à la clef du jour, seule l'orientation du brouilleur était modifiée. Cette nouvelle orientation ne figurant pas dans le carnet de codes, l'expéditeur devait la transmettre de la manière suivante : d'abord, l'expéditeur règle sa machine selon la clef du jour, qui comporte une orientation, disons QCW. Ensuite, il choisit au hasard une nouvelle orientation pour les rotors, disons PGH. Il va maintenant chiffrer PGH selon la clef du jour. En fait le message-clef est tapé deux fois sur Enigma, afin que le destinataire ait un double contrôle. Par exemple, l'expéditeur peut chiffrer le message-clef PGHPGH en KIVBJE. Notez que les deux PGH sont chiffrés différemment (le premier en KIV, le second en BJE), ce qui découle de la rotation des rotors d'Enigma après chaque lettre, changeant le mode de cryptage général. L'expéditeur règle ensuite sa machine sur PGH et crypte le message principal selon le message-clef. Du côté du destinataire, la machine est initialement réglée selon la clef du jour, QCW. Les six premières lettres d'un message entrant, KIVBJE, ressortent sous la forme PGHPGH. Le destinataire réglera donc ses rotors sur PGH, le message-clef, et pourra ensuite déchiffrer le corps principal du message.

Cela équivaut à mettre au point entre les deux correspondants une clef de chiffrement générale. Mais au lieu d'utiliser cette même clé pour crypter tous les messages, on l'utilise seulement pour transmettre une nouvelle clef de chiffrement pour chaque message, et on crypte ensuite le vrai message selon la nouvelle clef.

Si les Allemands n'avaient pas utilisé de messages-clefs, ce sont des milliers de messages, contenant des millions de caractères, qui auraient été envoyés avec la même clef du jour. Alors que si la clef du jour ne sert qu'à transmettre le message-clef, elle ne crypte qu'une petite quantité de texte. S'il y a mille messages-clefs par jour, la clef du jour ne crypte que six mille lettres. Et, comme chaque message-clef est formé au hasard et ne s'applique au chiffrement que d'un seul message, il ne crypte qu'un texte limité, peut-être une petite centaine de caractères.

À première vue, ce système semblait imprenable, mais les cryptanalystes polonais ne se laissèrent pas impressionner. Ils avaient décidé d'explorer toutes les voies pour trouver un point faible dans la machine Enigma et son usage de clefs du jour et de messages-clefs. Au premier rang de la bataille apparaissait une nouvelle race de cryptanalystes. Depuis des siècles, on avait admis que les meilleurs cryptanalystes étaient des spécialistes des formes de construction de la langue, mais l'arrivée d'Enigma conduisit les Polonais à modifier leur politique de recrutement. Enigma était un chiffre mécanique et le Biuro pensa qu'un cerveau scientifique serait plus à même de le briser. Le Biuro organisa un cours de cryptographie et invita vingt mathématiciens, qui s'engagèrent au secret sous le sceau du serment. Tous appartenaient à l'université de Poznan, qui n'était pas l'institution la plus réputée de Pologne, mais qui bénéficiait de sa situation à l'ouest du pays, sur un territoire qui avait fait partie de l'Allemagne jusqu'en 1918. Tous ces mathématiciens parlaient donc couramment l'allemand.

Trois des vingt mathématiciens montrèrent une aptitude particulière pour résoudre des chiffres, et le Biuro les recruta. Le plus doué était Marian Rejewski, un timide jeune homme à lunettes de vingt-trois ans, qui avait étudié les statistiques car il se destinait à une carrière dans les assurances. Bien qu'il fût un bon étudiant à l'université, c'est au Biuro Szyfrów que se révéla sa véritable vocation. Il commença son apprentissage en brisant un certain nombre de chiffres traditionnels et fut ensuite lancé contre Enigma. Travaillant absolument seul, il concentra toutes ses facultés sur les dédales de la machine de Scherbius. En bon scientifique, il voulait analyser tous les aspects du fonctionnement de la machine, comprendre le rôle des rotors et des connexions. Mais les mathématiques requièrent de l'inspiration en plus de la logique. Un autre mathématicien cryptanalyste insistait sur ce côté inspiré de son travail lorsqu'il déclarait « être obligé de pactiser quotidiennement avec le diable pour gagner le combat dans ce jiu-jitsu mental ».

Rejewski développa sa stratégie autour du fait que la répétition est l'ennemie de la sécurité, puisqu'elle entraîne des schémas que les cryptanalystes peuvent exploiter. La répétition la plus évidente avec Enigma était celle du message-clef, qui était chiffré à deux reprises au début de chaque message. Si l'opérateur choisissait le message-clef ULJ, il cryptait ULJULJ, ce qui donnait PEFNWZ, et il envoyait cette suite en tête de son message. Les Allemands avaient imposé le doublement pour éviter des erreurs dues à des interférences radio ou à une faute de

l'opérateur, ils n'avaient pas pensé que cela portait atteinte à la sûreté de la machine.

Chaque jour Rejewski se trouvait devant une nouvelle moisson de messages interceptés, qui commençaient tous par les six lettres du message-clef de trois lettres répété deux fois, en suivant la même clef du jour. Ainsi, il pouvait recevoir quatre messages qui commençaient par les messages-clefs suivants :

	1 ^{re}	2 ^e	3 ^e	4 ^e	5 ^e	6 ^e	
1 ^{er} message	L	O	K	R	G	M	...
2 ^e message	M	V	T	X	Z	E	...
3 ^e message	J	K	T	M	P	E	...
4 ^e message	D	V	Y	P	Z	X	...



Fig. 42 Marian Rejewski.

Dans chaque cas, la 1^{re} et la 4^e lettres sont deux chiffrements de la même lettre, la première du message-clef. De même, la 2^e et la 5^e sont des cryptages de la même lettre, à savoir la deuxième du message-clef, et la 3^e et la 6^e sont des cryptages de la même lettre, à savoir la troisième lettre du message-clef. Dans le premier message *L* et *R* sont des cryptages de la même lettre, la première lettre du message-clef. Cette lettre est cryptée différemment, une fois *L* et une fois *R*, puisque, entre ces deux cryptages, le rotor a avancé de trois places, changeant à chaque fois l'ensemble du brouillage.

Le fait que L et R soient des cryptages de la même lettre permet à Rejewski de déduire une indication sur le positionnement initial de la machine. La position du brouilleur, qui est inconnue, décidait du cryptage de la première lettre de la clef du jour, elle aussi inconnue, en L , et ensuite un autre positionnement, trois places après la position initiale toujours inconnue, cryptait la même lettre de la clef du jour en R .

Ce développement peut sembler vague, car plein d'inconnues, mais au moins il démontrait que les lettres L et R étaient étroitement liées dans la position initiale de la machine Enigma, la clef du jour. À chaque nouveau message intercepté, on peut identifier d'autres liens entre la 1^{re} et la 4^e lettres du message-clef répété, et tous ces liens sont des indications sur le positionnement initial de la machine Enigma. Le deuxième message, par exemple, nous montre une relation entre M et X , le troisième entre J et M , et le quatrième entre D et P . Rejewski commença par relever toutes ces relations sur un tableau. Pour les quatre messages que nous avons vu jusqu'ici, le tableau va refléter les relations entre (L,R) , (M,X) , (J,M) et (D,P) :

1 ^{re} lettre	ABCDEF GHI J KLMNOPQRST UVWXYZ
4 ^e lettre	P M RX

Si Rejewski avait accès à suffisamment de messages le même jour, il pouvait compléter l'alphabet des relations. Le tableau suivant établit la liste complète de ces relations.

1 ^{re} lettre	ABCDEF GHI J KLMNOPQRST UVWXYZ
4 ^e lettre	FQHP LWOGBMVRXUYCZ I TNJ EASDK

Rejewski n'avait aucune idée de la clef du jour, et il n'avait aucune idée des messages-clefs choisis, mais il savait que ce tableau des relations en découlait. Si la clef du jour avait été différente, ce tableau aurait lui aussi été entièrement différent. La question suivante était : Y a-t-il un quelconque moyen de déterminer la clef du jour en se fondant sur le tableau des relations ? Rejewski commença à chercher des modèles dans le tableau, des constructions qui pourraient indiquer la clef du jour. En fin de compte, il commença à se pencher sur un certain modèle qui impliquait des chaînes de lettres. Dans le tableau ci-dessus, le A de la rangée supérieure est lié au F de la rangée du bas, aussi se reporta-t-il ensuite au F de la rangée supérieure. Ce F était lié au W, aussi

chercha-t-il le W sur la rangée supérieure. Ce W était lié avec A, la lettre avec laquelle il avait commencé. La chaîne était bouclée.

Avec les autres lettres de l'alphabet, Rejewski généra d'autres chaînes. Il les nota toutes, ainsi que le nombre de liens pour chacune d'entre elles :

A → F → W → A	3liens
B → Q → Z → K → V → E → L → R → I → B	9liens
C → H → G → O → Y → D → P → C	7liens
J → M → X → S → T → N → U → J	7liens

Jusqu'ici, nous n'avons considéré que les liens entre la 1^{re} et la 4^e lettres des six lettres formant la clef répétée. Rejewski, lui, répéta cet exercice pour les relations entre la 2^e et la 5^e lettres et la 3^e et la 6^e, établissant les chaînes dans chaque cas, et le nombre de liens dans chaque chaîne.

Il nota que les chaînes changeaient chaque jour. Parfois, il y avait des séries de chaînes courtes, parfois juste quelques longues chaînes, et, bien sûr, les lettres à l'intérieur des chaînes étaient issues du positionnement de la clef du jour, une conséquence complexe des connexions du tableau, des réglages du rotor et de son orientation. Mais comment déduire de ces chaînes la clef du jour ?

C'est alors que Rejewski eut une inspiration. Bien que le tableau de connexions et le brouilleur influent tous deux sur la composition des chaînes, leurs contributions pouvaient jusqu'à un certain point être démêlées. Il y a en particulier un aspect de la chaîne qui dépend entièrement des règles du brouilleur, et qui ne doit rien aux branchements des connexions : le nombre des liens dans les chaînes ne découle que des ajustements du brouilleur. Prenons l'exemple donné plus haut et décidons que la clef du jour requiert que les lettres S et G soient liées par une connexion. Si nous changeons cet élément de la clef du jour, en enlevant le câble qui relie S et G, et que nous l'utilisons pour permuter respectivement T et K, les chaînes subiront la transformation qui suit :

A → F → W → A	3liens
B → Q → Z → T → V → E → L → R → I → B	9liens
C → H → S → O → Y → D → P → C	7liens
J → M → X → G → K → N → U → J	7liens

Certaines des lettres ont changé dans les chaînes, mais le nombre de liens dans chaque chaîne est resté constant. Rejewski a donc repéré une propriété des chaînes ne dépendant que des réglages du brouilleur.

Le nombre total des positions du brouilleur est constitué par le nombre des dispositions possibles des rotors (6) multiplié par le nombre des orientations possibles des rotors (17 576) ce qui le porte à 105 456. Au lieu de se demander laquelle des 10 000 000 000 000 000 clefs du jour possibles était associée à un ensemble de chaînes donné, Rejewski pouvait donc se confronter à un problème plus simple : laquelle des 105 456 dispositions du brouilleur correspondait à un ensemble de chaînes donné. Le nombre est encore élevé, mais il est environ cent milliards de fois plus petit que le nombre total possible de clefs du jour. La tâche s'en trouvait facilitée, et devenait humainement possible.

Rejewski procéda comme suit. Grâce aux renseignements de Hans-Thilo Schmidt, il avait accès à une réplique de la machine Enigma. Son équipe commença la besogne laborieuse de vérifier les 105 456 dispositions, et de répertorier les longueurs de chaînes qu'engendrait chacune. Cela prit un an pour terminer ce répertoire, mais lorsque le Biuro eut connaissance de toutes les données, il fut finalement en mesure de révéler le chiffre d'Enigma.

Chaque jour, Rejewski notait les messages-clefs cryptés, les six premières lettres de tous les messages interceptés et il utilisait cette information pour dresser son tableau des relations. Cela lui permettait de faire le relevé des chaînes, et de déterminer le nombre de liens dans chaque chaîne. Par exemple, analyser la 1^{re} et la 4^e lettres peut donner 4 chaînes avec 3, 9, 7 et 7 liens dans chacune. Analyser la 2^e et la 5^e lettres peut aussi donner 4 chaînes avec 2, 3, 9 et 12 liens. Analyser la 3^e et la 6^e lettres peut donner 5 chaînes avec 5, 5, 5, 3 et 8 liens. Jusque-là, Rejewski n'avait toujours pas idée de la clef du jour, mais il savait qu'elle engendrait 13 chaînes avec les nombres suivants de liens entre elles :

4 chaînes de la 1^{re} et de la 4^e lettres, avec 3, 9, 7 et 7 liens
4 chaînes de la 2^e et de la 5^e lettres, avec 2, 3, 9 et 12 liens
5 chaînes de la 3^e et de la 6^e lettres, avec 5, 5, 5, 3 et 8 liens

Rejewski pouvait maintenant se reporter à son répertoire, qui contenait toutes les dispositions du brouilleur indexées suivant les sortes de chaînes qu'elles génèrent. En trouvant dans le répertoire l'entrée qui

commandait le juste nombre de chaînes avec le nombre approprié de liens pour chacune, il savait immédiatement quelles étaient les dispositions du brouilleur pour cette clef du jour particulière. Les chaînes jouaient le rôle d'empreintes digitales, elles trahissaient l'agencement original du brouilleur et ses orientations. Rejewski avait travaillé comme un détective qui relève une empreinte sur le lieu du crime, et la confronte ensuite à un fichier afin de l'attribuer à un suspect.

S'il avait déterminé le rôle du brouilleur dans la clef du jour, Rejewski devait encore établir les connexions du tableau. Il commença par régler les rotors de sa copie d'Enigma selon la disposition récemment définie par la clef du jour. Il débrancha ensuite complètement les fiches du tableau. Puis il prit un texte chiffré et l'entra dans la machine Enigma. Ceci eut pour résultat un fouillis de lettres, puisqu'il manquait les connexions du tableau. Pourtant, assez souvent, des bouts de phrases semblaient presque identifiables comme « alliveenbelrin », qui pouvait être « arrive en Berlin ». Si cette supposition était juste, on pourrait déduire que les lettres R et L doivent être connectées et permutées par un fil du tableau, alors que A, I, V, E, B, et N ne doivent pas l'être. En analysant d'autres phrases, on parviendra à identifier les cinq autres paires de lettres qui ont été liées sur le tableau. Rejewski avait maintenant la clef du jour complète, et pouvait par conséquent déchiffrer n'importe quel message envoyé ce jour-là, crypté avec la même clef.

Rejewski avait beaucoup facilité la découverte de la clef du jour en scindant la recherche des dispositions du brouilleur de celle des connexions du tableau. Chacun de ces problèmes était plus abordable si on le traitait séparément. Nous avons estimé que la durée de vie de l'univers serait nécessaire pour essayer toutes les clefs d'Enigma. Rejewski, lui, n'avait eu besoin que d'une année pour dresser son répertoire des longueurs de chaînes, et il réussit ensuite à trouver la clef du jour avant qu'une journée soit écoulée. Dès l'instant qu'il avait cette clef, il en savait autant que le destinataire désigné, et il pouvait tout aussi bien que lui déchiffrer le message.

Les travaux de Rejewski avaient rendu les communications allemandes transparentes. Si les Polonais pouvaient savoir ce que les généraux allemands avaient en tête, ils avaient une chance de pouvoir se défendre. Le destin de la Pologne dépendait de Rejewski, et il ne déçut pas les espoirs de son pays.

L'assaut de Rejewski sur Enigma est véritablement l'une des plus importantes réalisations de la cryptanalyse. Pour résumer son travail en

quelques pages, j'ai dû omettre de nombreux détails techniques et faire bien des impasses. Enigma est une machine à chiffrer élaborée, et la briser exigeait une extraordinaire puissance intellectuelle. Mes simplifications ne doivent pas amener le lecteur à sous-estimer l'incroyable performance de Rejewski.

On pouvait attribuer ce succès polonais à trois facteurs : la menace, les mathématiques et l'espionnage. Sans la crainte d'une invasion, les Polonais auraient pu être découragés par l'apparente invulnérabilité du chiffre. L'analyse des chaînes par Rejewski était une application des mathématiques qu'il avait étudiées à l'université. Mais sans Schmidt (sous son nom de code de « Asche ») et ses documents, on n'aurait pas connu les câblages des rotors et la cryptanalyse n'aurait eu aucune base d'où partir. Rejewski ne cacha pas ce qu'il devait à Schmidt : « Les documents de Asche furent reçus comme une bénédiction du ciel, et toutes les portes s'ouvrirent immédiatement. »

Les Polonais utilisèrent la technique de Rejewski pendant plusieurs années. Quand Hermann Göring se rendit à Varsovie en 1934, il était loin de se douter que ses communications étaient interceptées et déchiffrées. Alors qu'il déposait, en compagnie d'autres dignitaires allemands, une couronne sur la tombe du Soldat inconnu près du Bureau Szyfrów, il était sous les yeux de Rejewski qui le regardait de sa fenêtre, jubilant à l'idée qu'il lisait ses correspondances les plus secrètes.

Lorsque les Allemands apportèrent une légère modification dans leur méthode de transmission, Rejewski repartit au combat. Son vieux répertoire des longueurs de boucles devenait périmé, mais plutôt que l'écrire à nouveau, il conçut une version mécanisée du système de répertoire, qui pouvait rechercher automatiquement les réglages exacts du brouilleur. L'invention de Rejewski était une adaptation de la machine Enigma, qui était capable de vérifier rapidement les 17 546 possibilités afin de sortir celle qui convenait. En raison des six placements des rotors possibles, il fallait faire travailler en parallèle six machines de Rejewski, chacune fondée sur l'un des arrangements. Tout ce matériel réuni formait un engin d'environ un mètre de haut, capable de trouver la clef du jour en deux heures environ. Ces équipements furent baptisés *bombes*, peut-être à cause du bruit qu'elles émettaient en exécutant leurs recherches. On dit aussi que Rejewski eut l'idée de ces machines alors qu'il se trouvait dans un café en train de manger une bombe glacée. Quoi qu'il en soit, ses bombes mécanisèrent le processus de déchiffrement. C'était une

réponse naturelle à Enigma, qui avait constitué une mécanisation du chiffrement.

Pendant une bonne partie des années 30, Rejewski et ses collègues travaillèrent sans répit à la recherche des clefs d'Enigma. Mois après mois, l'équipe dut réparer les défaillances des bombes, et traiter un flot ininterrompu de cryptages interceptés. Leurs vies étaient consacrées à la poursuite de la clef du jour. Ce qu'ignoraient les briseurs de codes polonais, c'est que le directeur du Biuro, le major Gwido Langer, avait déjà les clefs du jour d'Enigma qu'il tenait bien cachées dans un tiroir de son bureau.

En effet, Langer, par l'intermédiaire des Français, continuait à recevoir des renseignements de Schmidt. Les activités de l'espion allemand ne s'étaient pas arrêtées en 1931 avec la remise des deux documents sur Enigma, elles se prolongèrent pendant les sept années suivantes. Il rencontra à vingt reprises l'agent secret français Rex, le plus souvent dans des chalets alpins retirés. À chaque entrevue, Schmidt remettait un ou plusieurs carnets de code, contenant chacun les clefs du jour pour un mois, ceux-là même qui étaient distribués à tous les opérateurs allemands sur Enigma, et qui contenaient l'information requise pour chiffrer et déchiffrer les messages. Schmidt fournit au total des carnets de code qui portaient trente-huit mois de clefs du jour. Ces clefs auraient épargné à Rejewski un énorme travail et beaucoup de temps, évitant l'élaboration des bombes et libérant une main-d'œuvre qui aurait trouvé à s'employer utilement dans d'autres sections du Biuro. Mais Langer jugea plus habile de ne pas révéler à Rejewski l'existence des clefs, afin de le préparer pour l'époque inévitable où elles seraient indisponibles. Si la guerre éclatait, il deviendrait impossible pour Schmidt de poursuivre ses rencontres discrètes, et Rejewski aurait à se débrouiller par lui-même. Langer décida donc que Rejewski devait acquérir cette autonomie le plus tôt possible, en prévision de ce qui l'attendait.

Les capacités de Rejewski trouvèrent leur limite lorsqu'en décembre 1938 les Allemands renforcèrent la sécurité d'Enigma. On distribua à tous les opérateurs deux nouveaux rotors, afin que l'agencement du brouilleur s'effectue avec trois des rotors, n'importe lesquels parmi les cinq maintenant disponibles. Auparavant, il n'y avait que trois rotors (numérotés 1, 2 et 3) entre lesquels choisir, et donc 6 manières de les disposer, mais avec deux rotors de plus (numérotés 4 et 5), le nombre des agencements possibles passait à 60, comme on le voit sur le [tableau 10](#).

Agencements avec 3 rotors	Agencements supplémentaires avec 2 rotors de plus								
123	124	125	134	135	142	143	145	152	153
132	154	214	215	234	235	241	243	245	251
213	253	254	314	315	324	325	341	342	345
231	351	352	354	412	413	415	421	423	425
312	431	432	435	451	452	453	512	513	514
321	521	523	524	531	532	534	541	542	543

Tableau 10 Agencements possibles avec cinq rotors.

Le nouvel objectif de Rejewski était de reconstituer les câblages intérieurs des deux nouveaux rotors. Du coup, il devait aussi construire dix fois plus de bombes, chacune représentant un agencement différent du brouilleur. Le simple coût de la construction de cette batterie de bombes représentait quinze fois le budget total d'équipement du Biuro. La situation s'aggrava encore le mois suivant, lorsque les connexions sur le tableau passèrent de six à dix. Au lieu de douze lettres appariées avant d'entrer dans les rotors, il y en avait maintenant vingt. Le nombre de clefs possibles s'était élevé à 159 milliards de milliards.

En 1938, les interceptions et les déchiffrements par les Polonais atteignirent leur niveau record, mais au début de 1939, ces perfectionnements tarirent le flot des renseignements. Rejewski, qui avait repoussé les limites de la cryptanalyse les années précédentes, était dépassé. Il avait prouvé qu'Enigma n'était pas un chiffre infracturable, mais sans les éléments nécessaires pour établir toutes les mises au point du brouilleur, il ne pouvait pas trouver la clef du jour, et le déchiffrement restait impossible. Dans ces circonstances désespérées, Langer aurait bien délivré les clefs obtenues par Schmidt, mais il n'en avait plus. Juste avant l'introduction des nouveaux rotors, Schmidt avait rompu le contact avec Rex. Pendant sept ans, il avait fourni des clefs dont les Polonais avaient pu se passer grâce à leur inventivité, et maintenant qu'ils en avaient un besoin dramatique, ils ne pouvaient plus se les procurer.

La nouvelle invulnérabilité d'Enigma portait un coup terrible à la Pologne, car Enigma n'était pas seulement un mode de communications, elle était au cœur de la stratégie du *blitzkrieg* d'Hitler. Le concept de *blitzkrieg* (guerre-éclair) était celui d'une attaque rapide, intense et coordonnée, et impliquait que les divisions blindées puissent communiquer entre elles, ainsi qu'avec l'infanterie et l'artillerie. De plus, les forces terrestres étaient appuyées par des bombardiers Stukas, ce qui exigeait une communication efficace et sûre entre les troupes du front et les terrains d'aviation. La force du *blitzkrieg* était dans *la rapidité de l'attaque grâce à la rapidité des transmissions*.

Si les Polonais ne pouvaient faire céder Enigma, il n'avaient aucune chance d'arrêter l'invasion allemande, qui semblait maintenant une affaire de mois. L'Allemagne occupait déjà les Sudètes quand, le 27 avril 1939, elle dénonça son pacte de non-agression avec la Pologne, et la rhétorique anti-polonaise se fit de plus en plus virulente. Langer voulait que ses avancées cryptanalytiques, tenues jusque-là cachées aux Alliés, ne fussent pas perdues en cas d'invasion de la Pologne. Si la Pologne ne pouvait bénéficier du travail de Rejewski, au moins les Alliés auraient la possibilité de l'utiliser et de le développer. Peut-être la Grande-Bretagne et la France, disposant de plus grands moyens, pourraient-elles exploiter à fond son concept de « bombe cryptanalytique ».

Le 30 juin, le major Langer télégraphia donc à ses homologues français et britannique, les invitant à le rejoindre à Varsovie pour discuter de sujets urgents concernant Enigma. Le 24 juillet, des cryptanalystes français et anglais arrivaient au quartier général du Biuro, ignorant ce qui les attendait. Langer les entraîna dans une pièce où se dressait un objet recouvert d'un drap noir. Il arracha le drap, révélant par cette mise en scène l'une des bombes de Rejewski.

L'auditoire fut stupéfait d'apprendre comment Rejewski avait brisé le chiffre d'Enigma. Les Polonais avaient dix ans d'avance sur n'importe qui dans le monde. Les Français étaient vaguement au courant, parce que le travail des Polonais avait été fondé sur les résultats de l'espionnage français. Ils avaient fourni les informations de Schmidt parce qu'ils les croyaient sans valeur, et les Polonais étaient en train de les détromper.

Comme surprise finale, Langer offrit aux Britanniques et aux Français deux répliques disponibles d'Enigma et les plans des bombes, qui seraient acheminés vers Paris par la valise diplomatique. Puis, le 19 août,

l'une des machines Enigma était acheminée vers Londres. Elle traversa la Manche dans les bagages de l'auteur dramatique Sacha Guitry et de son épouse, l'actrice Yvonne Printemps, afin de ne pas éveiller de soupçons chez les espions allemands qui surveillaient les ports. Deux semaines plus tard, le 1^{er} septembre, Hitler envahissait la Pologne.

Les oies qui ne cacardent jamais.

Pendant treize ans, Britanniques et Français avaient tenu pour acquis qu'Enigma était intouchable, et voilà que l'espoir renaissait. Les révélations polonaises avaient fait apparaître des failles dans le chiffrement, ce qui remonta le moral des cryptanalystes alliés. Certes, les avancées polonaises avaient été contrées par les nouveaux rotors et les connexions supplémentaires, mais Enigma n'était plus tenu pour un chiffre parfait.



Fig. 43 Véhicule de commandement du général Heinz Guderian. On peut voir en bas à gauche une machine Enigma en action.

Le chemin parcouru par les Polonais montrait aussi aux Alliés l'intérêt d'utiliser des mathématiciens comme décrypteurs. En Angleterre, le Bureau 40 était jusque-là dominé par des linguistes et des littéraires, mais on s'efforça dès lors d'équilibrer les compétences en recrutant des mathématiciens et des scientifiques. Cela se fit à travers le réseau *old-boy* (les anciens), dont certains membres, appartenant déjà au Bureau, contactèrent leurs anciens collèges d'Oxford et de Cambridge. Il y avait également un réseau d'anciennes qui recruta des étudiantes du Newnham College et du Girton College de Cambridge.

Les nouvelles recrues ne furent pas intégrées au Bureau 40 à Londres, mais allèrent à Bletchley Park, dans le Buckinghamshire, siège de la *Government Code and Cypher School* (GC&CS), l'École du code et du chiffre, une structure récemment créée et qui dépendait du Bureau 40. Bletchley Park pouvait accueillir beaucoup plus de monde, ce qui semblait important devant le déluge prévisible d'interceptions cryptées qui suivrait immédiatement le début des hostilités. Pendant la Première Guerre mondiale, l'Allemagne avait transmis deux millions de mots par mois, on pouvait s'attendre, avec la prolifération des radios, à une transmission de deux millions de mots par jour.

Au centre de Bletchley Park s'élevait un grand manoir victorien de style gothique-Tudor, construit au XIX^e siècle par le financier sir Herbert Leon. Le manoir, avec sa bibliothèque, sa grande salle à manger et sa salle de bal très ornementée, abritait l'administration centrale de toute l'opération Bletchley. Le commandant Alastair Denniston, directeur de la GC&CS, avait un bureau au rez-de-chaussée donnant sur les jardins, une vue qui fut bientôt gâchée par l'érection de nombreuses *Huttes*. Dans ces constructions de fortune en bois furent logées les différentes activités nécessaires à l'attaque des codes. La Hutte 6, par exemple, était spécialisée dans les communications de l'armée allemande sur Enigma. La Hutte 6 passait ses textes décryptés à la Hutte 3, où un service de renseignements traduisait les messages, rassemblait l'information et essayait de l'exploiter. La Hutte 8 se consacrait à l'Enigma navale et passait ses messages décryptés à la Hutte 4 pour la traduction et la réunion des informations. Au départ, Bletchley Park rassembla une équipe de deux cents personnes, mais au bout de cinq ans, le manoir et les huttes finirent par abriter sept mille hommes et femmes.



Fig. 44 En août 1939, les responsables des services de décryptage visitèrent Bletchley Park pour juger si le lieu était adapté à l'installation de la nouvelle Code & Cipher School. Pour ne pas éveiller de soupçons dans la région, ils prétendirent participer à une chasse organisée par le capitaine Ridley.

Pendant l'automne 1939, les scientifiques et les mathématiciens se familiarisèrent avec la complexité du chiffre Enigma, et ils maîtrisèrent rapidement les méthodes polonaises. Bletchley disposait de plus de personnel et de ressources que le Biuro Szyfrów polonais, c'est-à-dire qu'on pouvait s'y attaquer au nombre accru de rotors et au fait qu'Enigma était maintenant dix fois plus difficile à percer. Tous les jours, les décrypteurs anglais accomplissaient le même travail routinier. À minuit, les opérateurs allemands sur Enigma réglaient la machine sur un nouveau code du jour, ce qui ruinait tout ce que Bletchley avait réussi à effectuer la veille. Il fallait recommencer en identifiant d'abord le nouveau code. Cela pouvait prendre plusieurs heures, mais dès que les réglages du jour avaient été trouvés, l'équipe de Bletchley pouvait commencer à déchiffrer les messages allemands qui s'étaient déjà accumulés, et en tirer des informations capitales pour la conduite de la guerre.

La surprise est une arme sans prix pour un commandement. Si Bletchley pouvait pénétrer Enigma, les projets allemands devenaient transparents, car les Anglais pouvaient lire dans les cerveaux du Haut Commandement allemand. Si les Anglais surprenaient l'annonce d'une attaque imminente, ils pourraient alors envoyer des renforts, ou tenter une manœuvre d'évitement. S'ils pouvaient déchiffrer des débats entre

Allemands sur leurs propres points faibles, ils seraient en mesure d'y concentrer leurs offensives. Les déchiffrements de Bletchley étaient donc de la plus haute importance.

Ainsi lorsque, en avril 1940, l'Allemagne envahit le Danemark et la Norvège, Bletchley procura un plan détaillé des opérations allemandes. De même, au début de la bataille d'Angleterre, les cryptanalystes purent avertir de bombardements, en précisant exactement où et quand ils auraient lieu. Ils purent aussi donner des informations constamment mises à jour sur la *Luftwaffe*, comme le nombre des appareils abattus et la vitesse à laquelle ils étaient remplacés. Bletchley envoyait tous ces renseignements au Quartier général M16, qui les transmettait au ministère de la Guerre, au ministre de l'Air et à l'Amirauté.

Au milieu de leurs activités, les cryptanalystes trouvaient parfois le temps d'une récréation. Selon Malcolm Muggeridge, qui servait dans les services secrets et qui se rendit à Bletchley, les parties de *balle-au-camp* y étaient le passe-temps favori.

Chaque jour après le déjeuner, si le temps était clément, les décrypteurs jouaient à la balle-au-camp sur la pelouse du manoir, avec un sérieux qu'affichent plutôt des universitaires engagés dans les activités moins frivoles comparées au poids de leurs responsabilités. Un point du jeu pouvait susciter autant de discussions qu'un débat sur la liberté d'action et le déterminisme, ou sur le big-bang originel et le processus continu de création.

Ayant maîtrisé les techniques polonaises, les cryptanalystes de Bletchley commencèrent à découvrir leurs propres raccourcis pour trouver les clefs d'Enigma. Ils repérèrent par exemple que les opérateurs allemands choisissaient parfois des messages-clefs évidents. Pour chaque message, l'opérateur était supposé utiliser un message-clef différent, dont les trois lettres étaient choisies au hasard. Mais dans la fièvre de la bataille, plutôt que se donner le mal de chercher une clef au hasard, les opérateurs débordés optaient quelquefois pour les trois lettres se suivant sur le clavier, comme *QWE* ou *BNM* ([figure 46](#)). Ces messages prévisibles furent baptisés *cillies*. Un autre exemple de cillie était l'usage répété du même message-clef (ce pouvait être les initiales de la petite amie de l'opérateur, du genre des lettres C-I-L, qui sont à l'origine du terme), ou d'un explétif allemand court. Avant d'attaquer Enigma par la

voie normale et difficile, les cryptanalystes essayaient systématiquement des cillies et, quelquefois, leurs pressentiments s'avéraient payants.



Fig. 45 Les décrypteurs de Bletchley se détendent en jouant à la balle-au-camp.

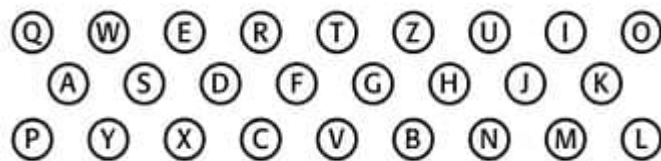


Fig. 46 Le clavier d'Enigma

Les « cillies » n'étaient pas des défauts inhérents à la machine Enigma, mais des faiblesses dans l'utilisation qui en était faite. L'erreur humaine à des niveaux plus élevés compromet également la sécurité du chiffre d'Enigma. Des responsables de l'application des carnets de code devaient décider quels rotors seraient utilisés chaque jour, et dans quelles positions. Ils tentaient d'assurer l'imprévisibilité des ajustements du brouilleur en excluant qu'un rotor reste à la même place deux jours de suite. Ainsi, si nous appelons les rotors 1, 2, 3, 4 et 5, le premier jour on pouvait avoir l'agencement 134, le deuxième jour 215, mais pas 214 puisque le rotor 4 ne doit pas rester à la même place deux jours de suite. Cela peut sembler une stratégie subtile puisque les rotors changent constamment de place, mais en se conformant trop rigide-ment à cette règle, on facilitait la tâche du cryptanalyste. Renoncer à certains agencements afin qu'un rotor ne reste pas à la même place réduisait de moitié le nombre des agencements possibles. Les cryptanalystes de

Bletchley comprirent ce qui se passait et l'exploitèrent magnifiquement. Ayant identifié l'agencement des rotors pour un jour donné, ils pouvaient immédiatement éliminer la moitié des positions possibles pour le jour suivant. Leur charge en était réduite de moitié.

De même, une règle stipulait que des connexions ne s'effectueraient pas entre deux lettres voisines, ce qui signifie que S pouvait être connecté à n'importe quelle lettre, sauf R et T. La théorie disait que des permutations aussi évidentes devaient absolument être évitées, mais, une fois encore, l'application de cette loi réduisait de manière drastique le nombre des clefs possibles.

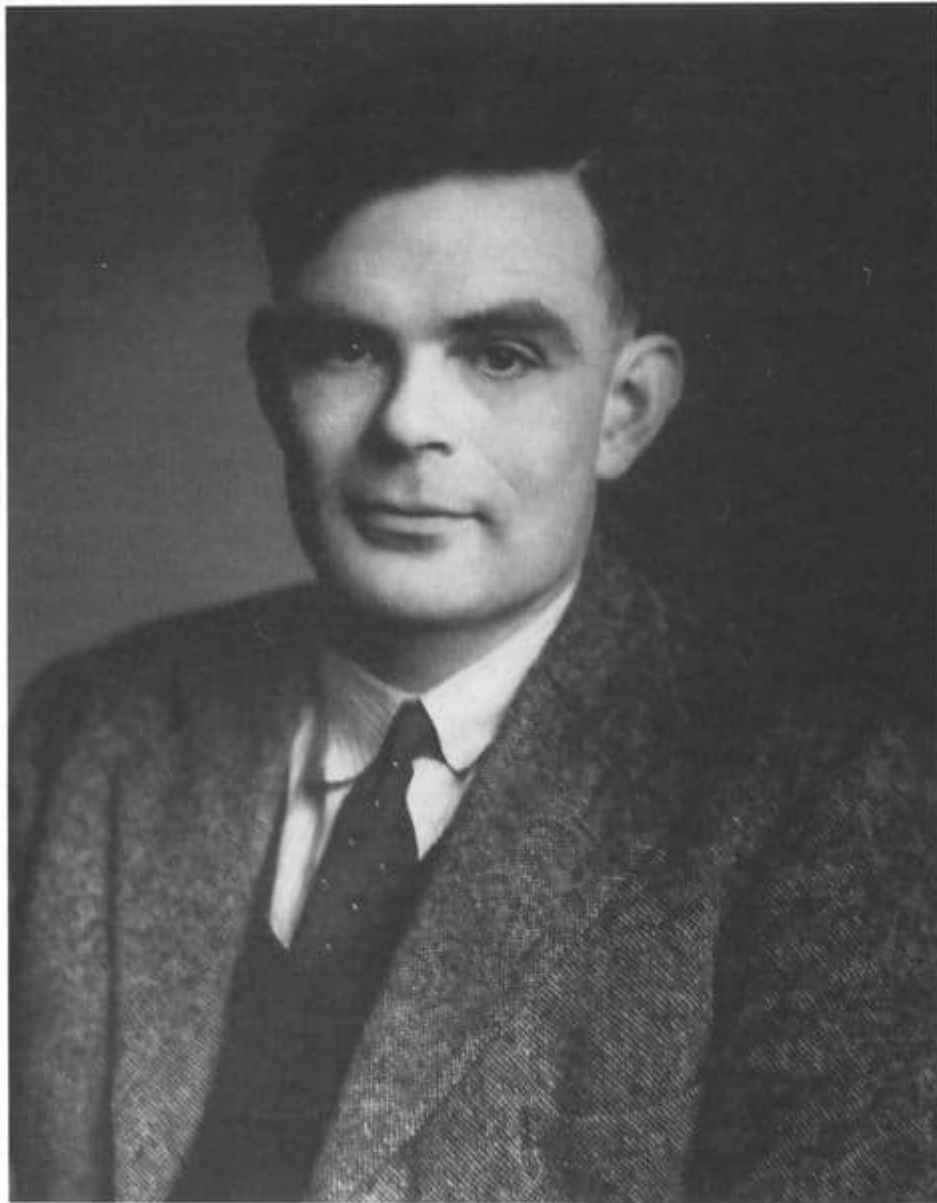
Cette recherche constante de raccourcis cryptanalytiques fut rendue nécessaire par l'évolution de la machine Enigma tout au long de la guerre. Les cryptanalystes étaient sans cesse contraints d'innover, de redessiner et sophistiquer les bombes, d'élaborer de nouvelles stratégies. Une grande part de leur succès est due à cette combinaison inhabituelle, à l'intérieur de chaque hutte, de mathématiciens, de scientifiques, de linguistes, de champions d'échecs, et de cruciverbistes fanatiques. Un problème apparemment insoluble passait de main en main, jusqu'à ce que quelqu'un disposant des bons outils intellectuels le résolve, ou qu'il parvienne à quelqu'un qui le résolvait partiellement avant de le faire circuler à nouveau. Gordon Welchman, le responsable de la Hutte 6, décrivait son équipe comme « une meute de chiens tentant de trouver une piste ».

Il y eut maints cryptanalystes remarquables, et des trouvailles d'une grande portée, et il faudrait plusieurs gros volumes pour détailler toutes les contributions individuelles. Mais si l'on ne doit évoquer qu'une seule personne, ce sera Alan Turing, qui cerna la plus grande faiblesse d'Enigma, et l'exploita impitoyablement. Grâce à Turing, il devint possible de briser le chiffre d'Enigma même dans les circonstances les plus difficiles.

Alan Turing fut conçu à l'automne 1911 à Chatrapur, près de Madras dans le sud de l'Inde, où son père, Julius Turing, était fonctionnaire de l'administration indienne. Julius et sa femme, Ethel, tenaient à ce que leur fils voie le jour en Angleterre et rentrèrent à Londres où Alan naquit le 23 juin 1912. Son père retourna en Inde peu après la naissance, et sa mère le suivit quinze mois plus tard, laissant Alan à la garde de nourrices et d'amis, jusqu'à ce qu'il atteigne l'âge d'aller en pension.

En 1926, à quatorze ans, Turing entra à l'école de Sherborne, dans le Dorset. Son premier jour de rentrée coïncida avec une grève générale, mais Turing ne voulait pas manquer et il pédala tout seul de Southampton à Sherborne, cent kilomètres sur sa bicyclette, anecdote rapportée dans le journal local. Au bout d'une année de scolarité, il s'était fait la réputation d'un garçon timide, gauche, dont les talents ne s'exprimaient qu'en sciences. Le but de Sherborne était de transformer les jeunes garçons en hommes formés aux nécessités du service de l'Empire, mais Turing ne partageait pas cette ambition et ses années de scolarité furent assez malheureuses.

Son seul véritable ami à Sherborne fut Christopher Morcom qui, comme Turing, était attiré par les sciences. Ils discutaient ensemble des plus récentes publications scientifiques, et menaient leurs propres expériences. Cette relation stimula la curiosité intellectuelle de Turing mais, surtout, elle eut sur lui des répercussions émotionnelles profondes. Andrew Hodges, le biographe de Turing, écrit : « C'était le premier amour... Il lui apportait, avec un sentiment d'abandon, une sensibilité plus grande, comme si soudain une couleur éblouissante explosait sur un monde en noir et blanc. » Leur amitié dura quatre ans, mais Morcom semble ne pas s'être rendu compte de la profondeur des sentiments que Turing lui portait. Et, pendant leur dernière année à Sherborne, Turing perdit pour toujours la chance de lui manifester son attachement : le 13 février 1930, Christopher Morcom mourut brutalement de tuberculose.



[Fig. 47](#) Alan Turing.

Turing fut bouleversé par la perte du seul être qu'il ait réellement aimé. Sa façon de surmonter la mort de Morcom fut de se plonger dans ses études scientifiques, comme s'il essayait de tenir la place de son ami. Morcom, qui semblait le plus doué des deux, avait déjà obtenu une bourse pour l'université de Cambridge et Turing crut qu'il était de son devoir d'intégrer lui aussi Cambridge et d'y faire un jour les découvertes que son ami aurait certainement faites. Il demanda une photographie à la mère de Christopher et, lorsqu'elle lui parvint, il lui écrivit pour la remercier : « Il est sur mon bureau maintenant, et m'encourage à travailler dur. »

En 1931, Turing fut admis au King's College de Cambridge. Il y arriva au moment où un débat passionné s'était instauré sur la nature des mathématiques et la logique, et se retrouva au milieu des principaux protagonistes, Bertrand Russell, Alfred N. Whitehead, et Ludwig Wittgenstein. Au centre du débat était la question de l'*indécidabilité*, une notion controversée développée par le logicien Kurt Gödel. On avait toujours admis qu'en principe, du moins, il y avait une réponse à toutes les questions mathématiques. Gödel démontrait au contraire qu'il peut exister un petit nombre de questions qui échappent à toute preuve logique, des questions « indécidables ». Les mathématiciens furent choqués d'entendre que les mathématiques n'étaient pas la discipline infaillible qu'ils avaient toujours cru. Ils tentèrent de défendre leur domaine en cherchant un moyen d'identifier les fameuses questions indécidables, afin de les réfuter. C'est cet objectif qui inspira à Turing son article mathématique le plus connu, *On Computable Numbers*, publié en 1937. Dans *Breaking the code*, la pièce de Hugh Whitmore inspirée par la vie de Turing, un personnage lui demande le sens de son article. Turing répond : « C'est à propos du vrai et du faux. En termes généraux. C'est un article technique de logique mathématique, mais c'est aussi sur la difficulté de discerner le vrai du faux. Les gens pensent — la plupart des gens pensent — qu'en mathématiques nous savons toujours ce qui est vrai et ce qui est faux. Cela ne se passe pas comme ça. Plus maintenant. »

Pour identifier les questions indécidables, l'article de Turing décrivait une machine imaginaire conçue pour exécuter une opération mathématique donnée, ou algorithme. Autrement dit, la machine pourrait enchaîner automatiquement une série d'étapes immuables pour arriver, par exemple, à multiplier deux nombres. Turing voyait ces nombres introduits dans la machine à l'aide d'une bande perforée, du genre de celles qu'on utilise pour mettre un air sur un piano mécanique. Le produit de la multiplication ressortirait sur une autre bande perforée. Turing imagina toute une série de ces *machines de Turing*, comme on les appela, chacune destinée à une tâche particulière comme diviser, élever au carré, factoriser un nombre. Puis, il se lança dans une voie plus hardie.

Il imagina une machine dont les fonctions internes seraient modifiables afin de pouvoir remplir toutes les fonctions de toutes les machines de Turing concevables. Les modifications consisteraient à insérer des bandes perforées soigneusement choisies, qui

transformeraient cette machine adaptable unique en une machine à diviser, à multiplier, ou à effectuer toute autre opération. Turing appela ce projet chimérique la machine universelle, puisqu'elle serait capable de répondre à n'importe quelle question entraînant une réponse logique. Malheureusement, il apparut que décider si une question était indécidable ne pouvait se faire logiquement, et la *machine universelle de Turing* elle-même ne pouvait identifier toutes les questions indécidables.

Les mathématiciens qui lirent l'article de Turing furent déçus de voir que le monstre de Gödel n'avait pas été dompté, mais, comme prix de consolation, Turing leur fournissait l'ébauche du calculateur programmable moderne. Turing connaissait le travail de Babbage et, d'une certaine façon, la machine universelle de Turing était une réincarnation du *Difference Engine n° 2*. En fait, Turing allait beaucoup plus loin, et apportait au calculateur une solide base théorique, lui conférant un potentiel jusque-là inimaginable. On était encore dans les années 30 et la technologie ne permettait pas de faire de la machine universelle une réalité, mais Turing ne fut pas du tout déçu que ses théories s'avèrent en avance sur ce qui était techniquement réalisable. Il voulait être reconnu par la communauté des mathématiciens, qui salua effectivement son travail comme l'une des avancées les plus importantes du siècle. Il n'avait alors que vingt-six ans.

Cette période fut pour Turing celle du bonheur et du succès. Au cours des années 30, il progressa jusqu'à être chargé de cours au King's College, une institution qui abrite l'élite intellectuelle mondiale. Il mena la vie typique d'un universitaire de Cambridge, mêlant aux mathématiques des activités ordinaires. En 1938, il se fit une obligation d'aller voir *Blanche-Neige et les Sept Nains*, avec la scène inoubliable où la sorcière trempe une pomme dans du poison. Ses collègues l'entendirent ensuite chantonner sans cesse : « Dans la potion la pomme trempe, que s'insinue la mort dormante. »

Turing aima ses années à Cambridge. En plus de ses succès académiques, il y trouva un environnement sportif et tolérant. L'homosexualité étant largement admise à l'université, il fut libre de nouer un certain nombre de relations sans se soucier du qu'en-dira-t-on. Bien qu'il n'eût pas une seule liaison durable, il semblait content de sa vie. Soudain, en 1933, sa carrière universitaire fut stoppée net. L'École du code et du chiffre l'invita à devenir cryptanalyste à Bletchley et, le 4 septembre 1939, lendemain du jour où Neville Chamberlain déclarait la

guerre à l'Allemagne, Turing quitta la superbe cour carrée de Cambridge pour l'Auberge de la Couronne, à Shenley Brook End.

Chaque jour, il parcourait à vélo les cinq kilomètres qui séparent Shenley Brook End de Bletchley Park, où il passait une partie de son temps dans les huttes, à travailler comme les autres au percement des codes, et le reste du temps dans le *think-tank*, le *réservoir de matière grise*, de Bletchley, qui avait été précédemment la resserre de pommes, de poires et de prunes de sir Herbert Leon. C'est là que les cryptanalystes réfléchissaient aux moyens de résoudre de nouveaux problèmes, ou anticipaient sur ceux qui pouvaient surgir dans un futur proche. Turing se concentrait sur le problème posé par une éventuelle modification par les Allemands dans le système de messages-clefs. Les premiers succès de Bletchley devaient tout aux travaux de Rejewski, qui exploitaient le fait que les opérateurs d'Enigma cryptaient chaque message-clef deux fois de suite ; si le message était YGB, les opérateurs chiffraient donc YGBYGB. Cette répétition était destinée à éviter une erreur pour le destinataire, mais elle constituait un point faible dans la sécurité d'Enigma. Les cryptanalystes anglais comprirent qu'il ne faudrait pas longtemps aux Allemands pour s'en apercevoir, et qu'à ce moment-là les opérateurs d'Enigma seraient amenés à supprimer cette répétition, réduisant à néant les méthodes en cours à Bletchley pour le décryptage. La mission de Turing était de trouver une autre voie pour attaquer Enigma, une voie qui ne serait pas fondée sur la répétition du message-clef.

Les semaines passant, une grande bibliothèque se remplissait à Bletchley des messages décryptés accumulés et Turing remarqua qu'un grand nombre d'entre eux se conformaient à une structure stricte. En étudiant de vieux messages décryptés, il pensa que l'on pourrait parfois prédire une partie du contenu d'un message, d'après la date de son envoi et sa source. L'expérience montrait, par exemple, que les Allemands envoyaient un bulletin météo, chiffré par Enigma, chaque jour peu après 6 heures du matin. Ainsi un message intercepté à 6 h 05 comportait presque sûrement le mot *Wetter*, le mot allemand pour *temps*. Le protocole rigoureux appliqué par toutes les organisations militaires entraînait que le style de ces messages soit parfaitement réglementé, aussi Turing avait une idée de la place du mot *Wetter* dans le message crypté. Des essais pourraient lui prouver si les six premières lettres d'un texte crypté donné correspondaient aux lettres du texte clair *Wetter*. On

appelle cette méthode, la méthode des *mots probables*. Pour les Anglais, c'était des *cribs*.

Turing avait l'intuition qu'armé de ces *cribs*, il pourrait vaincre Enigma. Devant un texte crypté, s'il connaissait le groupement de lettres représentant *Wetter*, disons *ETJWPX*, il s'agissait d'identifier quels réglages de la machine Enigma transformeraient *Wetter* en *ETJWPX*. Le chemin le plus direct, serait de prendre une machine Enigma, de taper *Wetter* et de voir si le texte chiffré exact en sortait. Dans le cas contraire, le cryptanalyste devrait modifier les agencements de la machine, en changeant les connexions de fils, en permutant les brouilleurs, ou en les réorientant, et taper *Wetter* à nouveau. Si l'on n'obtient toujours pas le texte chiffré exact, on change une nouvelle fois tous ces agencements, et on recommence encore et encore. Le seul problème avec cette approche est que, parmi les 159 milliards de milliards d'ajustements possibles à tester, il est hautement improbable de trouver celui qui transformera *Wetter* en *ETJWPX*.

Afin de simplifier le problème, Turing essaya d'appliquer la même stratégie que Rejewski. Il voulait séparer la question des réglages de rotors (quel rotor est à quelle place, et quelles sont leurs orientations respectives) de la question des connexions du tableau. S'il pouvait trouver quelque chose dans le *crib* qui n'ait rien à voir avec les connexions, il pourrait essayer les 1 054 560 combinaisons possibles des rotors (60 dispositions x 17 576 orientations). Ayant établi les positions exactes des rotors, il pourrait ensuite déduire les connexions du tableau.

Il se fixa sur un type particulier de *cribs*, ceux à l'intérieur desquels on notait des boucles semblables aux chaînes de Rejewski. Les chaînes de Rejewski liaient les lettres dans les messages-clefs. Les boucles de Turing n'avaient rien à voir avec les messages-clefs, puisqu'il travaillait sur l'hypothèse que les Allemands cesseraient bientôt d'en envoyer. À la place, les boucles de Turing connectaient les lettres du texte clair et du texte chiffré dans un mot probable. L'exemple montré sur l'illustration contient une boucle.

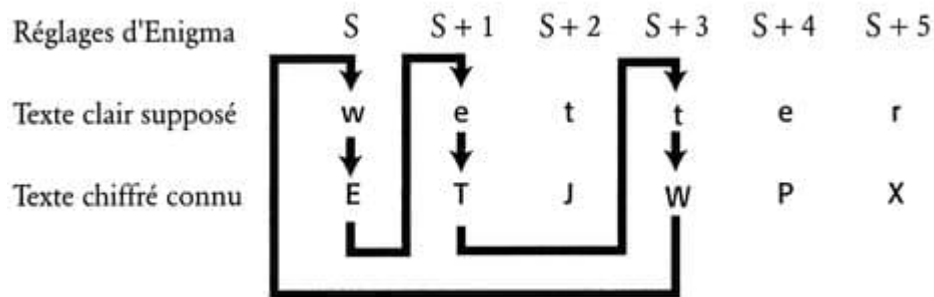


Fig 48 Un des mots probables de Turing, montrant une boucle

On s'en souvient : les mots probables ne sont que devinés, mais si nous estimons que ce *crib* est correct, alors nous pouvons lier les lettres $W \rightarrow E$, $e \rightarrow T$, $t \rightarrow W$ dans une partie de la boucle. Bien qu'ignorant les réglages initiaux d'Enigma, nous pouvons désigner cette disposition, quelle qu'elle soit, par S. Dans cette première disposition, nous savons que w est crypté E. Après ce cryptage, le premier rotor tourne d'une place et arrive en position (S+1) et la lettre e est cryptée T. Le rotor tourne d'une autre place et crypte une lettre qui ne fait pas partie de la boucle, et nous l'oublions. Le rotor se remet en marche et avance d'une place où nous atteignons de nouveau une lettre qui fait partie de la boucle. Dans cette disposition (S+3), nous savons que la lettre t est cryptée W. En résumé nous savons que :

En position S, Enigma crypte w en E
 En position S+1, Enigma crypte e en T
 En position S+3, Enigma crypte t en W

Cette boucle semble n'être rien de plus qu'un dessin curieux, mais Turing en examina rigoureusement les implications, et il découvrit qu'elles lui procuraient le raccourci qu'il cherchait. Au lieu de travailler sur une seule machine et d'en essayer toutes les dispositions, Turing commença par imaginer trois machines séparées, chacune travaillant sur le chiffrement d'un élément de la boucle. La première machine essaierait de chiffrer w en E, la seconde machine essaierait de chiffrer e en T et la troisième machine essaierait de chiffrer t en W.

Les trois machines auraient des réglages identiques, sauf que la deuxième aurait l'orientation de son brouilleur avancée d'une place par rapport à la première (S+1), et que la troisième serait réglée initialement en (S+3). Pour appliquer ces critères, Turing se représentait un cryptanalyste frénétique, changeant sans arrêt les connexions, essayant toutes les positions des rotors, modifiant les orientations. Tout câblage

modifié dans la première machine devait l'être aussi dans les deux autres. Et surtout, quelles que fussent les orientations fixées dans la première machine, elles devaient être décalées d'une place dans la deuxième et de trois places dans la troisième.

On ne voit pas encore très bien l'avantage de cette démarche. Le cryptanalyste doit toujours essayer les 159 milliards de milliards de dispositions possibles et, pour tout arranger, il doit le faire maintenant sur les trois machines simultanément. Mais Turing fit un nouveau pas qui simplifia considérablement les opérations. Il imagina de relier les trois machines par des fils électriques ([figure 49](#)), de façon que le circuit électrique reproduise en dur la boucle virtuelle du *crib*. Les connexions et les rotors changeraient sur la machine, comme décrit ci-dessus, mais le circuit ne serait achevé que lorsque tous les réglages seraient justes pour les trois machines, permettant au courant de passer à travers les trois. Si Turing introduisait dans le circuit une ampoule électrique, elle ne s'allumerait que lorsque les réglages exacts auraient été trouvés. À ce stade, les trois machines avaient toujours à essayer le même nombre colossal d'options pour allumer l'ampoule. Mais tout ceci n'avait été que la préparation du bond logique final de Turing, qui devait rendre la tâche cent millions de millions de fois plus facile d'un seul coup.

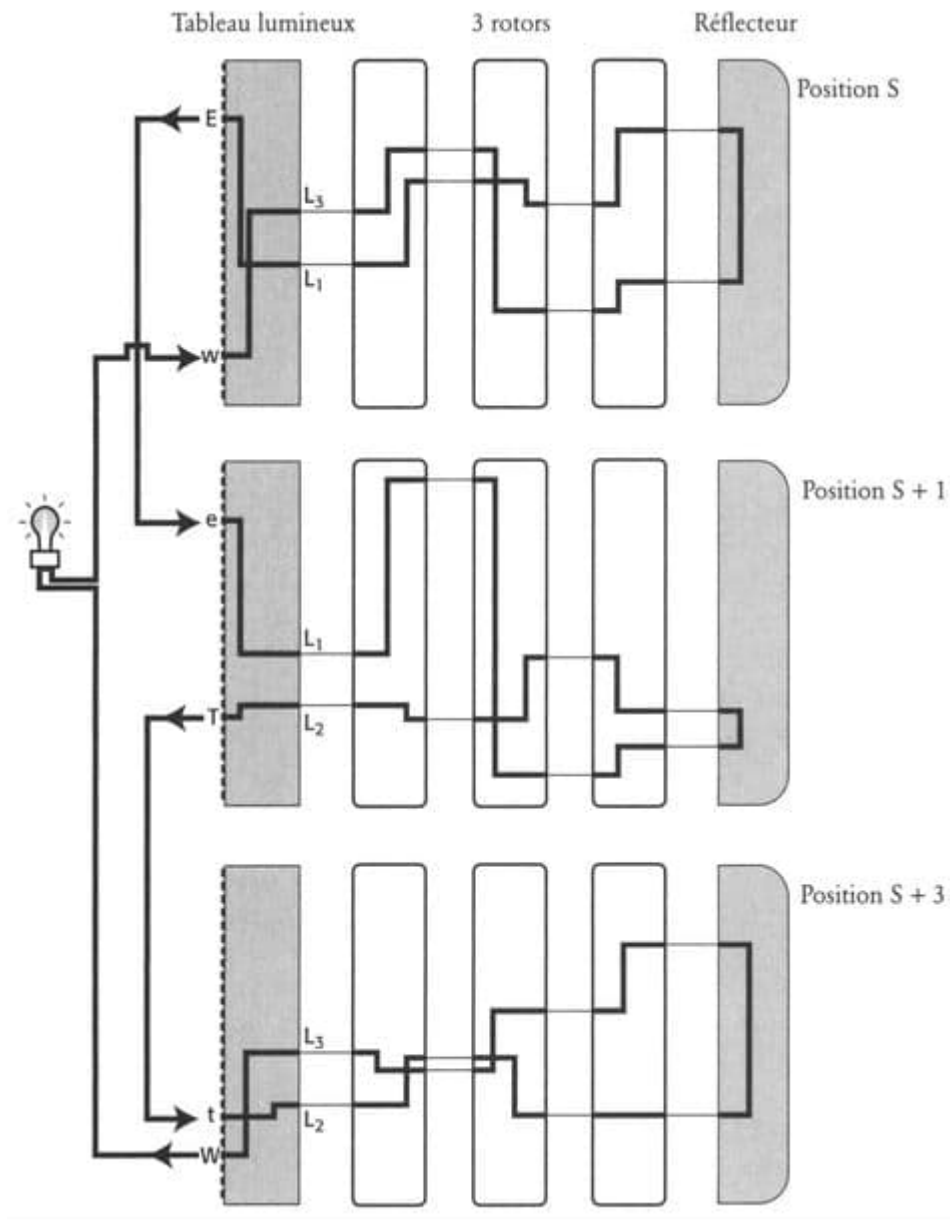


Fig. 49 Analogie électrique de la boucle du *crib* (ou mot probable). Trois machines Enigma sont réglées de manière identique, mais la deuxième a son premier rotor avancé d'un cran (disposition S+1) et la troisième a son rotor avancé de deux crans supplémentaires (S+3). Les fils sortant de chaque Enigma sont connectés à ceux entrant dans la suivante. Les trois jeux de rotors cliquent à l'unisson jusqu'à ce que le circuit soit bouclé et qu'une lampe s'allume. À ce moment-là, la disposition exacte est trouvée. Dans le diagramme ci-dessus, le circuit est bouclé.

Turing avait construit son circuit électrique de manière à annuler l'effet du tableau de connexions, s'autorisant ainsi à ignorer les milliards de branchements du tableau. Si nous regardons la [figure 49](#), sur la première Enigma le courant électrique pénètre dans les rotors et sort à une lettre inconnue, disons L_1 . Le courant ensuite passe par le tableau de connexions et transforme L_1 en E . Cette lettre E est reliée par un câble à la lettre E de la deuxième Enigma, et lorsque le courant passe à travers le

deuxième tableau de connexions, elle est transformée à nouveau en L_1 . Autrement dit, les deux tableaux s'annulent l'un l'autre. De même le courant sortant des rotors de la deuxième Enigma pénètre dans le tableau à L_2 , avant d'être transformé en T . Cette lettre T est connectée par un câble à la lettre T de la troisième Enigma, et lorsque le courant passe par le troisième tableau de connexions, elle redevient L_2 . En clair les tableaux de connexions s'annulent entre eux au long du circuit, et Turing pouvait donc se dispenser d'en tenir compte.

Turing devait simplement lier la lettre issue du premier groupe de rotors, L_1 , à la lettre entrant dans le deuxième groupe L_1 , et ainsi de suite. Il ne connaissait malheureusement pas l'identité de L_1 , et il devait connecter les 26 sorties du premier groupe de rotors aux 26 entrées dans le deuxième, et ainsi de suite. Il y avait maintenant 26 boucles électriques, et chacune était équipée d'une ampoule électrique pour signaler lorsqu'un circuit électrique était bouclé. Les trois groupes de rotors pouvaient alors essayer chacune des 17 576 orientations, avec le deuxième groupe toujours un cran en avance sur le premier, et le troisième deux crans en avance sur le deuxième. Si les rotors changeaient d'orientation toutes les secondes, il ne faudrait que cinq heures pour essayer toutes les orientations.

Il restait deux problèmes. D'abord, il se pouvait que les machines fonctionnent sur un mauvais ajustement du brouilleur, puisque l'Enigma opérait avec trois des cinq rotors disponibles, placés dans n'importe quel ordre, selon soixante dispositions possibles. Ainsi lorsque les 17 576 orientations avaient été essayées, si l'ampoule ne s'était pas allumée, il fallait essayer l'une des soixante autres dispositions des rotors et continuer jusqu'à ce que le circuit soit bouclé. Ou alors, le cryptanalyste aurait dû avoir soixante séries de trois Enigma fonctionnant en parallèle.

Le deuxième problème était de trouver les branchements du tableau de connexions, une fois établies la disposition des rotors et leurs orientations. Cela était relativement simple. En se servant d'une Enigma réglée conformément aux positions et orientations correctes des rotors, le cryptanalyste tape un texte chiffré et regarde le texte clair qui en sort. Si le résultat est *tewwer*, au lieu de *wetter*, il est clair qu'une connexion permute le *w* et le *t*. Taper d'autres extraits de textes chiffrés révélera d'autres connexions.

La combinaison des mots probables, des boucles et des machines reliées électriquement fournissait un outil remarquable à la cryptanalyse,

et seul Turing, avec son expérience unique sur les machines mathématiques, pouvait en être l'auteur. Ses rêveries sur les imaginaires machines de Turing tendaient à répondre à des questions ésotériques sur l'indécidabilité mathématique, mais cette recherche purement académique l'avait préparé à concevoir une machine utilisable, capable de résoudre des problèmes bien réels.

Bletchley réussit à obtenir 100 000 livres pour concrétiser l'idée de Turing sous forme de machines que l'on appela des *bombes*, en référence à la bombe de Rejewski. Chacune des bombes de Turing devait être constituée de douze groupes de rotors reliés électriquement, ce qui leur permettrait de s'attaquer à de plus longues boucles de lettres. L'élément complet mesurait presque deux mètres de haut, deux mètres de long, et un mètre de large. Turing finalisa son projet au début de 1940 et la construction en fut confiée à l'usine British Tabulating Machinery, à Letchworth.

En attendant la livraison des bombes, Turing continua son travail à Bletchley. Son invention fut bientôt connue des autres cryptanalystes du lieu qui saluèrent en lui un décrypteur d'exception. Selon Peter Hilton, un de ses collègues de Bletchley, « Alan Turing était évidemment un génie, mais un génie amical que l'on pouvait approcher. Il était toujours prêt à perdre du temps et à se donner du mal pour expliquer ses idées ; mais ce n'était pas un spécialiste étroit, et ses réflexions embrassaient un vaste domaine des sciences ».

Bien entendu, tout était tenu secret au GC&CS, et personne en dehors de Bletchley n'était au courant de la réalisation de Turing. Ses parents eux-mêmes ignoraient totalement qu'il travaillait sur les codes, à plus forte raison qu'il était le premier cryptanalyste anglais. Il avait dit un jour à sa mère qu'il était impliqué dans la recherche militaire, mais sans autre précision. Elle fut surtout déçue de voir qu'on n'avait pas imposé à son fils une coupe de cheveux plus convenable. Bien que Bletchley fût dirigé par des militaires, ils avaient compris qu'il leur fallait tolérer le laisser-aller et les excentricités de ces intellectuels. Turing prenait rarement la peine de se raser, ses ongles étaient noirs et ses vêtements froissés. Si les militaires fermèrent aussi les yeux sur son homosexualité, c'est ce que nous ignorons. Jack Good, un vétéran de Bletchley, déclara : « Heureusement que les autorités de Bletchley ne savaient pas que Turing était homosexuel, autrement nous aurions perdu la guerre. »

Le premier prototype de bombe, baptisé *Victoire*, arriva à Bletchley le 14 mars 1940. La machine fut mise immédiatement en service, mais ses débuts ne furent guère satisfaisants. Elle se révéla beaucoup plus lente qu'on ne l'attendait, mettant parfois une semaine à trouver une clef. Il fallut un effort concerté pour accroître l'efficacité de la bombe, et un plan modifié fut prêt quelques semaines plus tard. Cela prit encore quatre mois pour construire cette bombe améliorée.

À la même époque, les cryptanalystes durent faire face à la catastrophe qu'ils avaient prévue. Le 10 mai 1940, les Allemands changèrent de protocole pour l'envoi des clefs. Ils ne répétaient plus le message-clef, et par conséquent le nombre de déchiffrements d'Enigma chuta dramatiquement. Cette panne de l'information dura jusqu'au 8 août, date de l'arrivée de la nouvelle bombe. Baptisée *Agnus Dei*, ou de son diminutif *Agnès*, cette machine allait enfin répondre aux espérances de Turing.

Pendant les huit mois suivants, quinze nouvelles bombes furent mises en service, faisant chacune le bruit d'un million d'aiguilles à tricoter. Quand tout allait bien, une bombe pouvait trouver une clef d'Enigma en une heure. Lorsque les connexions du tableau et les positions des rotors (le message-clef) avaient été établis pour un message donné, il était facile d'en déduire la clef du jour. Tous les autres messages envoyés le même jour pouvaient alors être déchiffrés.

Pour autant, le déchiffrement n'était pas devenu une simple formalité. Il y avait bien des obstacles à surmonter avant que les bombes ne commencent à chercher la clef. Il fallait, par exemple, un mot probable. Les décrypteurs devaient fournir des mots probables aux opérateurs, mais il n'était pas garanti qu'ils avaient deviné le sens exact du texte chiffré. Même s'ils avaient le mot juste, il pouvait être à la mauvaise place ; les cryptanalystes pouvaient avoir deviné qu'un message crypté contenait une certaine phrase, mais avoir associé cette phrase à une fausse partie du texte. Il y avait un truc pour voir si un mot probable était à sa place. Dans l'exemple suivant, le cryptanalyste sait que le texte clair est juste, mais il ne sait pas s'il correspond bien aux lettres du texte chiffré.

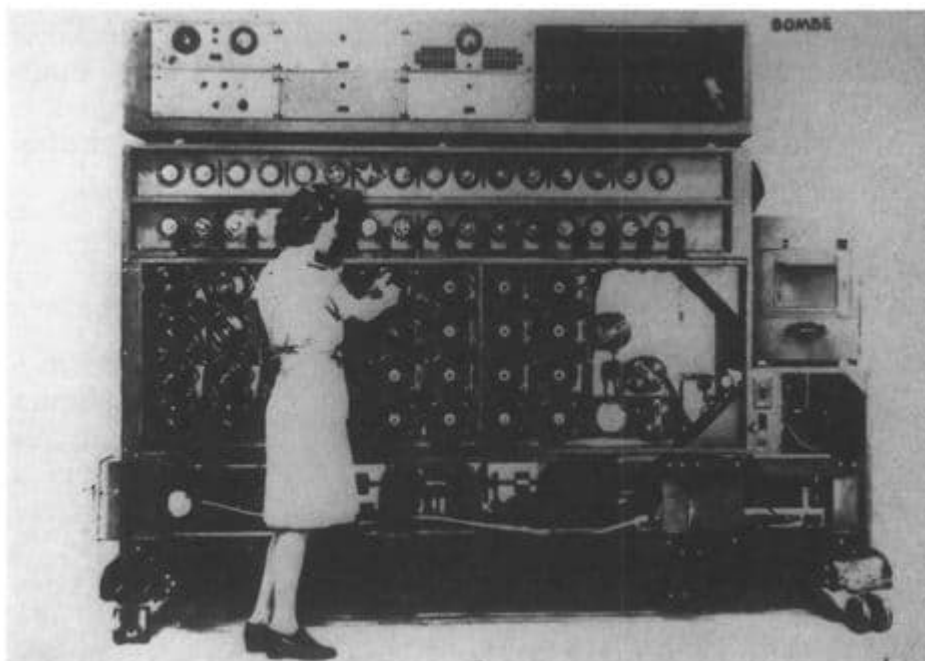


Fig. 50 Une bombe en action à Bletchley Park.

Texte clair probable	w e t t e r n u l l s e c h s
Texte chiffré connu	I P R E N L W K M J J S X C P L E J W Q

Nous avons mentionné plus haut qu'un des traits d'Enigma était de ne jamais chiffrer une lettre par elle-même, ce qui était une conséquence du réflecteur. La lettre a ne serait jamais chiffrée A, la lettre b jamais chiffrée B et ainsi de suite. Par conséquent, les lettres ci-dessus sont mal alignées, puisque le premier e de *wetter* correspond à un E du texte chiffré. Pour trouver le bon alignement, nous allons faire glisser le texte clair et le texte chiffré l'un par rapport à l'autre, afin qu'aucune lettre ne soit appariée avec elle-même. Si nous déplaçons le texte clair d'une lettre vers la gauche, cela ne convient toujours pas, puisque cette fois le premier s de *sechs* répond au S du texte chiffré. Si, par contre, nous décalons le texte clair d'une place vers la droite, nous ne voyons plus de chiffrements interdits : le texte probable a bien des chances de se trouver à la bonne place et pourra être utilisé comme base de déchiffrement par la bombe.

Texte clair probable	w e t t e r n u l l s e c h s
Texte chiffré connu	I P R E N L W K M J J S X C P L E J W Q

Les renseignements réunis à Bletchley n'étaient communiqués qu'aux principaux chefs militaires et à quelques membres du Cabinet de guerre.

Winston Churchill était très conscient de l'importance des déchiffrements de Bletchley, et le 6 septembre 1941, il rendit visite aux décrypteurs. Rencontrant quelques-uns des cryptanalystes, il fut surpris par la bizarre composition de la troupe qui lui procurait des informations si précieuses ; outre les mathématiciens et les linguistes, il y avait là un expert en porcelaine, un conservateur du musée de Prague, le champion anglais d'échecs et de nombreux bridgeurs. Churchill murmura à sir Stewart Menzies, qui était à la tête de l'Intelligence Service : « Je vous avais dit de ne pas omettre de retourner une seule pierre, mais je ne m'attendais pas à ce que vous me preniez au pied de la lettre. » Malgré ce commentaire, cette équipe hétéroclite lui plut, et il qualifia ses membres d'« oies qui déposent des œufs d'or et qui ne cacardent jamais ».

Cette visite avait pour but de remonter le moral des décrypteurs, en leur montrant que leur travail était apprécié en très haut lieu. Elle mit aussi Turing et ses collègues en position d'en appeler directement à Churchill quand une crise menaçait. Pour exploiter au mieux les bombes, Turing avait besoin de personnel supplémentaire, mais ses demandes avaient été bloquées par le commandant Edward Travis, qui avait pris la direction de Bletchley, et qui ne trouvait pas justifié de recruter du monde. Le 21 octobre 1941, les cryptanalystes décidèrent d'ignorer la hiérarchie, et ils écrivirent directement à Churchill.

Monsieur le Premier Ministre,

Il y a quelques semaines, vous nous avez honoré de votre visite, et nous croyons que vous jugez notre travail utile. Vous avez vu que, grâce à l'énergie et à la prévoyance du commandant Travis, on nous a fourni les bombes nécessaires à l'attaque des codes allemands d'Enigma. Nous croyons toutefois devoir vous informer que ce travail est retardé, et parfois même pas fait du tout, parce que nous n'avons pas assez de personnes pour l'exécuter. Nous nous adressons directement à vous parce que, depuis des mois, nous avons tenté tout ce qui est possible par les voies normales, et que nous désespérons d'obtenir la moindre amélioration sans votre intervention...

Nous sommes, Monsieur, vos obéissants serviteurs,

A.M. Turing

W.G. Welchman

C.H.O'D Alexander

P.S. Milner-Barry

Churchill n'hésita pas sur la réponse à envoyer. Il adressa immédiatement une note à son officier d'état-major :

À FAIRE AUJOURD'HUI

Assurez-vous qu'ils aient ce qu'ils veulent de toute urgence et tenez-moi informé.

À partir de là, il n'y eut plus de restrictions au recrutement ni à l'achat de matériel. À la fin de 1942, il y avait quarante-neuf bombes, et un nouveau site regroupant des bombes fut créé à Gayhurst Manor, au nord de Bletchley. Entre autres moyens de recrutement, la GC&CS fit passer une annonce anonyme dans le *Daily Telegraph*. On lançait un défi aux lecteurs, qui consistait à résoudre les mots croisés du journal en moins de douze minutes. Il était prouvé que les bons cruciverbistes peuvent se révéler de bons décrypteurs, mais ceci n'était évidemment pas spécifié dans le journal. Les vingt-cinq lecteurs qui répondirent furent invités à Fleet Street pour participer à un test au siège du journal. Cinq d'entre eux remplirent la grille dans le temps imparti, et un autre n'avait qu'un mot manquant à l'expiration du délai de douze minutes. Quelques semaines plus tard, tous les six eurent un entretien avec le service des renseignements militaires, et furent recrutés pour Bletchley Park.

Comment piquer des carnets de code

Nous avons traité jusqu'ici le trafic effectué sur Enigma comme un système géant de communication, mais en fait il y avait plusieurs réseaux distincts. L'armée allemande d'Afrique du Nord, par exemple, avait son propre réseau, et leurs opérateurs avaient des carnets de codes différents de ceux utilisés en Europe. Identifier la clef du jour pour l'Afrique du Nord, permettait de déchiffrer tous les messages échangés en Afrique du Nord ce jour-là, mais ne servait à rien en ce qui concernait les messages transmis en Europe. De même, la Luftwaffe avait son propre réseau, et pour déchiffrer les échanges de la Luftwaffe, Bletchley devait trouver sa clef du jour.

Certains réseaux étaient mieux défendus que d'autres, et le réseau de la marine allemande était le plus fort de tous, car la Kriegsmarine opérait sur une version sophistiquée d'Enigma. Les opérateurs de l'Enigma navale avaient le choix entre huit rotors, au lieu de cinq, ce qui entraînait presque six fois plus de dispositions possibles des rotors, et donc presque six fois plus de clefs à essayer pour Bletchley. L'autre différence de l'Enigma navale concernait le réflecteur. Dans l'Enigma standard, le réflecteur était toujours placé selon la même orientation, alors que dans l'Enigma navale, il pouvait être tourné dans 26 orientations différentes. Le nombre de clefs était ainsi accru d'un facteur 26.

La cryptanalyse de l'Enigma navale était rendue encore plus compliquée du fait que ses opérateurs prenaient garde à ne pas envoyer de messages stéréotypés, privant ainsi Bletchley de mots probables. De plus, la Kriegsmarine institua un système plus sûr pour choisir et transmettre le message-clef. Des rotors supplémentaires, un réflecteur variable, des messages non stéréotypés et un nouveau système d'envoi des messages-clefs, tout cela rendait les communications navales allemandes impénétrables.

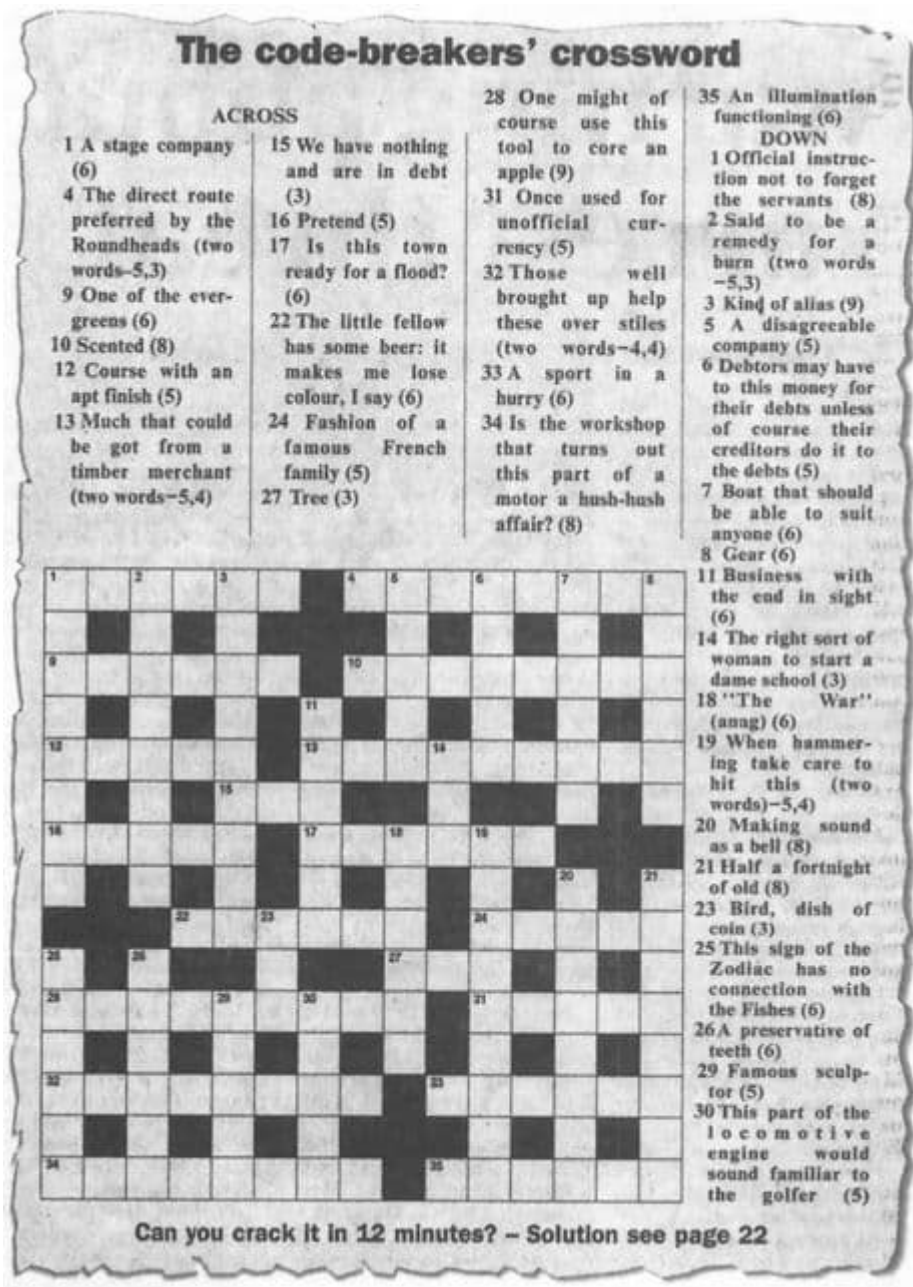


Fig. 51 Les mots croisés du *Daily Telegraph* utilisés pour le recrutement de nouveaux décrypteurs (Solution dans l'Annexe H).

L'incapacité pour Bletchley de résoudre l'Enigma navale signifiait que la Kriegsmarine allait prendre le dessus dans la bataille de l'Atlantique. L'amiral Karl Dönitz avait mis au point une stratégie en deux temps, dont le premier consistait à faire écumer l'Atlantique par ses sous-marins, à la recherche des convois alliés. Dès que l'un d'eux avait repéré une cible, il passait à la deuxième étape, en appelant d'autres sous-marins à la rescousse. L'attaque ne commençait que lorsque leur nombre était suffisant. Pour mener ces attaques coordonnées, il était essentiel de pouvoir compter sur le secret des communications. L'Enigma navale le

permettait, et les attaques des sous-marins se révélèrent dévastatrices pour les transports maritimes alliés, qui apportaient à l'Angleterre la nourriture et les armements indispensables.

Tant que les transmissions des sous-marins restèrent protégées, les Alliés n'eurent aucune idée de l'endroit où ils se trouvaient, et ne savaient quelles routes choisir pour assurer la sécurité des convois. Entre juin 1940 et juin 1941, les Alliés perdirent en moyenne cinquante bâtiments par mois, et virent le moment arriver où ils ne seraient plus en mesure de construire assez de nouveaux bateaux pour les remplacer. Outre l'intolérable destruction des bateaux, le coût humain était encore plus insupportable : 50 000 marins alliés moururent pendant la guerre.

L'Angleterre risquait donc de perdre la bataille de l'Atlantique, ce qui voulait dire perdre la guerre. « Dans un torrent d'événements tragiques, écrivit plus tard Churchill, une angoisse dominait. Des batailles pouvaient être gagnées ou perdues, des mouvements pouvaient rencontrer le succès ou l'échec, des territoires pouvaient être conquis ou abandonnés, mais ce qui nous permettait de continuer la guerre, ou simplement de rester vivants, était notre maîtrise des voies maritimes et la possibilité d'entrer et de sortir librement de nos ports. »

L'expérience polonaise et le cas de Hans-Tilo Schmidt avaient enseigné à Bletchley Park que, si les ressources intellectuelles ne parviennent pas à briser un chiffre, il peut être nécessaire de faire appel à l'espionnage, à l'infiltration, voire au vol, pour obtenir les clefs de l'ennemi. De temps en temps, Bletchley réussissait à percer l'Enigma navale grâce à un stratagème impliquant la Royal Air Force. Les avions anglais disposaient des mines dans un endroit précis, obligeant les bâtiments allemands proches du site à envoyer des mises en garde à d'autres équipages. Les avertissements contenaient nécessairement une carte pour le repérage, carte déjà connue des Anglais et qui pourrait être utilisée comme mot probable. Bletchley savait qu'une partie de ce texte crypté donnerait un ensemble de coordonnées fixées par les Anglais. Mais semer des mines pour récolter des mots probables — ce que la RAF appelait le *jardinage* — exigeait des missions spéciales qui ne pouvaient être répétées indéfiniment : Bletchley devait trouver un autre moyen de casser l'Enigma navale.

L'autre solution consistait à voler les clefs. L'un des plans les plus audacieux fut concocté par Ian Fleming, le créateur du personnage de James Bond, qui était membre des services de renseignements de la marine. Il suggéra de faire s'écraser dans la Manche un bombardier

allemand déjà capturé, à proximité d'un bateau allemand. Les marins allemands s'approcheraient alors pour sauver leurs camarades, et l'équipage de l'avion — des pilotes anglais se faisant passer pour allemands — monterait à bord du bâtiment et s'emparerait des carnets de codes. Ceux-ci portaient les renseignements nécessaires à l'établissement des clefs et, comme les bateaux étaient souvent éloignés de leur base pour de longues périodes, les carnets de codes devaient servir au moins un mois. Bletchley pourrait donc déchiffrer tous les envois sur l'Enigma navale pendant un mois.

Après avoir donné leur accord au plan de Fleming, baptisé *Opération Sans-Pitié*, les services secrets anglais commencèrent à préparer le bombardier Heinkel destiné à s'écraser, et ils réunirent un équipage anglais parlant l'allemand. L'opération devait avoir lieu en début de mois, afin de s'emparer d'un carnet de codes neuf. Fleming se rendit à Douvres pour surveiller les préparatifs, mais il n'y avait pas de bâtiment allemand dans les environs, et le plan fut reporté *sine die*. Quatre jours plus tard, Frank Birch qui dirigeait la section navale à Bletchley, rapporta la réaction de Turing et de son collègue Twinn : « Turing et Twinn vinrent me voir avec des têtes de croque-morts privés d'un beau cadavre, dans tous leurs états à la suite de l'annulation, deux jours auparavant, de l'opération Sans-Pitié. »

On renonça finalement à cette opération, et les carnets de codes allemands furent saisis au cours d'une série de raids audacieux menés contre des bateaux-météo et des sous-marins. Ces documents « piqués » donnaient à Bletchley ce dont il avait besoin pour mettre fin à la panne du renseignement. En voyant clair dans les messages de l'Enigma navale, Bletchley pouvait épingle la position des sous-marins et la bataille de l'Atlantique se retournait en faveur des Alliés. Les convois transitèrent à l'écart des sous-marins et les destroyers britanniques purent même passer à l'offensive en les recherchant et les coulant.

Naturellement, le commandement allemand ne devait pas soupçonner que ses carnets de codes avaient été saisis : les Allemands auraient alors renforcé leurs machines Enigma, et Bletchley se serait retrouvé à la case départ. Comme lors de l'épisode du télégramme de Zimmermann, les Anglais prirent diverses précautions pour détourner les soupçons, allant jusqu'à couler un navire allemand après avoir saisi ses codes — ceci pour persuader l'amiral Dönitz que le matériel de chiffrement avait été envoyé par le fond, et n'était pas tombé dans des mains anglaises.

Une fois le matériel saisi, des précautions supplémentaires devaient être prises avant d'exploiter les renseignements. Les déchiffrements d'Enigma donnaient l'emplacement des sous-marins, mais il aurait été maladroit de les attaquer tous, car une augmentation soudaine de la réussite anglaise aurait alerté les Allemands sur la lisibilité de leurs communications. Aussi les Alliés permirent-ils à certains sous-marins de leur échapper et n'en attaquèrent-ils d'autres qu'après qu'un avion d'observation eut fait d'abord un repérage, justifiant ainsi la venue d'un destroyer quelques heures plus tard. Ou bien les Alliés envoyaient un faux message faisant état du repérage d'un sous-marin, ce qui suffisait à expliquer l'attaque qui suivait.

En dépit de cette mise en scène, certaines actions anglaises inquiétèrent les experts allemands de la sécurité. À une occasion, Bletchley déchiffra un message Enigma qui donnait la position exacte d'un groupe de pétroliers allemands et de ravitailleurs, neuf unités au total. L'Amirauté décida de ne pas couler tous les bâtiments, pour éviter que ce nettoyage ne soulève des questions chez les Allemands. Ils n'envoyèrent aux destroyers que la position de sept bateaux, épargnant le *Gadania* et le *Gonzenhein*. Les sept bateaux ciblés furent coulés, mais les destroyers de la Royal Navy rencontrèrent par hasard les deux autres bâtiments et ils les envoyèrent également par le fond. Les destroyers n'étaient au courant ni d'Enigma, ni de la politique menée pour égarer les soupçons, ils pensèrent simplement faire leur devoir. De retour à Berlin, l'amiral Kurt Fricke ouvrit une enquête pour tenter de savoir si ces pertes étaient imputables à la malchance ou à un agent anglais qui aurait infiltré la Kriegsmarine. Personne ne soupçonna qu'il s'agissait d'une victoire sur Enigma.

Les cryptanalystes anonymes

Bletchley Park avait réussi non seulement à briser le chiffre de l'Enigma allemande, mais aussi à déchiffrer les messages italiens et japonais. Le renseignement provenant de ces trois sources reçut pour nom de code *Ultra*, et les documents fournis par Ultra donnèrent aux Alliés un net avantage sur tous les théâtres du conflit. En Afrique du Nord, Ultra aida à détruire les voies du ravitaillement allemand, et renseigna les Alliés sur l'état des forces du général Rommel, permettant à la VIII^e armée de repousser l'avance allemande. Ultra prévint aussi de l'invasion de la Grèce, ce qui permit aux troupes britanniques de se replier sans trop de pertes. Ultra procura des rapports précis sur la position de l'ennemi dans toute la Méditerranée. Cette information fut particulièrement précieuse lorsque les Alliés débarquèrent en Italie et en Sicile en 1943.

Mais surtout, Ultra joua un rôle prépondérant dans le débarquement allié en Europe, en 1944. Dans les mois précédant le jour J, les déchiffrements de Bletchley procurèrent un tableau détaillé des concentrations de troupes allemandes sur la côte française. Sir Harry Hinsley, historien officiel du renseignement anglais pendant la guerre, écrivit :

Au fur et à mesure qu'Ultra empilait des messages, on reçut quelques chocs peu agréables. En particulier Ultra révéla, dans la deuxième moitié de mai — alors que déjà d'inquiétantes informations antérieures signalaient que les Allemands avaient conclu que la zone entre Le Havre et Cherbourg serait un des sites probables du débarquement, peut-être même le principal —, qu'ils envoyaient des renforts en Normandie et dans le Cotentin. Mais cette information parvint à temps pour que les Alliés modifient les plans concernant leur arrivée à Utah Beach et la progression au-delà ; et de fait, avant que l'expédition ne lève l'ancre, les Alliés disposaient de l'estimation, de l'identification et de la localisation des divisions ennemies dans l'ouest — cinquante-huit au total

—, et tous ces points, qui allaient être d'une importance capitale, étaient exacts, à deux près.

Les cryptanalystes ne recevaient jamais de compte rendus des opérations et ils ne savaient pas comment on utilisait leurs déchiffrements. N'ayant pas été informés de la date du jour J, ils avaient organisé une soirée dansante la veille du débarquement. Cela contraria le commandant Travis, directeur de Bletchley, seule personne sur le site à être dans le secret du jour-J. Il ne voulut pas dire au comité de la danse de la Hutte 6 d'annuler leur fête, ce qui aurait été une indication claire qu'une offensive majeure allait se dérouler, et aurait nui à la sécurité. En fait, le mauvais temps repoussa l'action de vingt-quatre heures, et les décrypteurs eurent le temps de se remettre de leur folle soirée. Le jour du débarquement, la Résistance française coupa les lignes télégraphiques terrestres, ce qui obligea les Allemands à communiquer par radio, et permit du même coup à Bletchley d'intercepter et de déchiffrer encore plus de messages. À ce tournant de la guerre, Bletchley était en mesure de dresser un tableau parfaitement détaillé des forces allemandes.

Stuart Milner-Barry, l'un des cryptanalystes de la Hutte 6, nota : « Je ne peux pas imaginer qu'aucune guerre, depuis l'Antiquité, ait été menée avec l'un des camps en mesure de pénétrer le renseignement de l'autre. » Un rapport américain parvient à la même conclusion : « Ultra créa dans les états-majors et au sommet de la politique un état d'esprit qui transforma la prise de décisions. Sentir que rien ne vous échappe chez l'ennemi vous donne confiance, et ce sentiment grandit au fur et à mesure que vous observez ses pensées et ses réactions, ses habitudes et ses actes. Une telle connaissance rend vos plans moins timides et plus assurés, moins hésitants et plus optimistes. »

Que Bletchley Park ait ou non joué un rôle décisif dans la victoire des Alliés reste prétexte à controverses. Ce qui est certain, c'est que les briseurs de codes de Bletchley ont sensiblement écourté la guerre. C'est particulièrement évident lorsqu'on reconstitue la bataille de l'Atlantique et qu'on se représente comment les choses se seraient passées sans l'aide d'Ultra. Pour commencer, les Allemands auraient conservé une plus grande flotte de sous-marins et davantage de capacités d'intervention. Cela aurait compromis le lien vital avec l'Amérique, et les Alliés auraient dû consacrer des moyens humains et financiers considérables à la construction de nouveaux bateaux. Les historiens estiment que les plans alliés en auraient été retardés de plusieurs mois, et le débarquement

repoussé au moins à l'année suivante. « Mon sentiment personnel, écrit sir Harry Hinsley, est que la guerre, au lieu de s'achever en 1945, se serait poursuivie jusqu'en 1948 si la GC&CS n'avait pas été capable de lire les chiffres d'Enigma et de procurer les renseignements d'Ultra. »

Ce délai aurait entraîné un surcroît de pertes humaines, Hitler aurait pu faire un plus large usage de ses V1 et V2, et frapper tout le sud de l'Angleterre. L'historien David Kahn résume le rôle du succès sur Enigma comme suit : « Cela sauva des vies. Pas seulement les vies des Russes ou des Alliés, mais aussi des vies allemandes, italiennes et japonaises. Un certain nombre de personnes vivantes après la Seconde Guerre mondiale ne l'auraient pas été sans cette résolution. Voilà la dette que le monde a envers les briseurs de codes : c'est la récompense en valeur humaine de leurs triomphes. »

Après la guerre, les prouesses de Bletchley restèrent un secret bien gardé. Les Anglais souhaitaient continuer leurs opérations de renseignement, et ne tenaient pas à divulguer leurs capacités. En fait, l'Angleterre avait saisi des milliers de machines Enigma qu'elle distribua à travers ses anciennes colonies, qui croyaient le chiffre aussi sûr que l'avaient pensé les Allemands. Les Anglais ne firent rien pour ébranler cette foi, et déchiffrèrent systématiquement toutes ces communications secrètes pendant les années qui suivirent.

Au même moment, on ferma l'École du code et du chiffre de Bletchley Park, et les milliers d'hommes et de femmes qui avaient contribué à la création d'Ultra se séparèrent. Les bombes furent démontées, et le moindre bout de papier lié aux déchiffrements du temps de guerre fut soit mis de côté sous bonne garde, soit brûlé. Les activités de décodage anglaises furent transférées officiellement au nouveau Quartier général des communications à Londres (GCHQ), qui fut déplacé à Cheltenham en 1952. Quelques-uns des cryptanalystes furent mutés au GCHQ, mais la plupart retournèrent à la vie civile, tenus au secret par leur serment, et ne pouvant donc pas révéler leur rôle central dans l'effort de guerre allié.

Alors que ceux qui étaient allés au front pouvaient parler de leurs luttes héroïques, ceux qui avaient mené des batailles intellectuelles d'une portée qui n'était pas inférieure étaient dans l'obligation d'éviter les questions ou de mentir dans leurs réponses. Un des jeunes cryptanalystes qui avait travaillé dans la Hutte 6 reçut une lettre insultante de son vieux

provisoire, qui l'accusait d'avoir évité de se battre et d'être une honte pour son école.

Après trente années de silence, le voile fut levé sur Bletchley Park au début des années 1970. Le capitaine F.W. Winterbotham, qui avait été responsable de la distribution des renseignements d'Ultra, commença à faire le siège du gouvernement anglais, faisant valoir que les pays du Commonwealth ne se servaient plus du chiffre d'Enigma et qu'il n'y avait donc plus de raison de cacher que les Anglais l'avaient fracturé. Le service des renseignements finit par donner son accord, et l'autorisa à écrire un livre sur le travail effectué à Bletchley Park. Publié à l'été de 1974, le livre de Winterbotham, *The Ultra Secret*, fut le signal pour le personnel de Bletchley qu'il lui était enfin permis de parler de ses activités pendant la guerre. Gordon Welchman se sentit très soulagé : « Après guerre, j'évitais toute discussion sur ces événements de crainte de révéler une information que j'avais obtenue grâce à Ultra et non dans une quelconque publication... La nouvelle tournure des événements me délivrait de mon engagement au secret du temps de guerre. »

Ceux qui avaient tellement contribué à l'effort de guerre pouvaient maintenant recevoir la reconnaissance qu'ils méritaient. La plus notable conséquence des révélations de Winterbotham fut sans doute que Rejewski apprit les suites stupéfiantes de sa lutte contre Enigma avant la guerre. Après l'invasion de la Pologne, Rejewski avait fui en France et, quand la France avait été occupée, il avait cherché refuge en Angleterre. Il eût été naturel de l'intégrer à l'entreprise anglaise contre Enigma, mais on préféra le reléguer au traitement de chiffres minables dans une unité de renseignements mineure à Boxmoor, près de Hemel Hempstead. Il n'a jamais été expliqué pourquoi ce brillant cerveau avait été tenu à l'écart de Bletchley Park, mais le fait est qu'il ignora tout des activités de la GC&CS. Jusqu'à la publication du livre de Winterbotham, Rejewski n'avait pas su que ses travaux avaient été à la base du déchiffrement d'Enigma pendant toute la guerre.

Pour certains, la publication de ce livre venait trop tard. De nombreuses années après la mort d'Alastair Dennison, le premier directeur de Bletchley, sa fille reçut une lettre de l'un de ses collègues : « Votre père était un grand homme, envers qui toutes les personnes de langue anglaise auront une dette, pour très longtemps, si ce n'est pour toujours. Que si peu sachent exactement ce qu'il fit est le côté triste des choses. »

Alan Turing, lui non plus, ne vécut pas assez longtemps pour connaître une reconnaissance publique. Au lieu d'être acclamé comme un héros, il fut persécuté pour son homosexualité. En 1952, venu déclarer un cambriolage à la police, il eut la naïveté de révéler qu'il avait une liaison homosexuelle. La police l'arrêta aussitôt et l'inculpa pour « grave indécence contraire à l'article 11 de l'Acte d'amendement de la loi criminelle de 1885 ». Les journaux rapportèrent le procès et la condamnation qui s'ensuivirent, et Turing eut à supporter cette publicité.

La vie privée de Turing avait été étalée sur la place publique, et sa sexualité était connue de tous. Le gouvernement anglais lui retira sa carte des services de sécurité, et il ne fut plus autorisé à travailler sur les projets de recherches touchant à l'élaboration du calculateur programmable. Il fut tenu de consulter un psychiatre et dut subir un traitement hormonal qui le rendit obèse et impotent. Il s'enfonça de plus en plus dans la dépression au cours des deux années suivantes, et, le 7 juin 1954, il se retira dans sa chambre en emportant une pomme et un flacon de cyanure. Vingt ans plus tôt, il chantait l'air de la sorcière : « Dans la potion la pomme trempe, que s'insinue la mort dormante », et ce jour-là il trempa la pomme dans le cyanure et en avala quelques bouchées. À quarante-deux ans, l'un des plus grands cerveaux de la cryptanalyse mettait fin à ses jours.

La barrière de la langue

Au moment où, en brisant le chiffre d'Enigma, les décrypteurs anglais changeaient le cours de la guerre en Europe, leurs homologues américains jouaient un rôle tout aussi important dans les événements du Pacifique en réussissant à briser le chiffre de la machine japonaise baptisée *Purple*. En juin 1942, les Américains déchiffrèrent un message exposant un plan japonais pour attirer les forces navales américaines vers les îles Aléoutiennes en feignant une attaque, ce qui permettrait à la marine japonaise d'atteindre son objectif réel, l'île Midway. Bien que les bateaux américains eussent commencé à quitter Midway, ils ne s'en étaient guère éloignés et se tenaient prêts à y retourner dès que nécessaire. Aussi, lorsque les cryptanalystes interceptèrent et déchiffrèrent l'ordre japonais d'attaquer Midway, les bateaux purent se rabattre rapidement et défendre l'île au cours d'une des plus importantes batailles de toute la guerre. L'amiral Chester Nimitz déclara que la victoire des Américains à Midway « fut essentiellement une victoire du renseignement. Alors qu'ils croyaient créer la surprise, ce sont les Japonais qui furent surpris ».

Presque un an plus tard, les cryptanalystes américains découvrirent un message indiquant l'itinéraire prévu pour une visite aux îles Salomon que devait faire l'amiral Isoruko Yamamoto, commandant en chef de la flotte japonaise. Nimitz décida d'envoyer une escadrille aérienne pour intercepter l'avion de Yamamoto et l'abattre. Yamamoto était renommé pour son exactitude maniaque. Il approcha de sa destination à 8 heures précises, comme le programme intercepté l'annonçait, pour se trouver face à dix-huit avions de combat américains P-38. Ainsi disparut l'un des principaux chefs de guerre japonais.

Avant d'être finalement pénétrés, *Purple* et Enigma, les chiffres japonais et allemand, avaient longtemps offert une certaine sécurité, et avaient dressé devant les cryptanalystes alliés de vrais obstacles. En fait, si les machines à chiffrer avaient été utilisées avec toutes les précautions, sans messages répétés, sans *cillies*, sans restriction sur les connexions ou

sur les placements des rotors, et sans messages stéréotypés comportant des mots probables, il est fort possible que l'on n'en serait jamais venu à bout.

La véritable force et le potentiel de ces machines furent démontrés par la machine à chiffrer *Typex* (ou Type X) utilisée par les armées de terre et de l'air britanniques, et la machine SIGABA (ou M-143-C) utilisée par l'armée américaine. Ces deux machines étaient plus complexes que l'Enigma, et toutes deux furent utilisées avec toute la rigueur nécessaire et restèrent par conséquent inviolées. Les cryptanalystes alliés avaient confiance dans ces machines à chiffrer électromécaniques. Il serait faux toutefois de prétendre que seules des machines compliquées fournirent le moyen d'envoyer des messages tenus secrets. En fait, l'un des cryptages les plus performants utilisés pendant la Seconde Guerre mondiale fut aussi l'un des plus simples.

Durant la campagne du Pacifique, les officiers américains s'aperçurent que les machines à chiffrer, comme SIGABA, avaient un inconvénient fondamental. Si le cryptage électromécanique offrait une bonne protection, il était désespérément lent. Les messages devaient être entrés dans la machine lettre après lettre, le résultat devait être noté lettre après lettre, et le texte chiffré obtenu devait être transmis par un opérateur radio qui devait ensuite le passer à un déchiffreur, lequel sélectionnerait soigneusement la bonne clef, taperait le texte chiffré dans la machine, et obtiendrait enfin le déchiffrement lettre à lettre. Le temps et la place nécessaires à cette délicate opération ne posaient aucun problème dans un quartier général ou à bord d'un navire, mais le cryptage mécanique était moins adapté à des environnements plus hostiles, comme les îles du Pacifique, sièges de combats intensifs. Un correspondant de guerre décrit ainsi les difficultés rencontrées par les transmissions au cours d'une bataille dans la jungle : « Lorsque le théâtre des opérations se rétrécit, on doit pouvoir tout faire en une seconde. On n'a pas le temps de chiffrer et de déchiffrer (...) À de tels moments, l'anglais du roi devient votre dernier souci, on préfère le langage des rues. » Malheureusement pour les Américains, de nombreux soldats japonais avaient fréquenté des collèges américains et parlaient couramment l'anglais, y compris l'argot. L'information sur les plans tactiques des Américains tombait donc aux mains de l'ennemi.

Philip Johnston, un ingénieur installé à Los Angeles, fut l'un des premiers à se soucier de ce problème. Il était trop âgé pour le service actif, mais il désirait quand même participer à l'effort de guerre. Début

1942, il commença à formuler un cryptage inspiré de son expérience d'enfant. Fils d'un missionnaire protestant, Johnston avait grandi dans les réserves navajos en Arizona, et il s'était trouvé immergé dans leur culture. Il était l'un des seuls Blancs à parler leur langue, ce qui lui permettait de servir d'interprète lors des discussions entre les Navajos et les fonctionnaires américains. Cela le conduisit jusqu'à la Maison Blanche où, à l'âge de neuf ans, il traduisit les requêtes de deux Navajos venus demander au président un meilleur traitement pour leur communauté. Sachant l'extrême difficulté de cette langue, sa quasi-impénétrabilité pour des étrangers, Johnston eut l'idée que le navajo, ou une autre langue indienne, pourrait être utilisé comme un code pratiquement incompréhensible. Si chaque bataillon du Pacifique était doté d'une paire d'indigènes comme opérateurs radio, la sécurité des communications serait garantie. Il parla de son idée au lieutenant-colonel James E. Jones, officier des transmissions à Camp Elliott, juste à côté de San Diego. Quelques exemples de phrases en navajo suffirent à persuader l'officier médusé que l'idée méritait considération. Quinze jours plus tard, Johnston revint accompagné de deux Navajos, prêts à faire une démonstration aux officiers supérieurs des *marines*. Les deux Navajos furent séparés l'un de l'autre et l'on donna au premier six messages classiques en anglais, qu'il traduisit en navajo et transmit à son collègue par radio. Le destinataire navajo re-traduisit les messages en anglais, les nota et les remit aux officiers, qui les comparèrent aux originaux : le transit entre les deux Navajos n'avait entraîné aucune faute. Les officiers des *marines* autorisèrent un projet-pilote, et ordonnèrent qu'on commence le recrutement immédiatement.

Auparavant, le lieutenant-colonel Jones et Philip Johnston devaient décider s'ils mèneraient le projet-pilote avec les Navajos, ou s'ils choisiraient une autre tribu. Johnston avait employé des Navajos pour sa démonstration parce qu'il avait des liens personnels avec cette tribu, mais cela n'entraînait pas nécessairement que ce choix était idéal. Le critère de sélection le plus important était la question du nombre : les *marines* avaient besoin d'un nombre important d'hommes parlant et écrivant couramment l'anglais, or l'illettrisme régnait dans la plupart des réserves, et l'on ne retint finalement que les quatre tribus les plus nombreuses : les Navajos, les Sioux, les Chippewas et les Pima-Papagos.

Les Navajos formaient la tribu la plus importante mais aussi la plus illettrée, alors que les Pima-Papagos étaient les plus lettrés mais les

moins nombreux. Cela n'aidait pas beaucoup au choix, et la décision reposa finalement sur un autre facteur. Selon le rapport officiel :

Les Navajos composent la seule tribu à ne pas avoir été envahie d'étudiants allemands pendant les vingt dernières années. Ces Allemands, qui étudiaient les dialectes au titre d'étudiants en art, en anthropologie, etc., ont certainement acquis une bonne connaissance de tous les dialectes tribaux, le navajo excepté. Pour cette raison, cette tribu est la seule à offrir une totale sécurité pour le type d'opération envisagé. On doit aussi noter que le dialecte navajo est incompréhensible pour toutes les autres tribus et tous les autres peuples, à l'exception probable des vingt-huit Américains qui ont étudié ce dialecte. Il équivaut donc à un code secret en face de l'ennemi, et il est parfaitement adapté à une communication rapide et sûre.

Quand l'Amérique entra en guerre, les Navajos vivaient dans des conditions difficiles et ils étaient regardés comme une peuplade inférieure. Pourtant le conseil de la tribu soutint l'effort de guerre en toute loyauté. Les Navajos avaient même une telle envie de se battre que certains d'entre eux mentaient sur leur âge, s'empiffraient de bananes ou avalaient des bonbonnes d'eau pour atteindre le poids minimum fixé à cinquante-cinq kilos. De même, il n'y eut aucun problème pour trouver des candidats au poste de *Navajo code-talker* (parleur de code navajo), comme on les appela. Dans les quatre mois qui suivirent Pearl Harbour, vingt-neuf Navajos, dont certains n'avaient pas plus de quinze ans, suivirent un cours de transmissions avec les marines.



Fig. 52 Les 29 premiers *code-talkers* (parleurs-de-code) navajos posent pour la traditionnelle photographie de promotion.

Avant de commencer l'entraînement, le corps des marines devait résoudre un problème qui avait perturbé le seul autre code jamais basé sur une langue indigène américaine. Pendant la Première Guerre mondiale, dans le nord de la France, le capitaine E.W. Horner, de la compagnie D du 141^e d'infanterie, avait imaginé d'employer huit hommes de la tribu choctaw comme opérateurs radio. Évidemment, chez l'ennemi, personne ne comprenait leur langue et les Choctaws assuraient la sécurité des communications. Mais ce codage avait un défaut majeur, c'est que la langue choctaw n'offre pas d'équivalent au langage militaire moderne. Par conséquent, un message comportant un terme technique spécifique devait être traduit par une vague expression choctaw, ce qui entraînait un risque de mauvaise interprétation à l'arrivée.

Le même problème se posait avec le navajo, mais afin d'éviter les ambiguïtés, les marines décidèrent d'établir un lexique de mots navajos pour remplacer les termes anglais autrement impossibles à traduire. Les stagiaires aidèrent à rédiger le lexique, et ils incitèrent à choisir des mots propres au milieu naturel pour exprimer les termes spécifiquement militaires. Ainsi des noms d'oiseaux remplaçaient les types d'avion, et des poissons étaient substitués aux bateaux ([tableau 11](#)) :

Chasseur

Oiseau-mouche

Da-he-tih-hi

Avion d'observation	Chouette	<i>Ne-as-jah</i>
Avion d'assaut	Hirondelle	<i>Tas-chizzie</i>
Bombardier	Buse	<i>Jay-sho</i>
Bombardier en piqué	Faucon	<i>Gini</i>
Bombes	Œufs	<i>A-ye-shi</i>
Véhicule amphibie	Grenouille	<i>Chal</i>
Cuirassé	Baleine	<i>Lo-tso</i>
Destroyer	Requin	<i>Ca-lo</i>
Sous-marin	Poisson en fer	<i>Besh-lo</i>

Tableau 11 Noms de code navajos pour les avions et les bateaux.

Bien que le lexique fût fort de 274 mots, il restait le problème de la traduction de mots imprévus et des noms de personnes ou de lieux. On convint donc de créer un alphabet pour épeler les mots difficiles. Le mot *Pacific*, par exemple, serait épelé en anglais (Pig, Ant, Cat, Ice, Fox, Ice, Cat) et serait ensuite traduit en navajo, soit (Bi-sodih, Wol-la-chee, Moasi, Tkin, Ma-e, Tkin, Moasi). L'alphabet navajo complet comportait les mots suivants :

A	Ant	<i>Wol-la-chee</i>	Fourmi	N	Nut	<i>Nesh-chee</i>	Noisette
B	Bear	<i>Shush</i>	Ours	O	Owl	<i>Ne-ahs-jsh</i>	Chouette
C	Cat	<i>Moasi</i>	Chat	P	Pig	<i>Bi-sodih</i>	Cochon
D	Deer	<i>Be</i>	Daim	Q	Quiver	<i>Ca-yeilth</i>	Carquois
E	Elk	<i>Dzeh</i>	Élan	R	Rabbit	<i>Gah</i>	Lapin
F	Fox	<i>Ma-e</i>	Renard	S	Sheep	<i>Dibeh</i>	Mouton
G	Goat	<i>Klizzie</i>	Chèvre	T	Turkey	<i>Than-zie</i>	Dinde
H	Horse	<i>Lin</i>	Cheval	U	U te	<i>No-da-ih</i>	Peau-rouge
I	Ice	<i>Tkin</i>	Glace	V	Victor	<i>A-keh-di-glini</i>	Vainqueur
J	Jac kass	<i>Tkele-cho-gi</i>	Baudet	W	Weasel	<i>Gloe-ih</i>	Belette
K	Kid	<i>Klizzie-yazzi</i>	Chevreau	X	Cross	<i>Al-an-as-dzoh</i>	Croix
L	Lamb	<i>Dibeh-yazzi</i>	Agneau	Y	Yucca	<i>Tsah-as-zih</i>	Yucca
M	Mouse	<i>Na-as-tso-si</i>	Souris	Z	Zinc	<i>Besh-do-gliz</i>	Zinc

Tableau 12 Le code alphabétique navajo.

En six semaines, les stagiaires apprirent par cœur le lexique entier et l'alphabet, afin d'éviter d'avoir besoin de carnets de codes, qui risquent toujours de tomber aux mains de l'ennemi. Pour un Navajo, cet exercice de mémoire était banal, puisque leur langue n'avait pas de forme écrite et qu'ils étaient entraînés à mémoriser leurs légendes ou l'histoire de leurs familles. William McCabe, l'un des stagiaires, dit : « Chez un Navajo, tout est en mémoire, les chants, les prières, tout. C'est ainsi que nous avons été élevés. »

À la fin du stage, les Navajos furent soumis à un examen. Des expéditeurs traduisirent des séries de messages de l'anglais au navajo, les envoyèrent, et les récepteurs traduisirent les messages à nouveau en anglais, en utilisant, selon les cas, le lexique appris ou l'alphabet. Les résultats furent parfaits au mot près. Pour vérifier la force du système, on donna au service des renseignements de la marine un enregistrement des transmissions. Ce même service avait fait céder le chiffre japonais le plus résistant, Purple. Après trois semaines de cryptanalyse intense, les décrypteurs de la Navy restaient désarmés devant les messages. Ils dirent que la langue navajo était « une succession bizarre de sons gutturaux, nasaux, impossibles à prononcer (...) Nous ne pouvions même pas la transcrire, encore bien moins la décrypter. » Le code navajo fut jugé excellent. Deux soldats navajos, John Benally et Johnny Manuelito, furent retenus pour assurer la formation d'un nouveau groupe de recrues, alors que les vingt-sept autres étaient assignés à quatre régiments et envoyés dans le Pacifique.

Après l'attaque de Pearl Harbour le 7 décembre 1941, les Japonais s'étaient vite rendus maîtres de zones importantes dans le Pacifique. Leurs troupes battirent les Américains à Guam le 10 décembre. Le 13 décembre, elles prenaient Guadalcanal, l'une des îles Salomon. Hong-Kong capitula le 25 décembre et les troupes américaines aux Philippines se rendirent le 2 janvier 1942. Durant l'été suivant, les Japonais formèrent le projet de consolider leur contrôle du Pacifique en construisant un aéroport sur Guadalcanal, afin d'en faire une base pour leurs bombardiers. Leur but était de couper les voies d'approvisionnement alliées, afin de rendre toute contre-attaque impossible. L'amiral Ernest King, chef des opérations navales américaines, lança une attaque sur l'île avant que le terrain d'aviation soit terminé, et le 7 août, la 1^{re} division de marines prenait la tête de l'invasion de Guadalcanal. Le premier groupe de *parleurs-de-code* était compris dans les forces du débarquement.

Leurs premières tentatives semèrent d'abord une grande confusion. Nombre des opérateurs réguliers n'étaient pas prévenus de ce nouveau code, et ils envoyèrent des signaux angoissés à travers toute l'île, assurant que les Japonais émettaient sur les fréquences américaines. Le colonel responsable suspendit immédiatement les communications navajos jusqu'à ce qu'il soit lui-même convaincu que cela valait la peine de les reprendre. L'un des parleurs-de-code se souvient de la remise en service du code navajo :

Le colonel eut une idée. Il dit qu'il nous garderait à une condition : que je puisse faire mieux que son code blanc, un objet cylindrique à frappe mécanique. Nous avons envoyé des messages tous les deux, par le cylindre blanc et par ma voix. Nous avons ensuite tous les deux reçu des réponses et la compétition consistait à voir lequel aurait décodé ses réponses le premier. On me demanda : « Combien de temps cela vous prendra-t-il ? Deux heures ? — Plutôt deux minutes », répondis-je. L'autre type était encore en train de décoder lorsque je reçus le signal Roger (reçu et compris) en retour de mon message après environ quatre minutes et demie. je dis : « Colonel, quand est-ce que vous laissez tomber votre machin, votre cylindre ? » Il ne répondit rien, alluma simplement sa pipe et s'en alla.

Les Navajos prouvèrent leur valeur sur le champ de bataille. Au cours d'un épisode sur l'île Saipan, un bataillon de marines s'empara des positions jusque-là tenues par des soldats japonais qui se replièrent. Soudain, une salve éclata à proximité. Les marines étaient sous le feu d'autres Américains qui ignoraient leur progression. Ils revinrent à l'anglais pour expliquer leurs positions par radio, mais les tirs continuèrent, car les troupes américaines qui les attaquaient crurent que ces messages étaient émis par les Japonais pour les induire en erreur. Ce ne fut que lorsqu'un message navajo fut émis que les attaquants suspendirent leur assaut. Un message en navajo ne pouvait être un faux.

La réputation des parleurs-de-code ne cessa d'augmenter et, à la fin de 1942, on demanda 83 hommes de plus. Les Navajos étaient présents dans les six divisions du corps des marines, et furent parfois empruntés par d'autres forces américaines. Leur guerre des mots fit d'eux des héros. D'autres soldats se proposaient pour porter leurs radios ou leurs fusils, et on leur donna des gardes du corps, en partie pour les protéger de leurs propres camarades : en trois occasions au moins, certains furent pris pour des soldats japonais, et capturés par des Américains. On ne les relâcha que lorsque des collègues de leur propre bataillon se portèrent garants pour eux.

L'impénétrabilité du code navajo est due à l'appartenance du navajo à la famille des langues Na-Dene, qui n'a aucun lien avec une quelconque langue européenne ou asiatique. Un verbe, par exemple, n'est pas conjugué seulement en accord avec son sujet, mais aussi avec son complément d'objet. La terminaison du verbe dépend de la catégorie à laquelle appartient son complément d'objet : long (une pipe, un crayon), souple et flexible (un serpent, une lanière), granuleux (le sucre, les matières fécales). On incorpore aussi les adverbes dans le verbe, et on prend en compte si la personne qui parle a expérimenté elle-même ce qu'elle dit ou si elle ne l'a appris que par ouï-dire. Finalement, un simple verbe peut valoir toute une phrase, ce qui rend impossible, pour des étrangers, d'en saisir la signification.

Malgré ses points forts, le code navajo souffrait lui aussi de deux faiblesses importantes. D'abord, les mots qui ne figuraient ni dans le vocabulaire navajo, ni dans la liste des 274 mots de code autorisés, devaient être épelés selon l'alphabet spécial. Cela demandait du temps, aussi décida-t-on d'ajouter 234 mots nouveaux au lexique. Les nations, par exemple, se virent baptisées avec des surnoms navajos ; *Chapeau*

roulé pour l'Australie, *Ceinturée d'eau* pour l'Angleterre, *Cheveux nattés* pour la Chine, *Chapeau d'acier* pour l'Allemagne, *Terre flottante* pour les Philippines et *Mouton chagrin* pour l'Espagne.

Le deuxième problème concernait les mots à épeler. Si les Japonais les comprenaient, il leur serait possible d'utiliser l'analyse de fréquences pour identifier quels mots navajos étaient mis pour quelles lettres. Il deviendrait vite évident que le mot le plus utilisé était *dzeh*, l'élan, qui représente le e, la lettre de l'alphabet la plus utilisée en anglais (comme en français). Épeler simplement le nom de l'île Guadalcanal et répéter quatre fois le mot *wol-la-chee* offrirait une piste sérieuse pour trouver le mot représentant a. La solution était d'ajouter des mots comme substituts supplémentaires pour les lettres les plus courantes (des homophones). Deux mots supplémentaires furent introduits pour fournir une alternative à chacune des lettres les plus courantes (en anglais e, t, a, o, i, n) et un mot supplémentaire fut introduit pour chacune des six suivantes (s, h, r, d, l, u). Ainsi, la lettre a serait remplacée par les mots *be-la-santa* (apple) ou *tse-nihl* (axe). Guadalcanal, pourrait donc être épelée sans une seule répétition : *klizzie, shi-da, wol-la-chee, lha-cha-eh, be-la-sana, dibeh-yazzie, moasi, tse-nihl, nesh-chee, tse-nihl, ah-jad*.



Fig. 53 Le caporal Henry Bake Jr (à gauche) et le soldat de première classe George H. Kirk utilisant le code navajo dans la jungle de Bougainville en 1943.

À mesure que la guerre s'intensifiait dans le Pacifique, et que les Américains progressaient des îles Salomon vers Okinawa, les Navajos jouaient un rôle de plus en plus prépondérant. Pendant les premiers jours de l'attaque sur Iwo-Jima, plus de huit cents messages furent envoyés sans une seule erreur. Selon le major général Howard Conner : « Sans les Navajos, les marines n'auraient jamais pris Iwo-Jima. » Leur contribution est encore plus remarquable si l'on considère que, pour remplir leur devoir, ils devaient souvent surmonter des peurs ancestrales ancrées profondément dans leurs esprits. Les Navajos croyaient que les esprits des morts, *chindi*, revenaient se venger sur les vivants si les rites traditionnels n'étaient pas respectés sur leurs cadavres. La guerre dans le Pacifique était particulièrement sanglante, avec des corps jonchant les champs de bataille, et cependant les Navajos trouvèrent le courage de continuer leur mission, en dépit des *chindi* qui les hantaient. Dans le livre de Doris Paul, *The Navajo Code-Talkers*, l'un des Navajos rapporte un incident qui montre leur bravoure, leur dévouement et leur sang-froid :

Le feu était si dense que si vous leviez la tête de deux centimètres vous étiez mort. Aussi, aux petites heures de l'aube, sans relâchement de leur part ou de la nôtre, nous restions immobiles, comme morts. La tension devint telle qu'un Japonais ne put plus la supporter. Il se leva et hurla, criant de sa voix la plus aiguë, et il s'élança vers notre tranchée en brandissant un long sabre de samouraï. Je pense qu'il fut touché 25 à 40 fois avant de tomber.

J'avais un copain avec moi dans la tranchée. Ce Japonais lui avait tranché la gorge jusqu'aux cordes vocales à l'arrière du cou. Il haletait encore par la trachée. Et le bruit qu'il faisait pour essayer de respirer était affreux. Il mourut, bien sûr. Quand le Japonais l'avait frappé, son sang chaud s'était répandu sur ma main qui tenait un microphone. J'étais en train de coder un appel à l'aide. On m'a dit que, en dépit de ce qui se passa, chaque syllabe de mon message parvint à destination.

En tout, 420 Navajos étaient employés au code. Bien que leur bravoure au combat fût reconnue, leur rôle particulier pour la sécurité des communications était un secret militaire. Le gouvernement leur

interdit de parler de leur travail et leur contribution exceptionnelle fut oubliée. Tout comme Turing et les cryptanalystes de Bletchley Park, les Navajos furent ignorés pendant des décennies. Ce n'est qu'en 1968 que le code navajo fut libéré du secret et, l'année suivante, les parleurs-de-code se retrouvèrent pour la première fois. Puis, en 1982, le gouvernement américain institua en leur honneur, à la date du 14 août, la journée nationale des parleurs-de-code navajos. Le plus grand hommage qu'on puisse leur rendre est de rappeler que c'est l'un des rares codes de l'histoire à n'avoir jamais été brisé. Le lieutenant-général Seizo Arisue, chef des renseignements japonais, reconnut que, s'ils avaient percé le code de l'American Air Force, ils n'avaient jamais trouvé la moindre faille dans le code navajo.

Déchiffrer des langues disparues et des écritures anciennes

Le succès du code navajo était essentiellement fondé sur le fait que la langue maternelle d'une personne peut être absolument incompréhensible pour quelqu'un à qui elle n'est pas familière. Par beaucoup de côtés, la tâche des cryptanalystes japonais s'apparentait à celle des archéologues tentant de déchiffrer une langue depuis longtemps oubliée, écrite dans une écriture disparue. La gageure est cependant beaucoup plus difficile à relever dans le cas des archéologues. Les Japonais voyaient passer un flot continu de mots navajos qu'ils pouvaient tenter d'identifier. Les archéologues, eux, ne disposent que de quelques tablettes d'argile, et n'ont souvent aucune idée du contexte ni du contenu du texte ancien, indices qui aident notablement les décrypteurs militaires à briser un chiffre.

Déchiffrer des textes anciens semble une démarche presque sans espoir, et cependant nombre d'hommes et de femmes se sont consacrés à cette tâche ardue, animés par le désir de comprendre les écrits de nos ancêtres, de nous permettre de prononcer leurs mots et d'avoir un reflet de leurs pensées. Cette soif de comprendre les écritures anciennes est très bien résumée par Maurice Pope, auteur de *l'Histoire du déchiffrement* : « Mener à bien un déchiffrement est de loin la réussite la plus éclatante qu'on puisse obtenir par ces recherches. Il y a une part de magie dans une écriture inconnue, surtout lorsqu'elle appartient à un passé reculé, ce qui explique la gloire qui auréolera la première personne à dissiper son mystère. »

À strictement parler, le déchiffrement des écrits anciens n'est pas partie prenante dans la permanente bataille entre concepteurs de codes et décrypteurs puisque, si les archéologues jouent le rôle des décrypteurs, il n'y a pas de codeurs en face d'eux. Dans la plupart des cas, le scribe n'avait pas, à l'origine, l'intention de dissimuler le sens de son texte. Aussi le reste de ce chapitre, qui traite de travaux archéologiques, constitue-t-il un petit détour, à l'écart du thème principal de ce livre. Toutefois les principes sont à peu près les mêmes que ceux de la cryptanalyse militaire conventionnelle. D'ailleurs, de nombreux décrypteurs ont eu envie de relever le défi posé par les écrits anciens. Il

est vrai que les textes anciens distraient de la cryptanalyse militaire en présentant une énigme purement intellectuelle, sans enjeu immédiat. La motivation est davantage la curiosité que l'animosité.

Le plus célèbre et le plus romanesque de tous les déchiffrements fut sans doute celui des hiéroglyphes. Pendant des siècles, ceux-ci avaient gardé leur mystère, et l'on ne pouvait que spéculer sur leur signification.

Les plus anciens hiéroglyphes remontent à 3000 avant J.-C., et cette forme d'écriture dessinée se perpétua pendant trente-cinq siècles. Si les symboles élaborés des hiéroglyphes étaient parfaits pour orner les murs de temples majestueux (le mot grec *hieroglyphika* signifie *gravure sacrée*), ils étaient beaucoup trop compliqués pour servir à des échanges banals. D'où le développement, parallèlement aux hiéroglyphes, de l'écriture *hiératique*, une forme simplifiée pour la vie quotidienne, dans laquelle chaque symbole était remplacé par une représentation stylisée, plus facile et plus rapide à écrire. En 600 avant J.-C., l'écriture hiératique fait place à une écriture encore plus simple, le *démotique*, du grec *demotika* (populaire), dont le nom reflète parfaitement la fonction. Les hiéroglyphes, l'écriture hiératique et le démotique étaient de la même essence et on peut presque les considérer comme différentes moutures de la même langue.

Ces trois formes d'écriture sont phonétiques, ce qui veut dire que les caractères représentent des sons distincts, tout comme les lettres de notre alphabet. Pendant plus de trois mille ans, les Égyptiens employèrent ces écritures dans toutes les activités de la vie, comme nous utilisons l'écriture aujourd'hui. Puis, en une génération, vers la fin du IV^e siècle, les écritures égyptiennes disparurent. Les exemples les plus tardifs furent trouvés dans l'île de Philae. Une inscription en hiéroglyphes avait été gravée sur un temple en 394 avant J.-C., et des traces de graffiti en démotique ont été datées de 450 avant J.-C. L'expansion de la religion chrétienne fut responsable de l'extinction de ces écritures, dont elle interdit l'usage afin d'éradiquer tout lien avec le passé païen de l'Égypte. Les écritures anciennes furent remplacées par le *copte*, qui utilisait vingt-quatre lettres de l'alphabet grec et six caractères démotiques pour traduire les sons qui n'existaient pas en grec. La domination du copte fut si complète que la capacité même de lire les hiéroglyphes et les écritures démotique et hiératique se perdit. On continua à parler l'égyptien ancien, qui peu à peu se transforma en ce qu'on appela la langue copte, mais au bout du compte le copte parlé et écrit recula devant la montée de l'arabe

au XI^e siècle. Le lien linguistique avec les antiques royaumes d'Égypte avait été brisé, et les connaissances nécessaires pour lire les récits des pharaons étaient perdues.

L'intérêt pour les hiéroglyphes se réveilla au XVII^e siècle, lorsque le pape Sixte V dessina dans la ville de Rome un nouveau réseau de rues, et érigea des obélisques égyptiens à chaque carrefour. Des érudits tentèrent de percer le sens de leurs hiéroglyphes mais en furent empêchés par une présomption fausse. Personne n'était prêt à admettre que les hiéroglyphes pouvaient être des caractères phonétiques, ou *phonogrammes*, en particulier parce que l'idée d'un alphabet phonétique semblait trop complexe pour une si ancienne civilisation. Les savants de l'époque étaient persuadés que les hiéroglyphes étaient des *idéogrammes*. Pour eux, ces caractères compliqués représentaient des concepts, et n'étaient rien de plus qu'une représentation picturale primitive.

Cette idée était déjà répandue chez les étrangers qui visitaient l'Égypte à l'époque où les hiéroglyphes étaient encore une écriture en usage. Diodore de Sicile, historien grec du I^{er} siècle avant J.-C., écrivait :

Il arrive que les figures des lettres égyptiennes prennent la forme de toutes sortes de créatures vivantes et des extrémités du corps humain et d'outils (...) car leur écriture n'exprime pas les concepts en combinant des syllabes l'une avec l'autre mais en montrant l'apparence extérieure de ce qu'on veut évoquer et grâce au sens métaphorique imprimé dans les mémoires par l'usage... Ainsi le faucon symbolise pour eux tout ce qui arrive rapidement, puisque cette créature est parmi les plus prompts des animaux ailés. Et l'idée est étendue, par le transfert métaphorique approprié, à toutes les choses rapides et aux choses dont la vitesse est la marque propre.

Il n'est pas surprenant que, en se fondant sur de telles déclarations, les savants du XVII^e siècle aient cherché à déchiffrer les hiéroglyphes en associant un concept à chacun d'eux. En 1652, le jésuite allemand Athanasius Kircher publia un dictionnaire des interprétations allégoriques intitulé *Œdipus aegyptiacus* et l'appliqua à des séries de

traductions intrigantes et merveilleuses. Voici comment il traduisait quelques hiéroglyphes, dont nous savons maintenant qu'ils représentent simplement le nom du pharaon Apriès : « Les bienfaits du divin Osiris seront sollicités par les cérémonies sacrées et par la chaîne des Génies, afin d'obtenir les bénédictions du Nil. » Aujourd'hui les traductions de Kircher semblent ridicules, mais leur impact sur les autres candidats au déchiffrement fut considérable, car Kircher n'était pas seulement égyptologue : il a écrit un livre de cryptographie, construit une fontaine musicale, inventé la lanterne magique (l'ancêtre du cinéma) et il est descendu dans le cratère du Vésuve, gagnant ainsi le titre de *père de la vulcanologie*. Il était considéré et salué comme le plus grand savant de son époque et l'on comprend que ses idées aient pesé sur des générations d'égyptologues.

Un siècle et demi après Kircher, pendant l'été 1798, les antiquités égyptiennes furent à nouveau au centre de l'actualité. Napoléon Bonaparte avait emmené en Égypte, dans les bagages de son armée d'invasion, une équipe de scientifiques, d'historiens et de dessinateurs. Ces chercheurs effectuèrent un travail remarquable, dressant des cartes, dessinant, transcrivant, mesurant et enregistrant tout ce qu'ils voyaient. En 1799, les savants français furent confrontés à ce qui allait devenir la dalle de pierre la plus célèbre de l'histoire de l'archéologie, et qui avait été mise à jour par des soldats français stationnés au fort Saint-Julien, près de la ville de Rosette située dans le delta du Nil. On avait chargé ces hommes de démolir un vieux mur pour agrandir le fort, mais, enchâssée dans le mur, il y avait une pierre portant une exceptionnelle suite d'inscriptions : le même texte avait été gravé trois fois, en grec, en démotique et en hiéroglyphes. La Pierre de Rosette semblait offrir des mots probables, comparables à ceux qui aidèrent les décrypteurs d'Enigma à Bletchley Park. On pouvait facilement lire le grec, et cela donnait un morceau de texte clair à rapprocher des textes chiffrés par le démotique et les hiéroglyphes. La Pierre de Rosette était une clef potentielle pour retrouver la signification des symboles de l'Égypte ancienne.

Les savants comprirent immédiatement l'importance de la pierre, et ils l'envoyèrent pour examen à l'Institut national du Caire. Mais, avant que l'Institut ait pu entamer des recherches sérieuses, il devint évident que l'armée française allait devoir reculer devant les forces anglaises. Les Français emportèrent la Pierre de Rosette du Caire à Alexandrie, où elle serait plus en sûreté. Ils durent finalement capituler, et l'article XVI du

traité attribua toutes les antiquités d'Alexandrie aux Anglais, alors que celles du Caire furent autorisées à partir pour la France. En 1802, l'incalculable dalle de basalte noir (mesurant 118 cm de haut, 77 cm de large, et 30 cm d'épaisseur et pesant 750 kilos) fut envoyée à Portsmouth à bord du HMS *l'Egyptienne*, et fut déposée au British Museum, à Londres, où elle se trouve toujours.

La traduction du grec révéla bientôt que la Pierre de Rosette portait un décret du conseil général des prêtres égyptiens formulé en 196 avant J.-C. Le texte rappelait les bienfaits que le pharaon Ptolémée avait répandus sur le peuple d'Égypte, et détaillait les honneurs dont les prêtres avaient, en retour, couvert le pharaon. Ils déclaraient par exemple qu'une fête serait consacrée au roi Ptolémée, l'immortel, l'aimé de Ptah, le dieu éclatant et bienfaisant, chaque année dans tout le pays à partir du premier jour de Troth et pendant cinq jours, où l'on porterait des guirlandes, pratiquerait des sacrifices et des libations, et tous les hommages habituels.

Si l'on suppose que les deux autres écrits représentent le même texte, on peut penser que le déchiffrement des hiéroglyphes et du démotique se fit sans difficulté. Pourtant, il restait trois obstacles importants. D'abord la Pierre de Rosette est sérieusement endommagée, comme le montre la [figure 54](#). Le texte grec couvre 54 lignes, dont 26 sont abîmées ; le démotique 32 lignes dont 14 ont le début endommagé (le démotique et les hiéroglyphes s'écrivent de la droite vers la gauche). Mais c'est le texte des hiéroglyphes qui est dans le plus mauvais état, avec la moitié des lignes manquant tout à fait et une partie des 14 autres qui manque aussi. Autre difficulté : les deux écrits égyptiens transcrivaient la langue de l'ancienne Égypte, que personne n'avait parlée depuis au moins huit siècles. On pouvait trouver une bribe de symboles égyptiens qui correspondrait à une bribe du texte grec, ce qui permettrait aux archéologues de comprendre le sens des symboles égyptiens, mais il était impossible de connaître le son des mots égyptiens. Or, si les archéologues ne savaient pas comment les mots étaient prononcés, ils ne pouvaient pas déduire la phonétique des symboles. Finalement, le legs de Kircher encourageait toujours les archéologues à penser l'écriture égyptienne en termes d'idéogrammes, plus que de phonogrammes, et seules quelques rares chercheurs tentèrent ce déchiffrement phonétique.

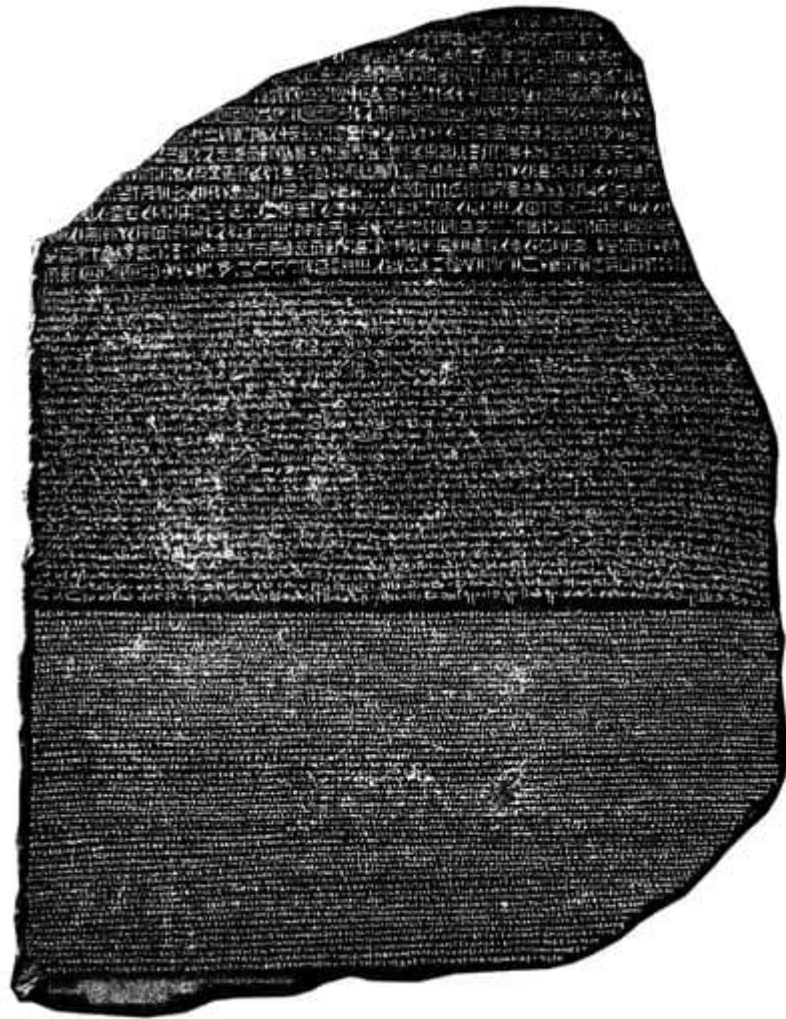
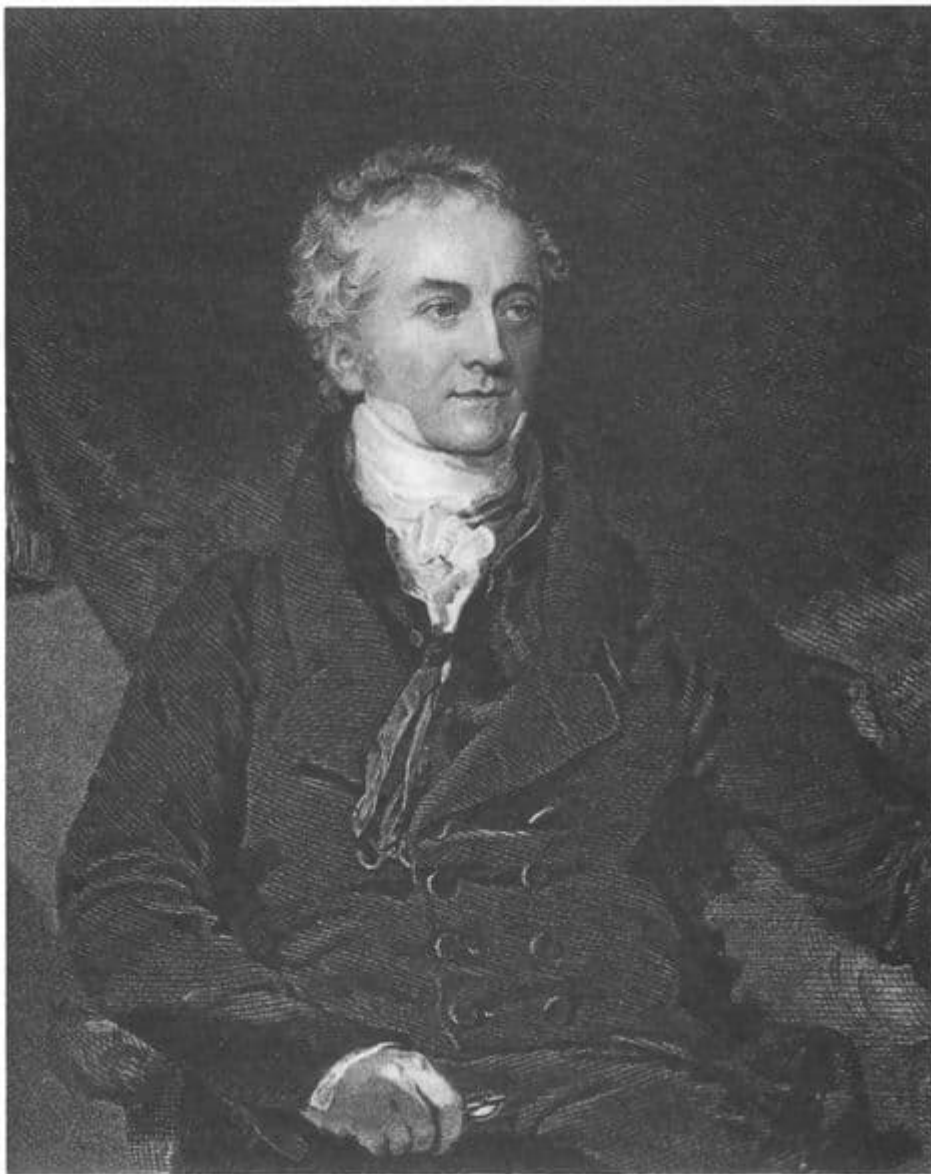


Fig. 54 La Pierre de Rosette, gravée en 196 avant J.-C. et retrouvée en 1799, porte le même texte en trois écritures différentes : hiéroglyphes en haut, démotique au centre et grec en bas.

L'un des premiers érudits à mettre en doute le préjugé qui identifiait les hiéroglyphes à une écriture picturale fut l'Anglais Thomas Young. Né en 1773 à Milverton, dans le Somerset, Young savait lire à l'âge de deux ans et, à quatorze ans, il avait étudié le grec, le latin, le français, l'italien, l'hébreu, le chaldéen, le syriaque, le samaritain, l'arabe, le turc et l'éthiopien. Quand il entra à l'Emmanuel College à Cambridge, il se montra si brillant qu'on le surnomma « le phénomène Young ». Il étudia la médecine, mais on disait qu'il ne s'intéressait qu'aux maladies, pas aux malades. Aussi se consacra-t-il de plus en plus à la recherche.

Young conduisit une étonnante série d'expériences de physiologie autour du fonctionnement de l'œil. Il découvrit que la perception de la couleur est le résultat de trois récepteurs indépendants, chacun sensible à l'une des trois couleurs primaires. Ensuite, en plaçant des cercles de métal autour d'un globe oculaire vivant, il démontra que la focalisation

ne demandait pas une distorsion de la totalité de l'œil, et postula que c'était le cristallin qui faisait le travail. Son intérêt pour l'optique l'entraîna vers la physique, et vers une autre série de découvertes. Il publia *La Théorie ondulatoire de la lumière*, un classique sur la nature de la lumière ; il donna une nouvelle et meilleure explication des marées ; il définit le concept d'énergie et publia des articles qui renouvelaient le sujet de l'élasticité. Young semblait capable de s'attaquer à presque tous les domaines, mais cela n'était pas entièrement en sa faveur. Son esprit était si facilement captivé qu'il sautait d'un sujet à l'autre, et s'embarquait sur un nouveau problème avant d'en avoir terminé avec le précédent.

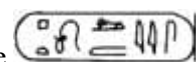


[Fig. 55](#) Thomas Young.

Quand Young entendit parler de la Pierre de Rosette, il se jura de relever ce défi. En 1814, passant ses vacances d'été dans la station balnéaire de Worthing, il emporta la copie des trois inscriptions, et c'est alors qu'il eut l'idée de concentrer son étude sur les signes entourés d'une boucle, qu'on appelle un *cartouche*. Il avait le pressentiment que si ces hiéroglyphes étaient ainsi mis en valeur, c'est qu'ils représentaient quelque chose de particulièrement important, peut-être le nom du pharaon Ptolémée, dont le nom grec, Ptolemaios, était mentionné dans le texte grec. Si c'était le cas, cela permettrait à Young de saisir les valeurs phonétiques des hiéroglyphes correspondants, puisque le nom d'un pharaon devait être prononcé à peu près de la même manière quelle que soit la langue. Le cartouche de Ptolémée est répété six fois sur la Pierre de Rosette, quelquefois dans une version dite « standard », et quelquefois dans une version plus longue et plus élaborée. Young supposa que la version longue contenait le nom de Ptolémée suivi de ses titres. Portant son attention sur les symboles apparaissant dans la version standard, il essaya d'en établir les valeurs phonétiques ([tableau 13](#)).

Hiéroglyphe	Valeur attribuée par Young	Valeur réelle
	p	p
	t	t
	indéterminé	o
	lo ou ole	l
	ma ou m	m
	i	i ou y
	osh ou os	s

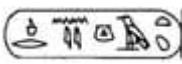
[Tableau 13](#) Déchiffrement par Young du cartouche de la Pierre de Rosette
Ptolémée (version standard).



Il l'ignorait à l'époque, mais Young avait bien attribué à la plupart des hiéroglyphes leur valeur phonétique exacte. Par chance, il avait placé les deux premiers hiéroglyphes (le petit carré □ et le demi-cercle ◐ qui figurent l'un au-dessus de l'autre, dans le bon ordre, par rapport à leur équivalent phonétique. Le scribe avait disposé les hiéroglyphes de cette manière pour des raisons esthétiques, aux dépens de la clarté phonétique. Les scribes aimaient éviter les blancs et que la disposition des hiéroglyphes soit harmonieuse. Dans certains cas, ils répartissaient les lettres sans lien aucun avec une quelconque orthographe phonétique, simplement pour embellir une inscription.

Juste après ce déchiffrement, Young découvrit un cartouche sur la reproduction d'une inscription du temple de Karnak à Thèbes, qu'il soupçonna être le nom de la reine Bérénice, de la famille des Ptolémée. Il lui appliqua la même méthode ([Tableau 14](#)).

Hiéroglyphe	Valeur attribuée par Young	Valeur réelle
	bir	b
	e	r
	n	n
	i	i
	indéterminée	k
	ke ou ken	a
	terminaison au féminin	terminaison au féminin

[Tableau 14](#) Déchiffrement par Young de , cartouche de Bérénice du temple de Karnak.

Des treize hiéroglyphes composant les deux cartouches, Young en avait identifié la moitié parfaitement, et avait presque réussi pour un

autre quart. Il avait aussi repéré exactement le symbole déterminant le féminin, placé après les noms des reines ou des déesses. En particulier, l'apparition du hiéroglyphe *deux plumes*  dans les deux cartouches, mis pour i dans les deux cas, aurait dû prouver à Young qu'il était sur la bonne piste et l'encourager à poursuivre. Pourtant, il suspendit brutalement ses travaux. Les arguments de Kircher pour une interprétation des hiéroglyphes comme idéogrammes semblent avoir lourdement pesé sur Young, et il n'était pas préparé à s'opposer à ce paradigme. Il expliqua ses propres découvertes phonétiques par l'origine de la dynastie des Ptolémée qui descendait de Lagos, un général d'Alexandre le Grand. Autrement dit, les Ptolémée étaient des étrangers, et Young supposait que leurs noms avaient été épelés phonétiquement parce qu'ils ne répondaient pas à un simple idéogramme de la liste des hiéroglyphes. Il résuma sa pensée en comparant les hiéroglyphes aux caractères chinois, sur lesquels les Européens commençaient à se pencher :

Il est extrêmement intéressant de refaire le chemin par lequel l'écriture alphabétique a découlé de l'écriture hiéroglyphique ; un processus qui peut dans une certaine mesure être illustré par la manière dont le chinois moderne exprime une combinaison étrangère de sons, les caractères étant rendus phonétiques par une simple marque appropriée, au lieu de garder leur habituelle signification ; cette marque, dans l'impression de certains livres, ressemblant beaucoup à l'anneau entourant les noms hiéroglyphiques.

Young commenta ses activités en les qualifiant de « distraction de quelques heures de loisir ». Il se désintéressa des hiéroglyphes et mit une conclusion à ses travaux en les exposant dans un article pour l'édition de 1819 du *Supplément à l'Encyclopedia Britannica*.

À la même époque, en France, un jeune linguiste, Jean-François Champollion, était prêt à mener les idées de Young jusqu'à leur conclusion naturelle. Bien qu'âgé de moins de trente ans, Champollion se passionnait pour les hiéroglyphes depuis bientôt vingt ans. Cette passion était née en 1800, après une visite chez le mathématicien Jean-

Baptiste Fourier, qui avait été l'un des savants emmenés en Égypte par Napoléon. Fourier lui montra sa collection d'antiquités égyptiennes, dont beaucoup portaient des inscriptions bizarres, et il lui expliqua que personne ne savait traduire cette écriture. Sur quoi le jeune garçon promit, du haut de ses dix ans, qu'il résoudrait un jour ce mystère. À dix-sept ans, il publiait un article intitulé *L'Égypte sous les pharaons*, tellement novateur qu'il fut immédiatement nommé professeur à l'académie de Grenoble. Lorsqu'il apprit qu'il obtenait un tel poste à son âge, Champollion fut si bouleversé qu'il s'évanouit.

Champollion continua à stupéfier ses pairs, maîtrisant le latin, le grec, l'hébreu, l'éthiopien, le sanscrit, le pehlvi, le syrien, le chaldéen, l'arabe, le persan, le chinois et le zend, afin de posséder les armes nécessaires pour donner l'assaut aux hiéroglyphes. Un jour de 1808, il rencontra dans la rue l'un de ses vieux amis qui lui apprit que le célèbre égyptologue Alexandre Lenoir venait de publier un déchiffrement complet des hiéroglyphes. Champollion en fut tellement affecté qu'il s'effondra sur le trottoir ; il semble qu'il avait l'évanouissement facile. Toute sa raison de vivre consistait à être le premier qui lirait les écritures des anciens Égyptiens. Heureusement pour lui, les déchiffrements de Lenoir étaient aussi fantaisistes que ceux de Kircher, et la course restait ouverte.

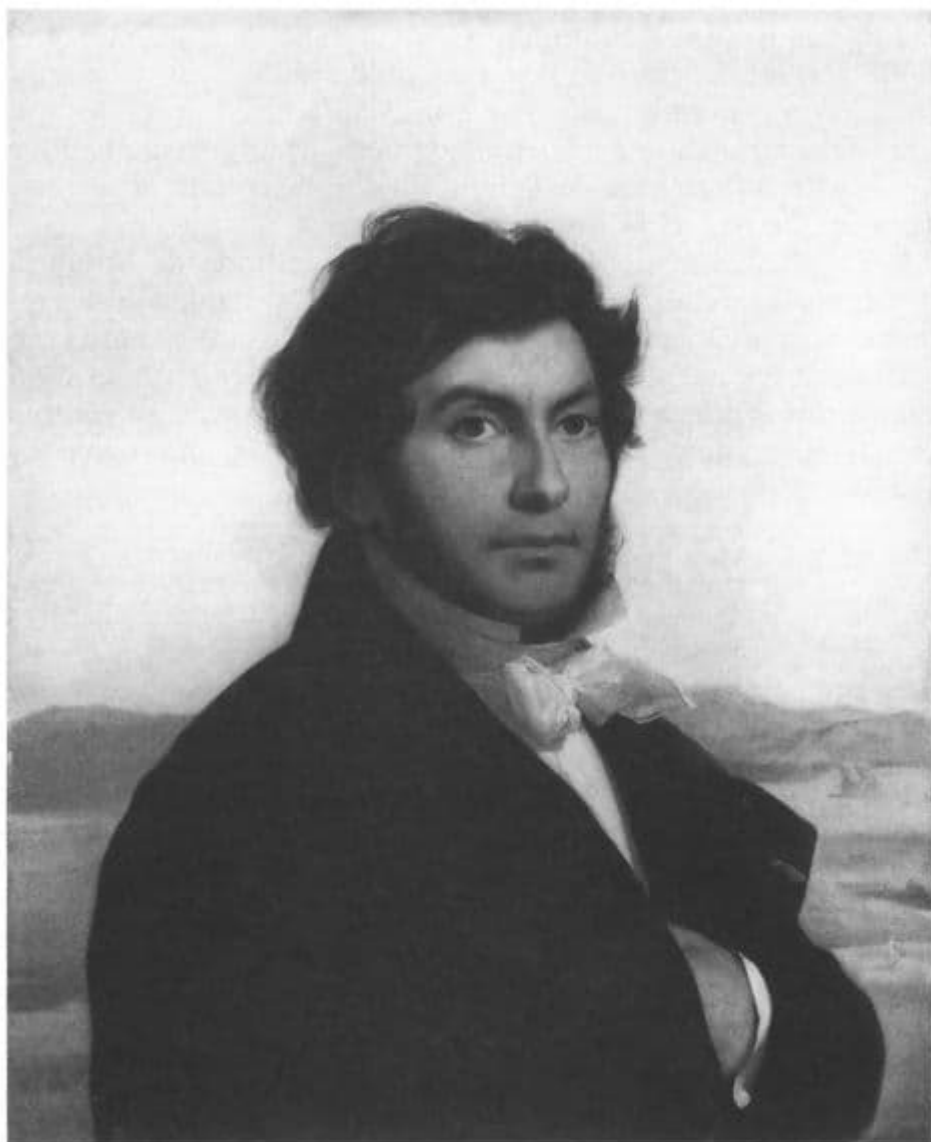


Fig. 56 Jean-François Champollion.

En 1822, Champollion appliqua la méthode de Young à d'autres cartouches. Le naturaliste anglais W.J. Banks avait rapporté dans le Dorset un obélisque portant des inscriptions qui incluaient les cartouches de Ptolémée et de Cléopâtre, et il en publia des lithographies. Champollion s'en procura une copie et assigna des valeurs phonétiques aux hiéroglyphes ([tableau 15](#)).

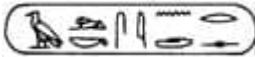
Hiéroglyphe	Valeur phonétique	Hiéroglyphe	Valeur phonétique
	p		c
	t		l
	o		e
	l		o
	m		p
	e		a
	s		t
			r
			a

Tableau 15 Déchiffrement par Champollion des cartouches de Ptolémée et Cléopâtre sur l'obélisque de Bankes.

Les lettres p, t, o, l et e sont communes aux deux cartouches ; dans quatre cas, elles incarnent le même son à la fois dans Ptolémée et Cléopâtre, et dans un seul cas, t, il y a une différence. Champollion supposa que le son t pouvait être représenté par deux symboles, exactement comme le son du c dur en français peut-être engendré par c ou k, comme dans « culture » et « kilo ». Encouragé par sa réussite, Champollion commença à s'attaquer à des cartouches portant une inscription dans une seule langue, et chaque fois que c'était possible il substitua aux hiéroglyphes les valeurs phonétiques qu'il avait déduites des cartouches de Ptolémée et de Cléopâtre. Son premier cartouche mystérieux ([tableau 16](#)) portait l'un des noms les plus célèbres de l'Antiquité.

Hiéroglyphe	Valeur phonétique
	a
	l
	?
	s
	e

	?
	t
	r
	?

Tableau 16 Déchiffrement par Champollion du cartouche  de Alksentrs (Alexandre).

Il sembla évident à Champollion que le cartouche (a-l- ?-s-e- ?-t-r- ?) représentait le nom *alksentrs* — Alexandre en grec. Champollion jugea aussi que les scribes n'aimaient pas utiliser les voyelles, et les omettaient souvent ; on supposait que le lecteur n'aurait aucun problème pour deviner les voyelles manquantes. Avec deux hiéroglyphes de plus à son actif, le jeune savant étudia d'autres inscriptions, et déchiffra une série de cartouches. En fait, ce travail ne faisait que poursuivre celui de Young. Tous ces noms — Alexandre, Cléopâtre — étaient des noms étrangers, ce qui renforçait la théorie d'une utilisation des phonétiques réservée aux mots ne figurant pas dans le lexique égyptien usuel.

Le 14 septembre 1822, Champollion reçut des reliefs provenant du temple d'Abou Simbel qui comportaient des cartouches antérieurs à la période de domination gréco-romaine, et donc assez anciens pour contenir des noms traditionnels égyptiens. Et pourtant ceux-ci étaient épelés, ce qui rendait évident que ce traitement n'était pas réservé aux noms étrangers. Champollion se concentra sur un cartouche ne portant que quatre hiéroglyphes . Les deux premiers symboles étaient inconnus, mais celui qui était répété à la fin  *crosses de deux bergers*, figurait déjà dans le cartouche d'Alexandre (*alksentrs*) et l'on savait depuis son déchiffrement qu'il représentait le s. Le cartouche signifiait donc (?- ?-s-s). À ce moment-là, Champollion fit appel à son vaste savoir linguistique. La langue copte, qui avait succédé à la langue égyptienne antique, avait cessé d'être une langue vivante au XI^e siècle. Mais elle était restée en usage, sous une forme figée, dans la liturgie de l'Église chrétienne copte. Champollion avait appris le copte pendant son adolescence, et le maîtrisait si bien qu'il s'en servait dans son journal intime. Jusque-là, pourtant, il n'avait jamais envisagé que le copte pût

être la langue des hiéroglyphes.

Champollion se demanda si le premier signe du cartouche, le disque ☉, n'était pas un idéogramme représentant le soleil, autrement dit une image du soleil utilisée comme symbole pour le mot *soleil*. Par pure intuition, il supposa que l'idéogramme était là pour évoquer le son du mot copte pour soleil, *ra*. Cela donnait la suite (ra- ?-s-s). Un seul nom de pharaon pouvait convenir. En tenant compte de l'agaçante suppression des voyelles et en imaginant que la lettre manquante était m, on avait là le nom de Ramsès, l'un des plus grands pharaons et l'un des plus anciens. Ainsi, le voile était levé. Même les noms traditionnels de l'Antiquité étaient épelés phonétiquement. Champollion surgit dans le bureau de son frère en criant « *Je tiens l'affaire* » mais, une fois encore, il fut terrassé par sa passion pour les hiéroglyphes. Il s'effondra sur place, et dut garder le lit pendant cinq jours.

Champollion avait démontré que les scribes appliquaient parfois le principe du rébus. Le rébus impose de découper des mots selon leurs composants phonétiques, et d'illustrer ensuite ces composants par des idéogrammes. Prenons le mot *cerfeuil*, il peut être coupé en deux syllabes, *cer-feuil*, réécrites *cerf-feuille*. Au lieu d'écrire le mot à l'aide des lettres de l'alphabet, on le représentera par l'image d'un cerf suivie de l'image d'une feuille. Dans l'exemple découvert par Champollion, seule la première syllabe(*ra*) est remplacée par une image de rébus, le dessin du soleil, tandis que le reste du mot est épelé plus conventionnellement.

La portée de l'idéogramme du cartouche de Ramsès est considérable car elle restreint le champ des interrogations sur la langue qu'utilisaient les scribes. Ils ne pouvaient pas avoir parlé grec, car alors le cartouche aurait été prononcé *Heliosmeses*. Le cartouche n'avait de sens que si les scribes parlaient une forme du copte, qui attribuait au cartouche la prononciation *Ra-meses*.

Certes, ce n'était là qu'un cartouche de plus, mais son déchiffrement illustre clairement les quatre principes fondamentaux communs à tous les hiéroglyphes. Premièrement, la langue dans laquelle le texte est écrit est plus ou moins proche du copte, et, à vrai dire, l'examen d'autres hiéroglyphes montra que c'était purement et simplement du copte. Deuxièmement, les idéogrammes servent à représenter certains mots, comme le mot *soleil* figuré par une simple image du soleil. Troisièmement, quelques mots longs sont bâtis complètement ou en partie suivant le principe du rébus. Enfin, pour la plupart de leurs écrits,

les scribes usaient d'un alphabet phonétique plus ou moins conventionnel. Ce dernier point est le plus important et Champollion qualifia les phonétiques d'*âme* des hiéroglyphes.

Grâce à sa profonde connaissance du copte, Champollion se mit à déchiffrer sans frein des hiéroglyphes en dehors des cartouches et, en deux ans, il avait atteint son but. Il avait identifié les valeurs phonétiques de la majorité des hiéroglyphes et découvert que certains d'entre eux représentaient une combinaison de deux ou même de trois consonnes. Cela permettait aux scribes d'avoir le choix entre une suite de hiéroglyphes simples et un seul hiéroglyphe exprimant plusieurs consonnes.

Champollion envoya communication de ses résultats dans une lettre à M. Dacier, secrétaire perpétuel de l'Académie des inscriptions et belles-lettres. Puis, en 1824, à trente-quatre ans, il publia l'ensemble de ses travaux dans un livre intitulé *Précis du système hiéroglyphique*. Pour la première fois depuis quatorze siècles, on pouvait lire l'histoire des pharaons comme leurs scribes l'avaient écrite. Pour les linguistes, il y avait là une occasion d'étudier l'évolution d'une langue, et de sa version écrite, à travers une période de plus de trois mille ans. On pouvait comprendre les hiéroglyphes et les suivre du III^e millénaire avant J.-C. au IV^e siècle après J.-C. De plus, l'évolution des hiéroglyphes pouvait être rapprochée d'écrits en hiératique et en démotique qui, désormais, pouvaient aussi être déchiffrés.

Intrigues et jalousies empêchèrent pendant plusieurs années la magnifique réussite de Champollion d'être universellement reconnue. Thomas Young, en particulier, en fit une critique acerbe. Certains jours, il niait que les hiéroglyphes pussent être largement phonétiques ; d'autres fois, il se rangait à cette opinion, mais prétendait être lui-même parvenu à cette conclusion avant Champollion, et protestait que le Français n'avait fait que compléter son travail. Une grande part de l'hostilité de Young était due au fait que Champollion ne lui rendait guère hommage alors que ce sont probablement les découvertes initiales de Young qui l'ont inspiré dans son déchiffrement.

En juillet 1828, Champollion embarqua pour sa première expédition en Égypte, qui se prolongea dix-huit mois. C'était enfin l'occasion de voir l'original des inscriptions qu'il n'avait connues jusque-là que grâce à des dessins ou des lithographies. Trente ans plus tôt, l'expédition napoléonienne avait joué aux devinettes autour de la signification des

hiéroglyphes qui ornaient les temples, mais maintenant Champollion pouvait aisément les lire, caractère après caractère, et les interpréter correctement. Trois ans plus tard, après avoir mis au propre les notes, les dessins et les traductions de son expédition égyptienne, il fut victime d'une attaque cardiaque. Les évanouissements dans les moments d'émotion qu'il avait subis toute sa vie étaient sans doute le symptôme d'une maladie sérieuse, aggravée par ses études intenses et obsédantes. Il mourut le 4 mars 1832, à l'âge de quarante et un ans.

Le mystère du Linéaire B

Pendant les deux siècles qui suivirent les découvertes de Champollion, les égyptologues continuèrent à progresser dans la compréhension des hiéroglyphes. Le niveau atteint dans ce domaine est tel aujourd'hui que des savants sont capables de mettre au clair des hiéroglyphes cryptés, qui sont parmi les plus anciens textes chiffrés au monde. Certaines inscriptions figurant sur les tombes des pharaons étaient cryptées selon des techniques variées, incluant le chiffre de substitution. Parfois, des symboles élaborés remplaçaient le hiéroglyphe habituel et, en d'autres occasions, un hiéroglyphe phonétiquement différent mais d'un aspect proche était employé à la place du bon. Le hiéroglyphe de la vipère à cornes, par exemple, qui représente normalement le *f*, sera utilisé à la place du serpent qui représente le *z*. Généralement, ces épitaphes cryptées n'avaient pas pour fonction de protéger un secret. Au contraire, ces casse-tête cryptiques étaient là pour susciter la curiosité chez les passants, qui s'attardaient alors près d'une tombe à laquelle ils n'auraient autrement jeté qu'un coup d'œil.

Ayant vaincu les hiéroglyphes, les archéologues entreprirent de déchiffrer de nombreuses autres écritures anciennes, comme l'écriture cunéiforme, les caractères runiques, et l'alphabet brahmi. Par chance pour les Champollion en herbe, il reste à déchiffrer plusieurs écritures importantes comme l'étrusque et l'indus (voir Annexe I). La grande difficulté avec ces écritures est qu'on ne dispose pas de mots probables, et rien n'offre au décrypteur la moindre prise sur le sens des textes. Dans le cas des hiéroglyphes égyptiens, les cartouches fournirent les mots probables et donnèrent à Young puis à Champollion leur première idée d'une écriture fondée sur la phonétique. Sans cette aide, le déchiffrement d'une écriture ancienne peut sembler impossible, et pourtant il y a un exemple notable d'une écriture déchiffrée sans l'appui de mots probables. Le Linéaire B, une écriture crétoise remontant à l'âge du bronze, fut déchiffrée sans le secours de la moindre indication laissée par les scribes. Elle fut mise au clair grâce à un mélange de logique et d'inspiration, exemple patent de pure cryptanalyse. Le déchiffrement du Linéaire B est d'ailleurs considéré généralement comme le plus extraordinaire déchiffrement archéologique.

L'histoire du Linéaire B commence avec les fouilles effectuées par sir Arthur Evans, un des plus éminents archéologues au monde. Evans s'intéressait à la période de l'histoire grecque évoquée par Homère dans l'*Illiade* et l'*Odyssée*. Homère raconte la guerre de Troie, la victoire des Grecs, et les exploits jalonnant l'odyssée de son héros conquérant, événements supposés se passer au XII^e siècle avant J.-C. Certains érudits du XIX^e siècle avaient prétendu que l'épopée contée par Homère n'était qu'une légende, mais en 1872 l'archéologue allemand Heinrich Schliemann découvrit le site de Troie, pas très éloigné du rivage ouest de la Turquie, et soudain les mythes homériques devinrent de l'histoire. Entre 1872 et 1900, les archéologues découvrirent d'autres indices d'une riche période pré-hellénique, antérieure à l'âge classique de Pythagore, Aristote et Platon de quelque six cents ans. La période pré-hellénique s'étendait de 2800 à 1100 avant J.-C., mais c'est pendant les quatre derniers siècles que cette civilisation atteignit son apogée. Le centre de la Grèce continentale était Mycènes, où les archéologues découvrirent une grande quantité d'objets façonnés et de trésors. Mais sir Arthur Evans s'interrogeait devant l'absence totale d'une forme quelconque d'écriture parmi les découvertes des archéologues. Il ne pouvait croire qu'une société aussi raffinée ait été totalement illettrée, et il s'acharna à prouver que la civilisation mycénienne possédait une certaine forme d'écriture.



Fig. 57 Sites antiques autour de la mer Égée. Ayant découvert des trésors à Mycènes, en Grèce continentale, sir Arthur Evans partit à la recherche de tablettes gravées. Les premiers éléments du

Linéaire B furent découverts dans l'île de Crète, au cœur de l'Empire minoen.

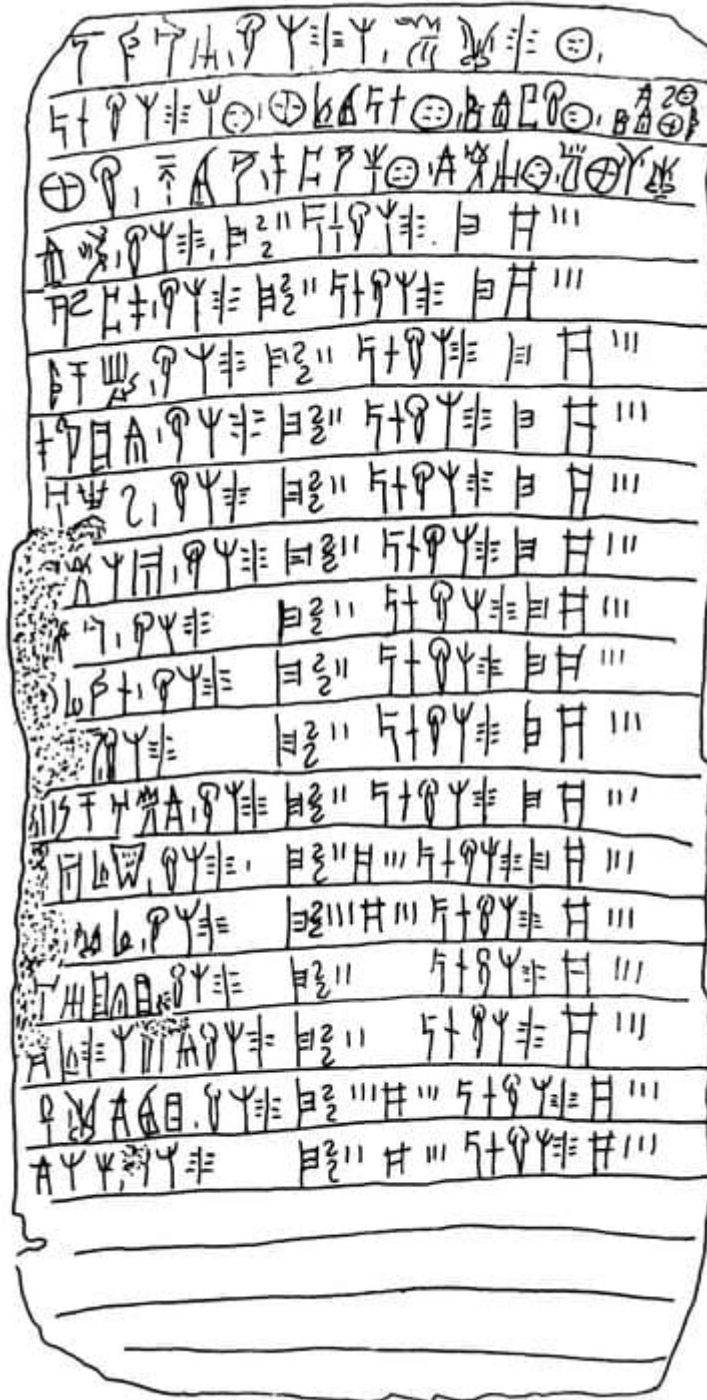
Après avoir rendu visite sans succès à nombre d'antiquaires athéniens, Evans finit par tomber sur des pierres gravées qui semblaient être des sceaux datant de l'âge du bronze. Les signes que portaient les sceaux semblaient, plutôt que de l'écrit, être des symboles proches de ceux utilisés en héraldique. Cette découverte encouragea Evans à poursuivre sa quête. Les sceaux provenaient de Crète, de Knossos précisément, où la légende situe le palais du roi Minos, au centre d'un empire qui s'étendait sur toute la mer Egée. En mars 1900, Evans partit pour la Crète et entreprit des fouilles. Les résultats furent aussi spectaculaires que rapides. Il dégagna les ruines d'un ancien palais, percé d'un réseau inextricable de couloirs et orné de fresques représentant des jeunes gens bondissant par-dessus de féroces taureaux. Cet exercice de saute-taureau était vraisemblablement lié à la légende du Minotaure, le monstre à tête de taureau mangeur de jeunes gens, et il pensa que le labyrinthe de corridors avait inspiré l'histoire du labyrinthe.

Le 31 mars, Evans se trouva en face du trésor qu'il convoitait : une tablette d'argile unique, portant une inscription. Quelques jours plus tard, il en trouva un plein coffre, plus une quantité de documents écrits dépassant ses espérances. Les tablettes d'argile étaient à l'origine séchées au soleil, et non pas au four, de façon à pouvoir les recycler simplement en les mouillant. Qu'elles n'aient pas été ramollies par la pluie au cours des siècles, et définitivement perdues, prouvait qu'elles avaient été cuites par le feu. Ainsi, l'incendie qui détruisit le palais de Knossos avait permis aux tablettes de se conserver pendant trois mille ans, dans un état tel qu'on pouvait encore y distinguer les empreintes digitales des scribes.

Les tablettes appartenaient à trois catégories. Le premier groupe, datant de 2000 à 1650 avant J.-C., ne portait que des dessins, sans doute des idéogrammes, que l'on pouvait rapprocher des symboles figurant sur les sceaux qu'Evans avait achetés à Athènes. Le second groupe de tablettes, de la période 1750 à 1450 avant J.-C., portait des caractères faits de simples traits, de lignes, d'où le nom de Linéaire A donné à cette écriture. L'écriture figurant sur le troisième groupe (1450 à 1375 avant J.-C.) semblait un perfectionnement de la précédente, d'où le nom de Linéaire B. Ces dernières tablettes étant les plus nombreuses et les plus récentes, Evans et d'autres archéologues jugèrent que c'était celles qu'ils auraient le plus de chances de déchiffrer.



Fig. 58 Une tablette en Linéaire B, 1400 environ avant J.-C.



Beaucoup de tablettes semblaient porter des inventaires. Avec un si grand nombre de colonnes de caractères numériques, il semblait assez facile de révéler la partie chiffrée, mais les caractères phonétiques étaient beaucoup plus embarrassants. Ils avaient l'air de gribouillages vides de sens. L'historien David Kahn décrivait certains des caractères comme « un arc gothique surmontant une ligne verticale, une échelle, un cœur traversé d'une flèche, un trident courbé en hameçon, un dinosaure à trois pattes regardant derrière lui, un A avec une seconde barre horizontale, un

S à l'envers, une grande chope de bière à moitié pleine, avec une anse fixée à son bord ; des douzaines d'autres ne ressemblaient à rien du tout ». Deux certitudes seulement purent être avancées à propos du Linéaire B. D'abord la direction de l'écriture était clairement de gauche à droite, car lorsqu'il y avait un espace vide sur une ligne, il était en général à droite. Ensuite il y avait 90 caractères distincts, ce qui tendait à prouver que l'écriture était syllabique. Les écritures alphabétiques ont généralement entre 20 et 40 signes (le russe, par exemple, a 36 signes et l'arabe 28). À l'opposé, les écritures qui utilisent des idéogrammes en ont des centaines, voire des milliers (le chinois en a plus de 5 000). Les écritures syllabiques, avec 50 à 100 caractères, se situent entre les deux. En dehors de ces deux points solides, le Linéaire B était un insondable mystère.

Le problème fondamental était que personne ne savait dans quelle langue était écrit le Linéaire B. On pensa d'abord qu'il s'agissait d'une forme de grec écrit, car sept des signes ressemblaient à des signes de l'écriture chypriote classique, une forme d'écriture grecque utilisée entre 600 et 200 avant J.-C. Cette hypothèse se heurta vite à un problème. Le *s* est la consonne finale la plus courante en grec, et par conséquent le caractère final le plus courant dans l'écriture chypriote est , qui représente la syllabe *se* (les caractères étant syllabiques, on doit représenter une consonne isolée par une combinaison consonne-voyelle, la voyelle restant muette). Le même signe apparaît dans le Linéaire B, mais rarement en fin de mot. D'où la conclusion que le Linéaire B ne pouvait être du grec, et qu'il s'agissait d'une langue inconnue qui, en disparaissant, avait laissé son écriture. Celle-ci, au cours des siècles, se serait transformée pour donner l'écriture chypriote, utilisée pour écrire le grec. Les deux écritures se ressemblaient donc, mais exprimaient des langues totalement différentes.

Evans était convaincu que le Linéaire B n'était pas une forme écrite du grec, et il crut immédiatement qu'il était l'écriture d'une langue indigène crétoise. Pour lui, de fortes preuves archéologiques venaient appuyer son hypothèse. Ses découvertes en Crète suggéraient que l'empire du roi Minos était en avance sur la civilisation de la Grèce continentale, que l'Empire minoen n'était pas une province de l'Empire mycénien, mais plutôt une puissance rivale, peut-être même dominante. Le mythe du Minotaure confortait cette position. La légende racontait comment le roi Minos exigeait des Athéniens l'envoi de groupes de jeunes gens et jeunes filles destinés à être sacrifiés au Minotaure. Evans en venait à

penser que les Minoens se jugeaient bien trop importants pour adopter la langue de leur rival, et avaient préféré garder leur propre langue.

L'idée que les Minoens avaient une langue propre représentée par le Linéaire B fit presque l'unanimité, mais il se trouva un ou deux contestataires qui soutinrent que les Minoens écrivaient et parlaient le grec. Evans ne prit pas ces opposants à la légère et usa de son influence pour sanctionner ceux qui s'opposaient à lui. Quand A.J.B. Wace, professeur d'archéologie à Cambridge, déclara adhérer à la théorie du Linéaire B comme écriture du grec, Evans l'exclut de toutes les fouilles et l'obligea à quitter l'Ecole anglaise d'Athènes.

En 1939, la controverse grec-pas grec enfla lorsque Carl Blegen, de l'université de Cincinnati, découvrit un nouveau coffre plein de tablettes en Linéaire B dans le palais de Nestor, à Pylos. C'était surprenant, car Pylos est sur le continent et avait fait partie de l'Empire mycénien. Les contestataires arguèrent de cet élément : on trouve du Linéaire B sur le continent où l'on parlait grec, le Linéaire B est donc du grec, et puisqu'on le trouve aussi en Crète, c'est que les Crétois parlaient également le grec. Le camp d'Evans retourna l'argument : les Minoens de Crète parlaient le minoen ; on trouve le Linéaire B en Crète, donc il représente la langue minoenne ; on trouve aussi le Linéaire B sur le continent, donc on y parlait également le minoen. Sir Arthur s'enflamma : « Il n'y a pas de place à Mycènes pour des dynasties parlant le grec (...) La culture comme la langue ont toujours été profondément minoennes. »

En fait, la découverte de Blegen n'entraînait pas nécessairement l'existence d'une langue commune aux Mycéniens et aux Minoens. Après tout, au Moyen Âge, de nombreux pays d'Europe, à côté de leur langue nationale, rédigeaient leurs archives en latin. La langue du Linéaire B était peut-être, de la même manière, d'un usage universel chez les comptables des rives de la mer Egée, afin de faciliter le commerce entre des nations qui ne parlaient pas la même langue.

Pendant quarante ans, toutes les tentatives de déchiffrement du Linéaire B considéré comme une langue non grecque échouèrent. Evans mourut en 1941, à l'âge de quatre-vingt-dix ans. Il ne fut pas témoin de la victoire sur le Linéaire B, et ne vécut pas assez pour lire les textes qu'il avait lui-même découverts. Il semblait alors y avoir bien peu d'espoir de les déchiffrer jamais.

Des syllabes qui font le pont

Après la mort d'Evans, les tablettes portant du Linéaire B et les notes personnelles d'Evans ne furent accessibles qu'à un cercle restreint d'archéologues, ceux qui avaient adhéré à sa théorie du Linéaire B comme langue minoenne. Vers le milieu des années 40 cependant, Alice Kober, un professeur de lettres classiques à Brooklyn College, se débrouilla pour avoir accès à ce matériel, et entama une analyse méticuleuse et impartiale des écrits.

Pour ceux qui la connaissaient peu, Alice Kober semblait une personne banale, un professeur terne, sans charme ni charisme, menant une existence plutôt terre à terre. Pourtant, elle avait une immense passion pour la recherche. « Elle travaillait avec une intensité maîtrisée », se rappelle Eva Brann, une étudiante qui devint plus tard archéologue à l'université Yale. « Elle me dit un jour : le seul moment où vous êtes sûre que vous avez réalisé quelque chose de vraiment important, c'est lorsque vous ressentez des picotements dans la colonne vertébrale. »

Pour venir à bout du Linéaire B, Kober comprit qu'elle devait abandonner toute idée préconçue. Elle se concentra uniquement sur la structure de l'écriture dans son ensemble et sur la construction de mots particuliers. Elle remarqua que certains mots formaient des triplets, si bien que l'on aurait dit que le même mot réapparaissait sous trois formes légèrement différentes. Dans un triplet, les radicaux étaient identiques, mais il y avait trois désinences possibles. Elle en conclut que le Linéaire B était une langue hautement flexionnelle, et que les terminaisons des mots s'accordaient selon le genre, le temps, le nombre, la personne, le cas, etc. Le français est légèrement flexionnel, puisque nous conjugurons par exemple : je déchiffre, tu déchiffres — à la deuxième personne du singulier, le verbe prend un s. Mais les langues anciennes tendent à pousser à l'extrême cet usage. Kober publia un article où elle décrivait la nature flexionnelle de deux groupes de mots, chaque groupe gardant ses radicaux respectifs, mais prenant des désinences différentes suivant les cas (voir [tableau 17](#)).



[Fig. 59](#) Alice Kober.

Mot A

Cas 1 𐀵𐀶𐀷𐀸

Cas 2 𐀵𐀶𐀷𐀹

Mot B

𐀶𐀷𐀸𐀹

𐀶𐀷𐀸𐀺

Cas 3 



Tableau 17 Deux mots flexionnels en Linéaire B.

Pour en faciliter l'expression, on attribua à chaque symbole du linéaire B un nombre de deux chiffres, comme le montre le [tableau 18](#). En appliquant ces nombres, les mots de Kober peuvent être réécrits comme dans le [tableau 19](#).

Ces deux groupes de mots peuvent être des noms dont la terminaison change en fonction du cas : le cas 1 pourrait être le nominatif, le cas 2 l'accusatif et le cas 3 le datif. Il est certain que les deux premiers signes dans les deux groupes de mots (25-67 et 70-52) sont des radicaux, puisqu'ils se répètent invariablement quel que soit le cas. Le troisième signe est plus curieux. S'il appartient au radical, il devrait rester constant pour un mot donné, quel que soit le cas, mais ce n'est pas ce qui se produit. Dans le mot A, le troisième signe est 37 dans les cas 1 et 2, mais 05 dans le cas 3. Dans le mot B, le troisième signe est 41 dans les cas 1 et 2, et 12 dans le cas 3. Par ailleurs, si le troisième signe ne fait pas partie du radical, il peut être une partie de la désinence, mais cette éventualité n'est pas certaine. Pour un cas donné, la terminaison serait la même, or pour les cas 1 et 2, le troisième signe est 37 dans le mot A, mais 41 dans le mot B et pour le cas 3, le troisième signe est 05 dans le mot A, mais 12 dans le mot B.

01	𐀀	30	𐀠	59	𐀡
02	𐀁	31	𐀡	60	𐀢
03	𐀂	32	𐀢	61	𐀣
04	𐀃	33	𐀣	62	𐀤
05	𐀄	34	𐀤	63	𐀥
06	𐀅	35	𐀥	64	𐀦
07	𐀆	36	𐀦	65	𐀧
08	𐀇	37	𐀧	66	𐀨
09	𐀈	38	𐀨	67	𐀩
10	𐀉	39	𐀩	68	𐀪
11	𐀊	40	𐀪	69	𐀫
12	𐀋	41	𐀫	70	𐀬
13	𐀌	42	𐀬	71	𐀭
14	𐀍	43	𐀭	72	𐀮
15	𐀎	44	𐀮	73	𐀯
16	𐀏	45	𐀯	74	𐀰
17	𐀐	46	𐀰	75	𐀱
18	𐀑	47	𐀱	76	𐀲
19	𐀒	48	𐀲	77	𐀳
20	𐀓	49	𐀳	78	𐀴
21	𐀔	50	𐀴	79	𐀵
22	𐀕	51	𐀵	80	𐀶
23	𐀖	52	𐀶	81	𐀷
24	𐀗	53	𐀷	82	𐀸
25	𐀘	54	𐀸	83	𐀹
26	𐀙	55	𐀹	84	𐀺
27	𐀚	56	𐀺	85	𐀻
28	𐀛	57	𐀻	86	𐀼
29	𐀜	58	𐀼	87	𐀽

Tableau 18 Les signes du Linéaire B et les nombres qui leur sont affectés.

	Mot A	Mot B
Cas 1	25-67-37-57	70-52-41-57
Cas 2	25-67-37-36	70-5241-36

Tableau 19 Les deux mots flexionnels réécrits en nombres.

Le troisième signe, 37, ne répond pas à ce qu'on attend, puisqu'il semble n'appartenir ni au radical, ni à la désinence. Kober résolut ce paradoxe en se fondant sur la théorie que chaque signe représente une syllabe, sans doute composée d'une consonne suivie d'une voyelle. Elle proposa donc que la troisième syllabe soit une *syllabe de liaison*, représentant une partie du radical et une partie de la désinence. La consonne pourrait se rattacher au radical, tandis que la voyelle appartiendrait à la désinence. Pour illustrer cette théorie, elle tira un exemple de la langue akkadienne, qui a elle aussi des syllabes de liaison et qui est particulièrement flexionnelle. *Sadanu* est un nom akkadien au premier cas, qui devient *sadani* au deuxième, et *sadu* au troisième :

Cas 1	sa-da-nu
Cas 2	sa-da-ni
Cas 3	sa-du

Tableau 20 Les syllabes de liaison dans le mot akkadien *sadanu*.

Il est clair que les trois mots sont constitués du radical *sadet* d'une désinence *-anu* (cas 1) *-ani* (cas 2) et *u* (cas 3) avec *-da-*, *-da-*, et *-du* comme syllabes de liaison respectives. Cette syllabe est la même dans les cas 1 et 2 et différente dans le cas 3. C'est exactement le modèle observé dans les mots du Linéaire B. Le troisième signe dans les mots du Linéaire B de Kober est donc une syllabe-pont.

En identifiant simplement la nature flexionnelle du Linéaire B et l'existence des syllabes-pont, Kober avait progressé plus avant que personne avant elle dans le déchiffrement de l'écriture minoenne, et pourtant ce n'était qu'un début. Elle allait faire une déduction encore plus importante. Dans l'exemple akkadien, la syllabe-pont change de *da* à *du*, mais la consonne reste la même dans les deux cas. Ainsi, les

syllabes 37 et 05 du mot A du Linéaire B doivent avoir en commun la même consonne et les syllabes 41 et 12 du mot B doivent aussi partager la même consonne. Pour la première fois depuis la découverte du Linéaire B par Evans, certains traits se précisaient quant à la phonétique des caractères. Alice Kober réussit à trouver un autre type de relation entre les caractères. Si nous examinons les mots A et B en Linéaire B, dans le cas 1 il apparaît qu'ils ont la même désinence. En revanche, la syllabe de liaison est changée de 37 en 41. Cela signifie que les signes 37 et 41 représentent des syllabes formées avec des consonnes différentes mais des voyelles identiques. Ceci expliquerait pourquoi les signes sont différents, tout en gardant la même désinence dans les deux mots. De même pour les noms au cas 3, les syllabes 05 et 12 auront une voyelle commune, mais des consonnes différentes.

Kober n'avait pas les moyens de repérer exactement quelle voyelle est commune à 05 et à 12, et laquelle à 37 et 41, de même qu'elle ne pouvait identifier la consonne commune à 37 et 05 et celle commune à 41 et 12. Cependant, sans référence à leurs valeurs phonétiques absolues, elle avait établi des rapprochements rigoureux entre certains caractères. Elle résuma ces résultats sous la forme d'une grille.

	Voyelle 1	Voyelle 2
Consonne 1	37	05
Consonne 2	41	12

Tableau 21 Grille de Kober des relations entre les caractères du Linéaire B.

Autrement dit, Kober ne savait pas quelle syllabe représentait le signe 37, mais elle savait qu'elle partageait sa consonne avec le signe 05 et sa voyelle avec le signe 41. De la même manière, elle ne savait pas quelle syllabe était représentée par le signe 12, mais elle savait que sa consonne était aussi celle du signe 41 et que sa voyelle était aussi celle du signe 05. Elle appliqua sa méthode à d'autres mots, réussissant à établir une grille de dix signes, de deux voyelles sur la largeur et de cinq consonnes sur la hauteur. L'étape suivante aurait pu être un pas décisif vers le déchiffrement. Peut-être même Kober serait-elle venue à bout de toute

l'écriture ? Malheureusement, elle ne vécut pas assez pour exploiter les retombées de ses recherches. En 1950, elle mourait d'un cancer du poumon, à l'âge de quarante-trois ans.

Une digression futile

Quelques mois avant sa mort, Alice Kober avait reçu une lettre de Michael Ventris, un architecte anglais fasciné depuis son enfance par le Linéaire B. Ventris était né le 12 juillet 1922 d'un officier de l'armée anglaise et d'une mère à moitié polonaise, qui fut grandement responsable de son intérêt pour l'archéologie. Elle l'accompagnait régulièrement au British Museum où il pouvait admirer les merveilles de l'Antiquité. Michael était un enfant brillant, prodigieusement doué pour les langues. Il commença sa scolarité à Gstaad, en Suisse, où il se parlait couramment le français et l'allemand. Il apprit tout seul le polonais à six ans.

Comme Jean-François Champollion, Ventris s'intéressa très jeune aux écritures anciennes. À sept ans, il étudiait un livre sur les hiéroglyphes. Impressionnant pour quelqu'un de cet âge, surtout lorsqu'on sait que le livre était en allemand ! Cet intérêt pour les écritures de l'Antiquité occupa toute son enfance et, à quatorze ans, il fut absolument transporté par une conférence de sir Arthur Evans, l'homme du Linéaire B, à laquelle il assista. Le jeune Ventris entendit évoquer la civilisation minoenne et le mystère du Linéaire B, et il se promit qu'il déchiffrerait cette écriture. Ce jour-là, était née une obsession qui ne le quitta plus de toute sa brillante mais courte existence.

À dix-huit ans, il publia dans le très sérieux *American Journal of Archaeology* un article présentant ses premières idées sur le Linéaire B. Lorsqu'il soumit cet article à la revue, il prit soin de cacher son âge de peur de ne pas être pris au sérieux. Son article allait dans le sens d'Evans et attaquait l'hypothèse grecque, affirmant que « la théorie selon laquelle le minoen serait du grec est évidemment fondée sur une ignorance délibérée de la plausibilité historique ». Il croyait, lui, que le Linéaire B était lié à l'étrusque, une idée vraisemblable puisqu'il était prouvé que les Étrusques étaient venus de la mer Egée pour s'établir en Italie. Même si son article ne portait aucun début de déchiffrement, il concluait avec confiance : « On peut le faire. »

Bien que devenu architecte, et non archéologue, Ventris resta passionné par le Linéaire B. Il passait ses loisirs à en étudier tous les aspects. Lorsqu'il entendit parler du travail d'Alice Kober, il désira en

savoir plus sur ses découvertes et lui écrivit pour lui demander des précisions. Elle mourut avant d'avoir pu lui répondre, mais il restait ses publications et Ventris les étudia méticuleusement. Il comprit toute l'utilité de la grille de Kober, et chercha de nouveaux mots ayant en commun des radicaux et des syllabes de liaison. Il agrandit la grille en y portant des signes supplémentaires, qui renfermaient d'autres voyelles et d'autres consonnes. Après une année de labeur intense, il remarqua quelque chose d'étrange, quelque chose qui semblait suggérer une exception à la règle selon laquelle les signes du Linéaire B représentent des syllabes.

On s'était généralement accordé à penser que chaque signe représentait la combinaison d'une consonne et d'une voyelle (CV) et donc que, pour épeler un mot, il fallait le décomposer en éléments CV. Par exemple, le mot *minute* serait épelé *mi-nu-te*, une suite de trois syllabes CV. Toutefois, de nombreux mots ne se divisent pas aisément ainsi. Si nous découpons *visible* en paires de lettres, nous obtenons *vi-si-ble*, ce qui pose un problème, puisque ce n'est plus une simple suite de syllabes CV. Il y a un groupe de deux consonnes *bl* et un *e* isolé à la fin du mot. Ventris supposa que les Minoens s'en tiraient en créant la syllabe artificielle *-bi-* par insertion d'un *i* muet, afin que le mot puisse s'écrire comme une combinaison de syllabes CV : *vi-si-bi-le*.

Le mot *invisible* est plus problématique. Là encore, il faudrait insérer des voyelles muettes, cette fois après le *n* et le *b*, pour en faire des syllabes CV. Mais il reste un *i* isolé en tête du mot *i-ni-vi-si-bi-le*. Ce *i* initial ne peut pas être aisément transformé en syllabe CV, car placer une consonne muette en tête prêterait à confusion. Ventris en conclut que certains signes du Linéaire B devaient représenter des voyelles isolées. Ces signes devaient être faciles à identifier, de par leur position. Ventris releva combien de fois chaque signe apparaissait au début, au milieu et à la fin de chaque mot, et il nota que deux signes, le 08 et le 61, étaient les plus fréquents en tête. Il en conclut qu'ils représentaient, non pas des syllabes, mais bien plutôt des voyelles isolées. Il publia sa théorie sur les signes représentatifs des voyelles et ses extensions à la grille de Kober, dans une série de *Notes de travail*, qu'il diffusa parmi les spécialistes.



[Fig. 60](#) Michael Ventris.

Le 1^{er} juin 1952, il publia dans sa Note 20 sa découverte la plus importante, qui marquait un tournant dans le déchiffrement du Linéaire B. Il avait passé les deux années précédentes à étendre la grille de Kober jusqu'à la version du [tableau 22](#). La grille rassemblait 5 colonnes de voyelles et 15 lignes de consonnes, dessinant au total 75 emplacements, plus 5 disponibles pour des voyelles isolées. Ventris avait rempli à peu près la moitié de sa grille.

Cette grille apportait un trésor d'informations. Sur la sixième ligne, par exemple, on peut lire que les signes syllabiques 37, 05 et 69 ont une consonne commune, VI, mais des voyelles différentes, 1, 2 et 4. Ventris ignorait les valeurs exactes de la consonne VI et des voyelles 1 et 2 et 4 et, jusque-là, il avait résisté à la tentation d'attribuer des valeurs phonétiques à l'un quelconque des signes. Cependant, il sentit qu'il était maintenant mûr pour se laisser guider par certains indices, deviner quelques valeurs phonétiques, et en tester les conséquences.

Ventris avait remarqué trois mots qui apparaissaient à de nombreuses reprises sur les tablettes (08-73-30-12), (70-52-12) et (69-53-12). En se fondant sur sa seule intuition, il imagina que ces mots pouvaient être des noms de villes importantes. Ventris avait déjà supposé que le 08 était une voyelle, le nom de la première ville devait donc commencer par une voyelle. Le seul nom connu qui s'adaptait était Amnisos, un port important. S'il avait raison, le deuxième et le troisième signes, 73 et 30, représentaient *-mi-* et *-ni-*. Ces deux syllabes contenaient la voyelle *i*, et les nombres 73 et 30 devaient se trouver sur la même colonne de voyelles sur la grille. Ils y étaient. Le signe final, 12, devait représenter *-so-*, et le *s* final ne figurait pas. Ventris décida d'ignorer pour le moment le problème du *s* final, et traduisit le mot ainsi :

Ville 1 = 08-73-30-12 = a-mi-ni-so = Amnisos

		Voyelles				
		1	2	3	4	5
Consonnes	I					57
	II	40		75		54
	III	39				03
	IV		36			
	V		14			01
	VI	37	05		69	
	VII	41	12			31
	VIII	30	52	24	55	06
	IX	73	15			80
	X		70	44		
	XI	53				76
	XII		02	27		
	XIII					
	XIV			13		
	XV		32	78		
	Voyelles isolées		61			08

Tableau 22 Grille de Ventris étendue à d'autres relations entre des caractères du Linéaire B. Bien que la grille ne spécifie pas quelles sont les voyelles et les consonnes, elle expose quels caractères ont des consonnes en commun. Tous les caractères de la première colonne, par exemple, partagent la même voyelle appelée 1.

Cela n'était qu'une conjecture, mais les répercussions sur la grille de Ventris étaient considérables. Le signe 12, qui représente le signe *-so-* est dans la deuxième colonne de voyelles et dans la septième ligne de consonnes. Si ses suppositions étaient avérées, d'autres signes syllabiques de la colonne 2 comporteraient donc la voyelle o

, et tous ceux de la ligne VII comporteraient la consonne s.

Quand Ventris examina la deuxième ville, il nota qu'elle comportait aussi le signe 12, *-so-*. Les deux autres signes, 70 et 52, étaient dans la même colonne de voyelles que *-so-*, ce qui signifiait que ces signes aussi comportaient la voyelle o. Pour la deuxième ville, il put insérer le *-so-* et le o à la place appropriée, et laissa des blancs pour les consonnes manquantes, ce qui donna :

$$\text{Ville 2} = 70\text{-}52\text{-}12 = ? \text{ o- } ? \text{ o-so} = ?$$

Cela pouvait-il être Knossos ? Les signes pouvaient représenter *ko-no-so*. Une fois encore, Ventris préféra ignorer la question de l'absence

du s final, au moins momentanément. Il fut heureux de voir que le signe 52, qu'il supposait représenter *-no-*, était sur la même ligne de consonnes que le signe 30 supposé représenter *-ni-* dans Amnisos. Cela pouvait le rassurer, puisque les deux signes contenant la même consonne *n*, ils devaient effectivement figurer sur la même ligne. En se servant des syllabes définies dans Knossos et Amnisos, il inséra entre les signes de la troisième ville les lettres suivantes :

Ville 3 = 69-53-12 = ? ?- ? i-so

Le seul nom qui se prêtait à ce schéma était Tulissos (tu-li-so), une ville importante du centre de la Crète. Là encore le s final manquait, là encore Ventris ignora le problème. Il avait maintenant identifié trois noms de villes et les valeurs phonétiques de huit signes différents

Ville 1 = 08-73-30-12 = a-mi-ni-so = Amnisos
 Ville 2 = 70-52-12 = ko-no-so = Knossos
 Ville 3 = 69-53-12 = tu-li-so = Tulissos

Les répercussions de l'identification de huit signes furent énormes. Ventris put attribuer des valeurs phonétiques à beaucoup d'autres signes figurant soit sur la même ligne, soit dans la même colonne de la grille. De nombreux signes révélèrent en partie leur signification syllabique, et quelques-uns purent être identifiés complètement. Le signe 05, qui est dans la même colonne que 12 (*so*), 52 (*no*) et 70 (*ko*), donc dans la colonne des o, contient évidemment la voyelle o. De la même façon, le signe 05, qui est sur la même ligne que 69 (*tu*), doit contenir la consonne *t*. Bref, le signe 05 représente la syllabe *-to-*. Allons au signe 31, qui est dans la même colonne que 08, la colonne des *a*, et sur la même ligne que 12, la ligne des s. Nous concluons que le signe 31 représente la syllabe *-sa-*.

Trouver les valeurs syllabiques de ces deux signes 05 et 31 était particulièrement important car cela permit à Ventris de lire deux mots entiers, 05-12-et-05-31-, qui apparaissaient souvent au bas des inventaires. Ventris savait déjà que 12 représente la syllabe *-so-*, car ce signe apparaissait dans le mot Tullisos, donc 05-12 se lisait *to-so*. Et l'autre mot, 05-31, se lisait *to-sa*. C'était un résultat étonnant. Des experts avaient supposé que, figurant au bas des inventaires, ils signifiaient total. Ventris les lisait maintenant *toso* et *tosa*, ce qui était étrangement similaire aux *tossos* et *tossa* du grec archaïque, formes

masculine et féminine du mot signifiant *tant*. Les découvertes de Ventris nourrissaient les arguments en faveur du grec comme langue du Linéaire B alors que, depuis ses quatorze ans, époque où il avait suivi la conférence de sir Arthur Evans, il vivait avec l'idée que la langue des Minoens ne pouvait pas être le grec.

C'est l'écriture chypriote ancienne qui avait fourni les premières indications portant à écarter le grec comme langue du Linéaire B, car on avait remarqué que les mots du Linéaire B se terminent rarement par *s*, alors que c'est une terminaison courante en grec. Et Ventris découvrait que si les mots du Linéaire B se terminaient rarement par *s*, c'était sans doute simplement parce que ce *s* était omis, par une sorte de convention. Amnisos, Knossos, Tulissos et *tossos* étaient tous écrits sans le *s* final, ce qui prouvait simplement que les scribes laissaient au lecteur le soin de réparer l'omission évidente.

Ventris eut bientôt déchiffré quelques mots de plus qui ressemblaient à du grec, mais il n'était pas encore tout à fait convaincu que le Linéaire B était une écriture grecque. En fait, les quelques mots qu'il avait déchiffrés pouvaient tous être tenus pour des mots importés dans la langue minoenne. Un étranger arrivant dans un hôtel à Bristol peut saisir des mots comme *rendez-vous* ou *bon appétit*, mais il aurait tort d'en déduire que les Anglais parlent français. De plus, Ventris tomba sur des mots qui, pour lui, n'avaient aucun sens, ce qui permettait de prêcher en faveur d'une langue jusque-là inconnue. Dans sa Note 20, il n'ignorait pas l'hypothèse grecque, mais il la qualifiait de *digression futile*. Il concluait : « Si on poursuit dans cette voie de déchiffrement, je soupçonne qu'elle nous mènera tôt ou tard à une impasse, ou se dissipera d'elle-même en absurdités. »

Malgré ses réserves, Ventris poursuivit la piste grecque. Alors que sa Note 20 était encore en circulation, il découvrit d'autres mots grecs. Il put identifier *poïmen* (berger), *kerameus* (potier), *khrusouorgos* (orfèvre), *khalkeus* (bronzier), et il traduisit même deux phrases complètes. Jusque-là, aucune des absurdités annoncées ne s'était mise en travers de son chemin. Pour la première fois en trois mille ans, l'écriture muette du Linéaire B chuchotait, et la langue qu'elle parlait était indubitablement le grec.

Durant cette période où il progressait rapidement, Ventris fut invité à parler à la BBC du mystère des écrits minoens. Il pensa que ce serait une occasion idéale pour rendre publique sa découverte. Après une discussion prosaïque sur l'histoire minoenne et le Linéaire B, il fit une

déclaration révolutionnaire : « Ces dernières semaines, j'en suis venu à penser que les tablettes de Pylos et de Knossos peuvent, après tout, avoir été écrites en grec, un grec difficile et archaïque, étant donné qu'il est de cinq cents ans antérieur à Homère, et écrit dans une forme assez abrégée, mais néanmoins du grec. »

Un des auditeurs se trouvait être John Chadwick, un chercheur de Cambridge qui s'était intéressé au déchiffrement du Linéaire B depuis les années 30. Pendant la guerre, il avait servi comme cryptanalyste à Alexandrie, où il brisait les chiffres italiens, avant d'être muté à Bletchley Park, où il s'attaqua aux codes japonais. Après la guerre, il entreprit à nouveau le déchiffrement du Linéaire B, avec des techniques expérimentées sur les codes militaires. Il eut peu de réussite.

Entendant l'entretien radiophonique de Ventris, et cette déclaration apparemment absurde à laquelle il n'était pas préparé, Chadwick, ainsi que la majorité des érudits, repoussa cette assertion comme venant d'un amateur, ce qui, après tout, était vrai. Pourtant, comme il enseignait le grec, Chadwick réalisa qu'il allait être assailli de questions sur la théorie de Ventris, et il décida d'examiner en détail ses arguments. Il se procura des copies des Notes de Ventris, et les étudia, s'attendant à y trouver quantité de failles. Au contraire, en quelques jours, le chercheur sceptique se transforma en l'un des premiers adeptes de la « théorie grecque » du Linéaire B.

Chadwick se prit d'admiration pour le jeune architecte :

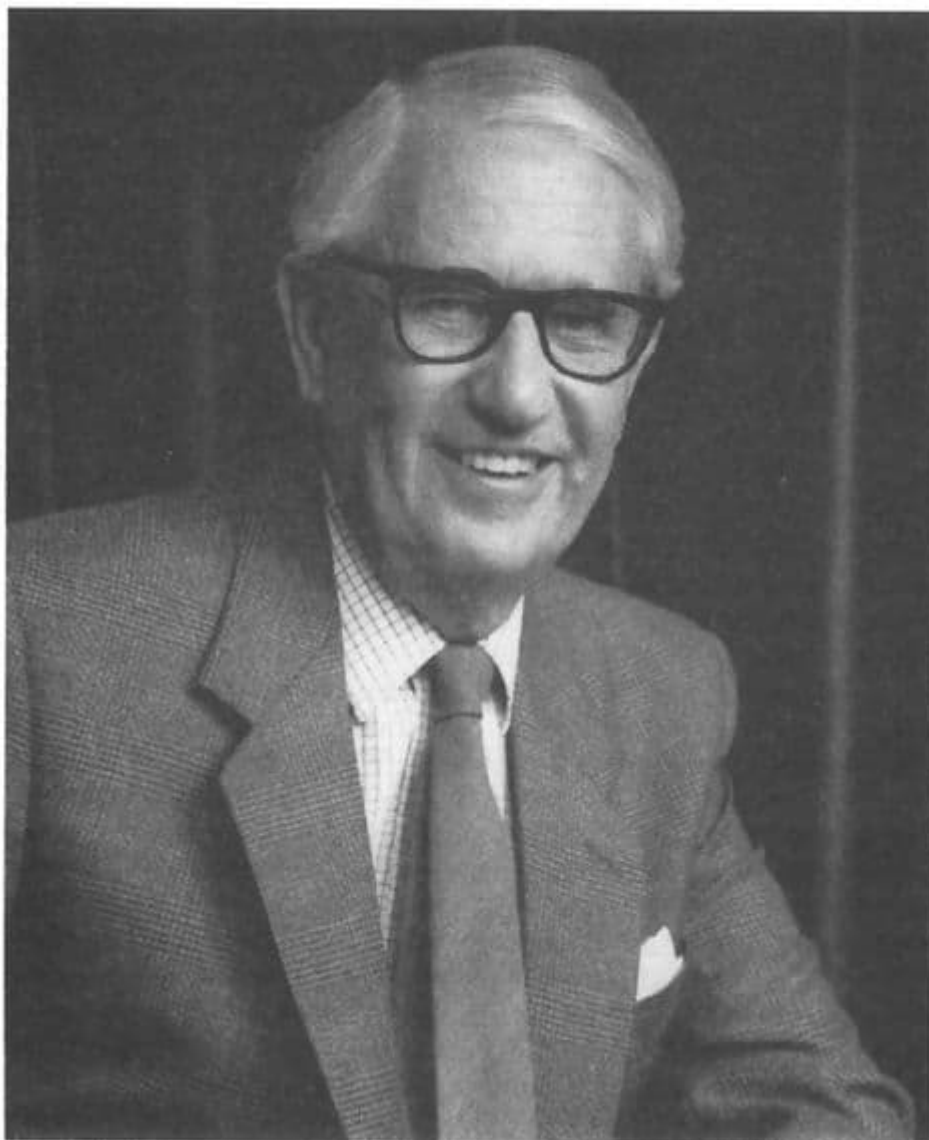


Fig. 61 John Chadwick.

Son cerveau fonctionnait à une vitesse incroyable, si bien qu'il pouvait déduire toutes les implications d'une hypothèse presque avant que vous l'ayez formulée. Il avait un jugement pénétrant sur le contexte de l'époque ; les Mycéniens n'étaient pas pour lui de vagues abstractions, mais des hommes dont on pouvait suivre la pensée. Il insistait lui-même sur le côté visuel du problème ; l'aspect des textes lui était devenu si familier que des portions importantes en étaient gravées dans sa mémoire comme des dessins, bien avant que le sens en ait été déchiffré. Mais une mémoire photographique ne suffit pas, et c'est ici que son expérience d'architecte venait à

son aide. L'œil de l'architecte voit dans une construction non pas une simple façade, mélange d'éléments structuraux et ornementaux. Il regarde au-delà des apparences et distingue dans le dessin les parties constitutives, la structure et la charpente du bâtiment. De la même manière, Ventris était capable de discerner, au milieu de la déroutante variété des signes, des modèles et des motifs réguliers qui en révélaient la structure sous-jacente. C'est cette capacité, ce pouvoir de trouver de l'ordre dans une confusion apparente, qui a marqué les travaux de tous les grands hommes.

Une arme manquait pourtant à Ventris, à savoir une bonne connaissance du grec archaïque. Les études de grec de Ventris remontaient à ses années de Collège, et il ne pouvait pas exploiter pleinement sa découverte. Il était incapable, par exemple, d'expliquer certains des mots déchiffrés, qui n'appartenaient pas à son vocabulaire grec. La spécialité de Chadwick était la philologie grecque, et l'évolution historique de la langue, ce qui lui permit de démontrer que ces mots problématiques s'accordaient aux théories sur les plus anciennes formes du grec. À eux deux, Chadwick et Ventris formaient une équipe idéale.

Il faut noter que le grec d'Homère remonte à trois mille ans, mais que le grec du Linéaire B est encore de cinq cents ans plus vieux. Aussi, pour le traduire, Chadwick dut extrapoler du grec ancien aux mots du Linéaire B, en tenant compte des trois facteurs principaux de l'évolution des langues. D'abord, avec le temps, la prononciation évolue. Ensuite, la grammaire change. Dans le Linéaire B, la terminaison du génitif est -*oio-*, mais en grec classique elle est remplacée par -*ou-*. Enfin, le lexique change considérablement. Certains mots naissent, d'autres meurent, et d'autres changent de sens. Dans le Linéaire B, *harmono* signifie roue, mais plus tard, le même mot signifiera chariot. On peut rapprocher cet exemple de l'usage que fait aujourd'hui le français de l'expression « deux roues ».

Ce tandem, unissant les talents de décrypteur de Ventris et les connaissances de Chadwick en grec, entreprit de convaincre le reste du monde que le Linéaire B était bien du grec. La progression de la traduction s'accélérait chaque jour. Dans le récit que fit Chadwick de leur travail, *Le déchiffrement du Linéaire B*, il écrit :

La cryptographie est une science qui procède de la déduction et de l'expérimentation ; on forme des hypothèses, on les teste, et souvent on y renonce. Mais peu à peu, les chercheurs voient se former, avec les éléments qui ont réussi à franchir le cap des essais, un sol suffisamment solide sous leurs pieds : leurs hypothèses trouvent leur cohérence et des fragments de sens émergent de leur camouflage. Le code craque. Peut-être pourrait-on mieux définir ce point en disant que les voies probables apparaissent alors plus vite qu'on ne peut les suivre. C'est comparable au début d'une réaction nucléaire en chaîne ; une fois passé le seuil critique, la réaction se poursuit toute seule.

Il ne fallut pas longtemps pour qu'ils soient en mesure de démontrer leur maîtrise de l'écriture en s'envoyant l'un à l'autre de courtes notes rédigées en Linéaire B.

Une vérification informelle de l'exactitude d'un déchiffrement peut reposer sur le nombre de noms de dieux dans le texte. Ceux qui, par le passé, avaient suivi de mauvaises pistes avaient naturellement engendré des mots vides de sens qu'ils n'avaient justifiés qu'en les attribuant à des divinités inconnues. Chadwick et Ventris n'eurent à faire appel qu'à quatre noms de dieux, déjà tous bien connus.

En 1953, confiants en leur analyse, ils publièrent leurs travaux dans un article modestement intitulé « Évidence d'un dialecte grec dans les archives mycéniennes », qui fut publié dans le *Journal des Études helléniques*. Des archéologues du monde entier commencèrent alors à comprendre qu'ils étaient témoins d'une révolution. Dans une lettre à Ventris, le savant allemand Ernst Sittig se faisait l'écho de l'état d'esprit de la communauté universitaire : « Je le répète : vos démonstrations sont, sur le plan de la cryptographie, les plus intéressantes qu'il m'ait été donné de voir, et sont réellement passionnantes. Si vous avez raison, les méthodes de l'archéologie, de l'ethnologie, de l'histoire et de la philologie des cinquante dernières années sont dénoncées *ab absurdum*. »

Les tablettes du Linéaire B contredisaient à peu près tout ce qu'avaient affirmé sir Arthur Evans et toute une génération de savants. D'abord par le simple fait que le Linéaire B *était* du grec. Ensuite, si les Minoens de

Crète écrivaient et, sans doute, parlaient grec, les historiens devaient reconsidérer leurs vues sur l'histoire minoenne. Il semblait évident maintenant que la puissance dominante dans la région était Mycènes, et la Crète minoenne un État mineur, dont les habitants parlaient la langue du puissant voisin. Il est pourtant prouvé que, avant 1450 avant J.-C., c'était un État indépendant avec sa langue propre. C'est autour de cette date que le Linéaire B avait succédé au Linéaire A et, bien que les deux écritures se ressemblent, personne n'a encore déchiffré le Linéaire A. Ce dernier représente probablement une langue entièrement différente. Il semble que vers 1450 avant J.-C., les Mycéniens conquièrent le pays des Minoens, imposèrent leur langue, et transformèrent le Linéaire A en Linéaire B, qui servit ainsi d'écriture pour le grec.

Tout en éclairant la vision générale de l'histoire, le déchiffrement du Linéaire B aide aussi à préciser certains détails. Ainsi, les fouilles de Pylos n'avaient mis à jour aucun objet précieux dans le somptueux palais, qui avait été détruit par le feu. Cela avait conduit à penser que le palais avait été incendié délibérément par les envahisseurs, qui l'avaient préalablement dépouillé de tout ce qui avait de la valeur. Bien que les tablettes en Linéaire B de Pylos ne décrivent pas précisément une telle attaque, elles font référence à des préparatifs d'invasion. Une tablette décrit la création d'une unité militaire spéciale pour protéger la côte, tandis qu'une autre raconte la réquisition des ornements de bronze pour en forger des fers de lances. Une troisième tablette, plus confuse que les deux autres, décrit un rituel particulièrement compliqué au temple, comportant peut-être un sacrifice humain. La plupart des tablettes en Linéaire B sont d'une parfaite netteté, ce qui veut dire que les scribes faisaient d'abord un brouillon qui était ensuite détruit. La tablette peu soignée comporte de grands blancs, des lignes à moitié remplies et du texte qui s'étale de l'autre côté. Une explication plausible est que la tablette portait l'ordre d'invoquer une intervention divine face à l'invasion, mais que le palais fut pris avant que la tablette ait été recopiée.

01	𐀀	da	30	𐀠	ni	59	𐀡	ta
02	𐀁	ro	31	𐀡	sa	60	𐀢	ra
03	𐀂	pa	32	𐀢	qo	61	𐀣	o
04	𐀃	te	33	𐀣	ra ₂	62	𐀤	pte
05	𐀄	to	34	𐀤		63	𐀥	
06	𐀅	na	35	𐀥		64	𐀦	
07	𐀆	di	36	𐀦	jo	65	𐀧	ju
08	𐀇	a	37	𐀧	ti	66	𐀨	ta ₂
09	𐀈	se	38	𐀨	e	67	𐀩	ki
10	𐀉	u	39	𐀩	pi	68	𐀪	ro ₂
11	𐀊	po	40	𐀪	wi	69	𐀫	tu
12	𐀋	so	41	𐀫	si	70	𐀬	ko
13	𐀌	me	42	𐀬	wo	71	𐀭	dwo
14	𐀍	do	43	𐀭	ai	72	𐀮	pe
15	𐀎	mo	44	𐀮	ke	73	𐀯	mi
16	𐀏	pa ₂	45	𐀯	de	74	𐀰	ze
17	𐀐	za	46	𐀰	je	75	𐀱	we
18	𐀑		47	𐀱		76	𐀲	ra ₂
19	𐀒		48	𐀲	nwa	77	𐀳	ka
20	𐀓	zo	49	𐀳		78	𐀴	qe
21	𐀔	qi	50	𐀴	pu	79	𐀵	zu
22	𐀕		51	𐀵	du	80	𐀶	ma
23	𐀖	mu	52	𐀶	no	81	𐀷	ku
24	𐀗	ne	53	𐀷	ri	82	𐀸	
25	𐀘	a ₂	54	𐀸	wa	83	𐀹	
26	𐀙	ru	55	𐀹	nu	84	𐀺	
27	𐀚	re	56	𐀺	pa ₃	85	𐀻	
28	𐀛	i	57	𐀻	ja	86	𐀼	
29	𐀜	pu ₂	58	𐀼	su	87	𐀽	

Tableau 23. Signes du Linéaire B avec leurs numéros et leurs valeurs phonétiques.

Le coffre de tablettes en Linéaire B contient des inventaires, et elles décrivent des transactions au jour le jour. Elles prouvent l'existence d'une bureaucratie capable de rivaliser avec n'importe quelle autre dans l'histoire, avec des tablettes contenant des précisions sur tous les objets manufacturés ou les produits agricoles. Chadwick compara ces archives au *Domesday Book* et le professeur Denys Page commente leur niveau de précision comme suit : « On peut compter les moutons jusqu'au total

impressionnant de vingt-cinq mille, mais il y a lieu également de spécifier qu'un animal avait été donné par Komawens... On peut supposer que pas une graine ne pouvait être semée, pas un gramme de bronze travaillé, pas une chèvre élevée ou un porc engraisé sans qu'un formulaire soit rempli au palais du roi. » Ces rapports au palais peuvent sembler prosaïques, mais ils font partie d'un héritage romanesque puisqu'ils sont liés intimement à l'*Illiade* et à l'*Odyssée*. Pendant que les scribes enregistraient ces transactions quotidiennes, la guerre de Troie se déroulait. La langue du Linéaire B est la langue de l'*Odyssée*.

Le 24 juin 1953, Ventris donna une conférence sur le déchiffrement du Linéaire B. Le lendemain on en parlait dans le *Times*, à côté d'un commentaire sur la récente conquête de l'Everest. Cela inspira de titrer sur la réussite de Ventris et Chadwick : « L'Everest de l'archéologie grecque ». L'année suivante, les deux hommes décidèrent d'écrire un traité en trois volumes, qui comporterait une description du déchiffrement, l'analyse détaillée de trois cents tablettes et un dictionnaire de 630 mots mycéniens. *Documents in Mycenaean Greek* (« Documents sur le grec mycénien ») fut terminé à l'été 1955 et prêt pour publication à l'automne 1956. Quelques jours avant que le livre sorte de l'imprimerie, le 6 septembre 1956, rentrant chez lui tard dans la nuit, Michael Ventris se tua au volant en percutant un camion. John Chadwick rendit hommage à son collègue, un homme qui rivalisait de génie avec Champollion et qui mourut lui aussi tragiquement jeune : « Le travail qu'il a fait est vivant, et l'on se souviendra de son nom aussi longtemps qu'on étudiera la langue et la civilisation grecques. »

6

Alice et Bernard s'affichent en public

Pendant la Seconde Guerre mondiale, les décrypteurs anglais avaient pris le dessus sur les concepteurs de code allemands, en partie parce que les hommes et les femmes de Bletchley Park, en suivant la voie ouverte par les Polonais, avaient développé une des premières technologies du déchiffrement. Après les *bombes* de Turing, qui servirent à percer le chiffre d'Enigma, les Anglais inventèrent un autre outil, le *Colossus*, conçu pour combattre une forme de chiffrement encore plus efficace, le *chiffre de Lorenz*. De ces deux types de machines, c'est Colossus qui ouvrit la voie à un nouveau développement de la cryptographie pendant la seconde moitié du XX^e siècle.

Le chiffre de Lorenz était utilisé pour crypter les messages entre Hitler et ses généraux. Le chiffrement était effectué par la machine SZ40 de Lorenz, qui fonctionnait sur le même principe qu'Enigma, mais était beaucoup plus complexe. Les décrypteurs de Bletchley se trouvèrent confrontés à un problème encore plus difficile à résoudre. Toutefois, deux des cerveaux de Bletchley, John Tiltman et Bill Tutte, découvrirent un point faible dans l'utilisation du chiffre de Lorenz, et Bletchley exploita cette faille pour lire les messages de Hitler.

Percer le chiffre de Lorenz requérait à la fois des recherches, des tâtonnements, de l'analyse statistique et du jugement, ensemble hors de portée pour les capacités purement techniques des bombes. Les bombes pouvaient exécuter une tâche spécifique à grande vitesse, mais elles ne pouvaient épouser les subtilités du chiffre de Lorenz. On devait donc révéler les messages cryptés de Lorenz à la main, ce qui demandait des semaines d'efforts constants, au terme desquelles le contenu des messages était évidemment obsolète. Jusqu'au jour où Max Newman, un mathématicien de Bletchley, trouva le moyen de mécaniser la cryptanalyse du chiffre de Lorenz. En s'appuyant sur le concept de la machine universelle de Turing, Newman mit au point une machine

capable de s'adapter à des problèmes différents — ce que nous appellerions un ordinateur programmable.

Malheureusement, il semblait techniquement impossible de construire la machine de Newman, et l'état-major de Bletchley enterra le projet. Pourtant Tommy Flowers, un ingénieur qui avait pris part aux discussions autour de l'idée de Newman, décida d'ignorer le scepticisme de Bletchley et entreprit d'élaborer la machine. Flowers suivit les plans de Newman et consacra dix mois à réaliser le Colossus qu'il livra à Bletchley Park le 8 décembre 1943. La machine comportait 1 500 valves électroniques qui étaient considérablement plus rapides que les lentes communications des relais électromécaniques des bombes. Plus important encore que sa rapidité, était le fait que le Colossus était programmable. C'est ce qui fait de lui le précurseur de l'ordinateur moderne.

Comme tout ce qui se trouvait à Bletchley Park, Colossus fut détruit après la guerre et on interdit d'en parler à ceux qui avaient travaillé dessus. Lorsqu'on ordonna à Tommy Flowers de détruire les plans de Colossus, il les porta avec obéissance à la chaufferie et les mit au feu. Les plans du premier ordinateur au monde étaient perdus à jamais. Cette obligation de secret permit à d'autres chercheurs de se voir créditer de l'invention de l'ordinateur. En 1945, J. Presper Eckert et John W. Mauchly, de l'université de Pennsylvanie, mirent au point l'ENIAC (Intégrateur et calculateur numérique électronique), constitué de 18 000 valves électroniques, capable d'effectuer 5 000 opérations par seconde. Pendant des dizaines d'années, on considéra l'ENIAC comme l'ancêtre de tous les ordinateurs, en ignorant Colossus.

Les cryptanalystes qui avaient contribué à la naissance de l'ordinateur s'employèrent après guerre à développer et à utiliser cette technologie pour briser toutes sortes de chiffres. La cryptanalyse pouvait exploiter la rapidité et la souplesse des calculateurs programmables pour rechercher, parmi toutes les clefs possibles, laquelle était la bonne. Évidemment, les cryptographes montèrent à leur tour au créneau, et exploitèrent la puissance des calculateurs électroniques pour créer des chiffres de plus en plus complexes. Ces calculateurs jouèrent un rôle capital après la guerre dans la lutte entre concepteurs et décrypteurs de codes.

Utiliser un ordinateur pour chiffrer un message ressemble, dans une large mesure, aux formes traditionnelles du chiffrement. Il y a cependant

trois différences essentielles. La première est que la machine à chiffrer mécanique (type Enigma, par exemple) est limitée à ce qui peut être construit en dur, alors qu'un ordinateur peut simuler une hypothétique machine à chiffrer d'une immense complexité. Un ordinateur peut être programmé pour simuler l'action de cent rotors, certains tournant dans le sens des aiguilles d'une montre, certains dans l'autre, d'autres disparaissant après dix lettres, d'autres encore tournant de plus en plus vite au fur et à mesure que le chiffrement avance. Une telle machine mécanique ne pourra être construite, mais son équivalent informatisé délivrera un chiffre remarquablement sûr.

La deuxième différence est une simple affaire de rapidité. Des brouilleurs électroniques opèrent beaucoup plus vite que des brouilleurs mécaniques : un ordinateur programmé pour appliquer un cryptosystème infiniment plus complexe pourrait encore effectuer sa tâche en un laps de temps raisonnable.

La troisième différence — et peut-être la plus significative — est qu'un ordinateur brouille des nombres plutôt que les lettres de l'alphabet. Les ordinateurs travaillent sur des nombres binaires — des suites de 1 et de 0 appelés chiffres binaires (*binary digits*) ou *bits* en abrégé. Avant tout chiffrement, un message est converti en nombres binaires. Cette conversion peut être effectuée selon divers protocoles, comme l'*American Standard Code for Information Interchange*, plus connu par son acronyme *ASCII*, prononcé Ass-Key en anglais (« la clef de l'âne »). ASCII assigne à chaque lettre de l'alphabet un nombre binaire à 7 chiffres. Pour l'instant, il nous suffit d'envisager chaque nombre binaire comme une simple suite de 1 et de 0, identifiant chaque lettre différemment ([tableau 24](#)), comme le code Morse identifiait chaque lettre avec une suite de traits et de points. Il y a 128 (2^7) manières de disposer une combinaison de 7 chiffres binaires, aussi ASCII peut-il représenter jusqu'à 128 caractères différents. Cela permet largement de définir toutes les lettres (exemple : $a = 1100001$), tous les signes de ponctuation (exemple : $! = 0100001$) et encore d'autres symboles (exemple : $\& = 0100110$). Une fois le message traduit en binaire, le chiffrement peut commencer.

A	1 0 0 0 0 0 1	N	1 0 0 1 1 1 0
B	1 0 0 0 0 1 0	O	1 0 0 1 1 1 1
C	1 0 0 0 0 1 1	P	1 0 1 0 0 0 0
D	1 0 0 0 1 0 0	Q	1 0 1 0 0 0 1
E	1 0 0 0 1 0 1	R	1 0 1 0 0 1 0
F	1 0 0 0 1 1 0	S	1 0 1 0 0 1 1
G	1 0 0 0 1 1 1	T	1 0 1 0 1 0 0
H	1 0 0 1 0 0 0	U	1 0 1 0 1 0 1
I	1 0 0 1 0 0 1	V	1 0 1 0 1 1 0
J	1 0 0 1 0 1 0	W	1 0 1 0 1 1 1
K	1 0 0 1 0 1 1	X	1 0 1 1 0 0 0
L	1 0 0 1 1 0 0	Y	1 0 1 1 0 0 1
M	1 0 0 1 1 0 1	Z	1 0 1 1 0 1 0

Tableau 24 Nombres binaires ASCII pour les lettres capitales.

Même si nous avons affaire à des ordinateurs et des nombres, et non plus à des machines et des lettres, le chiffrement s'effectue selon les vieux principes de substitution et de transposition, dans lesquels on remplace les éléments du message par d'autres éléments, ou bien on change les éléments de place, ou bien encore on fait les deux à la fois. Chaque chiffrement, aussi complexe qu'il soit, peut être ramené à des combinaisons de ces opérations simples. Les deux exemples suivants mettent en évidence la simplicité qui est à la base du chiffrement par ordinateur, en montrant comment un ordinateur peut appliquer un chiffre élémentaire de transposition.

D'abord, imaginons que nous voulons crypter le message HELLO, en utilisant une version ordinateur d'un chiffre de transposition. Avant de commencer le chiffrement, nous devons transcrire le message en ASCII selon le [tableau 24](#).

Texte clair : HELLO = 1001000 1000101 1001100 1001100 1001111

Une des formes de transposition les plus simples serait de permuter le premier chiffre avec le deuxième, le troisième avec le quatrième et ainsi de suite. Dans ce cas, le chiffre final resterait inchangé, puisqu'il y a un nombre impair de chiffres. Pour suivre cette opération plus clairement, j'ai supprimé les espaces entre les blocs ASCII dans le texte clair d'origine pour engendrer une unique séquence et je l'ai aligné au-dessus du texte chiffré final pour les comparer.

Texte clair : 10010001000101100110010011001001111
 Texte chiffré : 01100010001010011001100011000110111

Un intérêt de la transposition de chiffres binaires est que l'on peut effectuer cette transposition à l'intérieur même d'une lettre. On peut encore permuter les bits d'une lettre avec ceux de la lettre voisine. Par exemple, en échangeant les places de la septième et de la huitième lettre, le 0 final du H est permuté avec le 1 initial du E. Le message crypté est une simple séquence de 35 chiffres binaires qui peut être transmise au destinataire qui n'aura alors qu'à inverser la transposition pour reconstituer la séquence d'origine. Le récepteur retraduit via ASCII les chiffres binaires pour retrouver le message HELLO.

Maintenant, imaginons que nous voulions crypter le même message, HELLO, en employant cette fois la version ordinateur d'un chiffre de substitution. Comme d'habitude, la substitution repose sur une clef sur laquelle se sont entendus l'envoyeur et le receveur. Dans ce cas-ci, la clef est le mot DAVID traduit en ASCII, et on l'utilise de la manière suivante. Chaque bit du texte clair est additionné au bit correspondant de la clef. Additionner des chiffres binaires se fait selon deux simples règles. Si les éléments du texte clair et de la clef sont semblables, l'élément du texte clair est transformé en 0 dans le texte chiffré. Mais si les éléments de la clef et du message diffèrent, l'élément du texte clair est remplacé par 1 dans le texte chiffré.

Message :	H	E	L	L	O
Message en ASCII :	10010001000101100110010011001001111				
Clef : DAVID	10001001000001101011010010011000100				
Texte chiffré :	00011000000100001101000001010001011				

Le message crypté est une simple séquence de 35 chiffres binaires qui peut être transmise au destinataire, qui utilise la même clef pour inverser la substitution, retrouvant ainsi les chiffres binaires d'origine. Il retraduit ces chiffres via ASCII pour reconstituer le message HELLO.

Au départ, le cryptage électronique était réservé à ceux qui possédaient des ordinateurs, c'est-à-dire le gouvernement et l'armée. Mais grâce à une série de progrès scientifiques, techniques et conceptuels, les ordinateurs et le chiffrement par ordinateur se répandaient. En 1947, les laboratoires AT&T Bell inventèrent le transistor, une alternative bon marché à la valve électronique. L'informatique commerciale devint une réalité lorsqu'en 1951 des entreprises comme Ferranti commencèrent à fabriquer des ordinateurs sur commande. En 1953, IBM lança son premier ordinateur, et quatre ans

plus tard présentait *Fortran*, un langage de programmation qui permettait à des gens « ordinaires » d'utiliser les programmes des ordinateurs. Puis, en 1959, l'invention du circuit intégré marqua le début d'une nouvelle ère de l'informatique.

Dans les années 60, les ordinateurs devinrent plus puissants, en même temps qu'ils devenaient moins chers. Les entreprises en achetaient de plus en plus volontiers, et, comme le chiffrement se répandait, les cryptographes furent confrontés à de nouveaux problèmes qui ne s'étaient pas posés aussi longtemps que la cryptographie était restée l'apanage des gouvernements et des armées. L'un des premiers soucis fut de trouver le moyen de standardiser les procédés. Une société pouvait utiliser un cryptosystème particulier pour protéger ses communications internes, mais ne pouvait pas l'utiliser pour un message destiné à un organisme extérieur, à moins que le récepteur n'utilisât le même système ; sinon le message ne pouvait être décrypté. Finalement, le 15 mai 1973, le National Bureau of Standards américain demanda que soit créé un système standard de chiffrement qui permettrait aux milieux d'affaires de s'entretenir en toute confidentialité.

L'un des algorithmes de chiffrement les plus reconnus, et candidat pour être choisi comme système standard, était une conception d'IBM appelée *Lucifer*. Il avait été établi par Horst Feistel, un émigré allemand arrivé en Amérique en 1934. On allait lui accorder la citoyenneté américaine lorsque l'Amérique entra en guerre, et il se retrouva en résidence surveillée jusqu'en 1944. Pendant les années qui suivirent, il préféra ne pas s'intéresser à la cryptographie pour éviter d'être inquiété par les autorités américaines. Lorsqu'il reprit ses recherches sur les chiffres, au *Air Force's Cambridge Research Center*, il se trouva vite en difficulté avec l'Agence nationale de sécurité (NSA), l'organisation responsable de la sécurité des communications militaires et gouvernementales, chargée également de l'interception et du déchiffrement des communications de l'étranger. Elle est la meilleure au monde pour fourrer son nez partout.

La NSA ne reprochait pas à Feistel ses origines, elle voulait seulement garder le monopole de la recherche en cryptographie, et il semble bien qu'elle réussit à faire annuler le projet de recherche de Feistel. Dans les années 60, Feistel partit à la *Mitre Corporation*, mais la NSA ne le lâcha pas et le contraignit à renoncer une deuxième fois à son emploi. Feistel arriva finalement dans le laboratoire T. J. Watson d'IBM, près de New

York, où pendant quelques années il put poursuivre ses recherches sans ennui. C'est là, au début des années 70, qu'il conçut le système Lucifer.

Lucifer crypte les messages en appliquant les opérations de brouillage suivantes. D'abord, le message est traduit en une longue suite de nombres binaires (bits). Cette suite est répartie en blocs de 64 bits et le cryptage est effectué séparément sur chaque bloc. En s'attaquant à un seul bloc, on brasse les 64 bits, puis on les sépare en deux demi-blocs de 32, appelé Gauche⁰ et Droite⁰ (G^0 et D^0). On applique ensuite à D^0 une fonction de permutation qui change les bits selon une substitution complexe. Le D^0 est, après cette intervention, ajouté au G^0 pour trouver un nouveau demi-bloc de 32 bits appelé D^1 . Le D^0 d'origine est rebaptisé G^1 . On appelle cet enchaînement d'opérations un cycle. Le processus est répété pour un deuxième cycle, qui part des nouveaux demi-blocs G^1 et D^1 et qui termine en G^2 et D^2 . Ce processus sera répété seize fois en tout. L'opération de chiffrement peut être comparée à la fabrication de la pâte feuilletée. Imaginons une longue bande de pâte avec un message écrit dessus. On découpe d'abord la bande en morceaux de 64 cm de long. Ensuite on prend la moitié d'un des morceaux, on le pétrit, on le replie, on l'ajoute à l'autre moitié et l'on étire le tout pour en faire une nouvelle bande. On répète le procédé jusqu'à ce que le message ait été complètement brouillé. Après seize tours, on envoie le texte chiffré, qui sera déchiffré en inversant le procédé.

Les modalités précises de la fonction de transformation peuvent varier et sont déterminées par une clef choisie par l'expéditeur et le destinataire. En d'autres termes, le même message peut être crypté selon une myriade de manières différentes, suivant la clef retenue. Les clefs utilisées dans la cryptographie par ordinateur sont de simples nombres. L'expéditeur et le destinataire doivent donc fixer ce nombre pour décider de la clef. Ensuite, pour chiffrer, l'expéditeur entre le nombre-clef et le message dans Lucifer, qui émet le texte chiffré. Pour décrypter, le destinataire entre la même clef et le texte chiffré dans Lucifer, qui ressort le texte original.

Lucifer fut généralement jugé l'un des plus sûrs cryptosystèmes sur le marché et fut donc utilisé par un grand nombre d'organismes. Il semblait inévitable qu'il soit adopté comme standard américain de chiffrement, mais, à nouveau, la NSA s'opposa aux travaux de Feistel. Lucifer offrait la possibilité d'un schéma de chiffrement que la NSA n'aurait peut-être pas toujours été capable de briser. On murmure qu'elle s'arrangea pour

affaiblir l'un des points forts de Lucifer — le nombre possible de clefs — avant de lui permettre d'être adopté comme référence.

Le nombre de clefs possibles est l'un des composants les plus importants pour la sécurité d'un chiffrement. Un cryptanalyste essayant de déchiffrer un message crypté peut tenter de vérifier toutes les clefs possibles, et plus le nombre de clefs est élevé, plus ces vérifications demanderont du temps. S'il n'y a qu'un million de clefs possibles, un cryptanalyste armé d'un ordinateur assez puissant peut trouver la bonne en quelques minutes, et déchiffrer un message intercepté. Mais si le nombre de clefs est suffisamment élevé, cela devient impossible. Si Lucifer devait être le système retenu, la NSA voulait être sûre qu'il n'opérerait qu'avec un nombre relativement restreint de clefs.

La NSA plaida donc pour une limitation du nombre de clefs à environ 100 000 000 000 000 000 (soit une clef de chiffrement de 56 bits, puisque ce nombre s'écrit en 56 chiffres binaires). Elle semblait croire qu'une telle clef apporterait une confidentialité suffisante pour le public, car aucun organisme privé ne disposait d'un ordinateur capable de vérifier un tel nombre de clefs en un temps raisonnable. La NSA elle-même, d'ailleurs, bien qu'équipée des plus grandes ressources en informatique au monde, serait tout juste capable de venir à bout des messages. Le chiffre Lucifer de Feistel dans sa version à 56 bits fut adopté officiellement le 23 novembre 1976 et appelée Data Encryption Standard (DES). Un quart de siècle plus tard, le DES demeure la norme américaine officielle de chiffrement. L'adoption du DES résolvait le problème de la normalisation et encourageait les échanges commerciaux à utiliser la cryptographie pour assurer leur sécurité. De plus, DES était assez fort pour les protéger contre les attaques de concurrents. Il était impossible pour une entreprise équipée d'un ordinateur civil de décrypter un message saisi, en raison du nombre très élevé de clefs possibles. Toutefois, malgré la standardisation et la force du DES, on se trouvait devant un autre problème majeur, celui de la *distribution de la clef*.

Imaginons qu'une banque souhaite envoyer à un client des données confidentielles par téléphone, mais craigne une écoute sur la ligne. La banque choisit une clef et utilise le DES pour crypter les données. Pour décrypter le message, le client aura non seulement besoin du logiciel DES sur son ordinateur, mais aussi de savoir quelle clef a été utilisée pour ce message. Comment la banque va-t-elle faire savoir à son client de quelle clef il s'agit ? Elle ne peut l'acheminer par téléphone. Le seul moyen vraiment sûr serait de remettre soi-même la clef à la personne

concernée, ce qui évidemment prendrait du temps. Un moyen moins sûr, mais plus pratique, est d'envoyer la clef par la poste. Dans les années 70, les banques essayèrent de faire distribuer les clefs par des coursiers spécialement sélectionnés, qui comptaient parmi les employés les plus sûrs de l'entreprise. Ces messagers devaient courir le monde munis de cartables cadenassés, et remettre en mains propres les clefs aux destinataires des messages de la banque la semaine suivante. Plus les contacts se multipliaient, plus les réseaux s'étendaient, et tant de clefs durent être distribuées que la logistique nécessaire, avec ses frais prohibitifs, devint un véritable cauchemar.

Ce problème de distribution de la clef a été le fléau constant des cryptographes au cours de l'histoire. Pendant la Seconde Guerre mondiale, le haut commandement allemand devait ainsi distribuer le registre mensuel des clefs quotidiennes à tous les opérateurs d'Enigma, ce qui constituait un problème de logistique considérable. Les sous-marins allemands, de même, en raison de longues périodes passées loin de leurs bases, devaient d'une façon ou d'une autre être alimentés en clefs. Plus loin de nous, les utilisateurs du chiffre de Vigenère devaient trouver un moyen pour transmettre le mot-clef de l'expéditeur au destinataire. Aussi sûr que soit un chiffrement en théorie, il est fragilisé en pratique par le problème de distribution de la clef.

Dans une certaine mesure, les gouvernements et les armées ont pu résoudre ce problème en y consacrant beaucoup d'efforts et en ne ménageant pas les investissements. Leurs messages sont d'une telle importance qu'ils iront aussi loin que nécessaire pour assurer une distribution sûre de la clef. Les clefs du gouvernement américain sont gérées et distribuées par la COMSEC, abrégé de *Communications Security*. Dans les années 70, la COMSEC acheminait des tonnes de clefs chaque jour. Quand des bateaux transportant du matériel de la COMSEC arrivaient à quai, des crypto-gardes montaient à bord, récupéraient des tas de cartes, des rouleaux de papier, des disques souples, ou n'importe quel autre support sur lequel les clefs avaient été stockées, et les portaient à leurs destinataires.

La distribution des clefs peut sembler une question annexe, mais elle constitua le problème primordial pour les cryptographes de l'après-guerre. Si deux personnes voulaient communiquer en toute sûreté, elles devaient s'en remettre à une troisième pour acheminer la clef, et ce maillon était le plus faible de la chaîne. Pour les transactions commerciales, le dilemme se posait clairement : si les gouvernements,

avec tout leur argent, avaient peine à garantir la sécurité de leurs clefs, comment des entreprises civiles pourraient-elles jamais espérer jouir d'une distribution de clefs sûre et non ruineuse ?

Vers 1975, enfin, une bande de francs-tireurs trouva la solution de ce problème réputé insoluble. Ils mirent au point un système de chiffrement qui semblait défier toute logique. Si les ordinateurs ont transformé l'application du chiffrement, la plus grande révolution du XX^e siècle a été le développement des techniques pour résoudre le problème de distribution des clefs. Aussi cette découverte est-elle considérée comme la plus grande réussite en cryptologie depuis l'invention du chiffre monoalphabétique, il y a plus de deux mille ans.

Bienheureux les fous...

Whitfield Diffie est l'un des plus extravagants cryptographes de sa génération. Sa seule apparence donne de lui une image surprenante et quelque peu contradictoire. Son costume impeccable reflète sa carrière pendant les années 90 dans l'une des compagnies géantes américaines d'informatique — son poste était officiellement celui d'ingénieur en chef chez Sun-Microsystems. En même temps, sa chevelure tombant sur les épaules et sa longue barbe blanche trahissent ses attaches sentimentales aux années 60. Il passe la plus grande partie de son temps dans une salle d'ordinateurs, mais il serait aussi à sa place dans un ashram à Bombay.

Diffie est né en 1944 et a passé ses jeunes années dans le Queens à New York. Enfant, il se passionnait pour les mathématiques et ses lectures allaient de *The Chemical Rubber Company Handbook of Mathematic Tables* au *Course of Pure Mathematics* de G.H. Hardy. Il alla ensuite étudier les mathématiques au *Massachusetts Institute of Technology*, dont il sortit diplômé en 1965. Il travailla alors dans plusieurs entreprises à la sécurité des ordinateurs, et devint l'un des rares experts en sécurité absolument indépendant, un cryptologue libre-penseur, ne servant ni le gouvernement ni aucune grande compagnie — le premier *punk* du chiffrement.

Diffie s'intéressa tout particulièrement au problème de la distribution des clefs, et il comprit que celui qui y apporterait une solution gagnerait sa place au panthéon de la cryptographie. Ce sujet l'obséda tellement qu'il occupe la plus grosse part de son carnet de notes personnelles intitulé *Problèmes pour une théorie ambitieuse de la cryptographie*. La motivation de Diffie devait beaucoup à sa vision d'un monde câblé. Dès les années 60, le Département américain de la Défense avait créé un organisme de recherches avancées, l'ARPA, *Advanced Research Projects Agency*, dont l'un des objectifs prioritaires était de connecter des ordinateurs militaires sur de grandes distances, pour permettre à un ordinateur endommagé de transférer sa mission à n'importe quel autre du réseau. Le but était d'abord de renforcer l'infrastructure informatique du Pentagone face à une attaque nucléaire, mais le réseau allait également permettre aux scientifiques de communiquer entre eux et d'exploiter les possibilités de calcul de machines éloignées. Le réseau ARPA —

ARPANet —fut créé en 1969, et dès la première année, il reliait quatre sites. Il se développa ensuite sans arrêt, et en 1982 il engendra Internet. À la fin des années 80, les utilisateurs qui n'étaient membres ni des organismes d'État, ni des centres de recherches universitaires, se virent ouvrir l'accès à Internet et le nombre des navigateurs sur le réseau se multiplia. Aujourd'hui, plus de cent millions de personnes échangent des informations et envoient du courrier électronique, les *e-mails*, sur Internet.

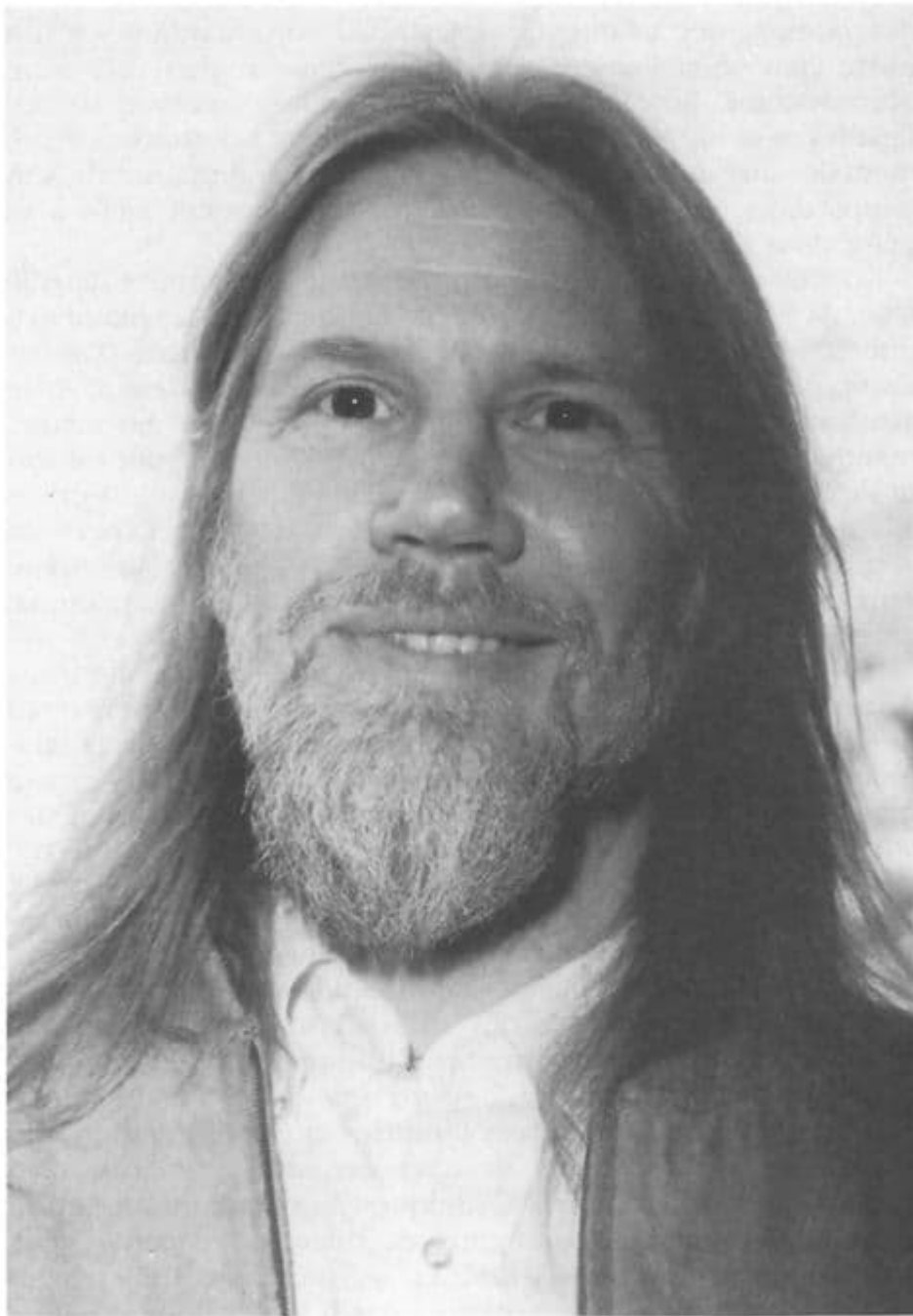


Fig. 62 Whitfield Diffie.

Alors que l'ARPANet en était encore à ses débuts, Diffie fut suffisamment clairvoyant pour pressentir l'avènement des autoroutes de l'information et la révolution informatique. Tout le monde aurait un jour son ordinateur personnel, et les ordinateurs seraient reliés entre eux par des lignes téléphoniques. Diffie pensait que, si les gens pouvaient alors échanger des *e-mails*, ils seraient justifiés à demander de crypter leurs messages pour en garantir la confidentialité. Et le chiffrement exigeait l'échange de clefs. Si les gouvernements et les grands groupes industriels avaient de si grandes difficultés à résoudre ce problème, ce serait tout à fait impossible pour le public, qui n'aurait donc pas droit à la confidentialité.

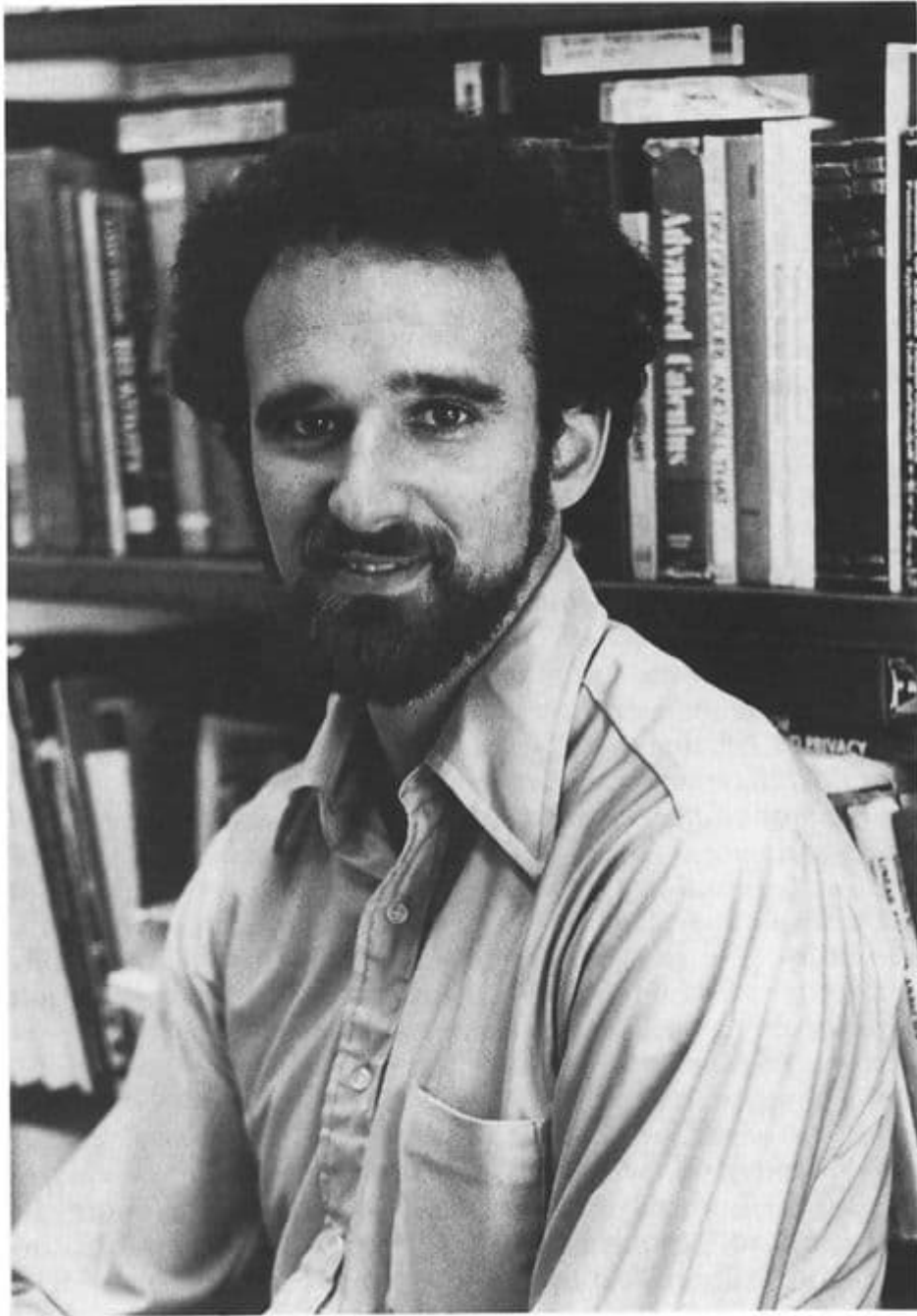
Diffie imagina deux personnes étrangères se rencontrant *via* Internet, et il se demanda comment elles pourraient s'adresser l'une à l'autre un message crypté. Il envisagea aussi le cas de quelqu'un souhaitant acheter un produit sur Internet. Comment pourrait-il envoyer par un *e-mail* des précisions sur sa carte de crédit en les cryptant de telle manière que seul le négociant puisse les déchiffrer ? Dans les deux cas il semblait que les deux parties devaient partager une clef, mais comment échanger cette clef ? Le nombre d'échanges commerciaux courants et la croissance spontanée du nombre d'*e-mails* dans le public atteindraient des chiffres énormes et rendraient impraticables la distribution de clefs.

En 1974, Diffie, toujours cryptographe indépendant, fut invité au laboratoire Thomas J. Watson d'IBM pour y donner une conférence. Il parla d'un certain nombre de stratégies ébauchées pour attaquer le problème de la distribution des clefs, mais ce n'étaient encore que des balbutiements, et son auditoire était sceptique sur les chances d'aboutissement. Le seul écho positif à l'exposé de Diffie vint d'Alan Konheim, un des principaux spécialistes d'IBM pour la cryptographie, qui mentionna que quelqu'un d'autre était venu récemment au laboratoire faire un exposé sur le même problème. Cet autre chercheur s'appelait Martin Hellman, et il était professeur à l'université Stanford, en Californie. Le soir même, Diffie prenait le volant pour faire les 5 000 kilomètres qui le séparaient de la côte Ouest, afin de rencontrer la seule personne qui semblait partager son idée fixe.

Martin Hellman est né en 1945 dans un quartier juif du Bronx, mais il n'avait que quatre ans lorsque sa famille déménagea et se retrouva dans un voisinage à prédominance catholique irlandais. Selon Hellman, cela influa sur son comportement dans la vie : « Les autres enfants allaient à l'église où ils apprenaient que les juifs avaient tué Jésus, et j'y gagnais le

surnom de “tueur du Christ”. Je me suis aussi fait battre. Pour commencer, je voulais être comme les autres, avoir un arbre de Noël et des cadeaux. Mais ensuite j’ai compris que c’était impossible et, dans un réflexe d’autodéfense, j’adoptai une attitude du genre *qui voudrait ressembler à tout le monde* ? ». Hellman situe la source de son intérêt pour le chiffrement dans ce désir de différence. Ses collègues lui avaient dit qu’il était fou de prétendre entrer en concurrence avec la NSA et son budget de plusieurs milliards de dollars. Comment pouvait-il espérer découvrir quelque chose qu’elle n’aurait pas déjà trouvé ? Et, s’il découvrait tout de même quelque chose, la NSA le classerait aussitôt confidentiel-défense.

Alors qu’il commençait ses recherches, Hellman tomba sur le livre de l’historien David Kahn, *The Codebreakers*. Cet ouvrage offrait le premier tableau précis du développement des chiffres et constituait la meilleure approche possible pour un cryptographe en herbe. *The Codebreakers* fut le seul compagnon de Hellman dans ses travaux, jusqu’en septembre 1974, date à laquelle il reçut un appel téléphonique inopiné de Whitfield Diffie, qui avait traversé le continent pour le rencontrer. Hellman comprit vite que Diffie était la personne la mieux informée qu’il eût jamais rencontrée. Il se souvient : « J’avais promis à ma femme de rentrer à la maison pour m’occuper des enfants, aussi je le ramenai avec moi et nous avons dîné ensemble. Il partit vers minuit. Nos personnalités sont très différentes — il est beaucoup plus “contre-culture” que moi — mais finalement l’opposition de nos caractères réussit une symbiose. C’était pour moi un tel souffle d’air. Travailler seul dans le vide avait été vraiment éprouvant. »



[Fig. 63](#) Martin Hellman.

Hellman n'avait pas de budget pour recruter sa nouvelle âme sœur sur un poste permanent, et il dut embaucher Diffie comme boursier de thèse ! Ils attaquèrent ensemble le problème de la distribution des clefs, cherchant désespérément à trouver une alternative à l'épuisante cavalcade à travers le monde pour transporter physiquement les clefs. Ils furent bientôt rejoints par Ralph Merkle. Merkle était un émigré d'un autre groupe de recherche, dont le directeur n'éprouvait aucun intérêt pour le rêve impossible de la distribution de clefs. Hellman raconte :

Comme nous, Ralph était un peu fou. Il faut être fou pour mener jusqu'au bout une recherche originale, et seuls des fous la poursuivront envers et contre tout. Vous avez une première idée, vous vous enthousiasmez, et ça ne marche pas. Alors vous passez à l'idée numéro 2, vous vous enthousiasmez, et ça ne marche pas. Alors vous avez l'idée 99, vous vous enthousiasmez, et ça ne marche pas. Seul un fou sera encore enthousiaste à sa centième idée, et il faudra peut-être avoir essayé cent voies avant que l'une conduise quelque part. À moins d'être assez fou pour retrouver à chaque fois tout votre enthousiasme, vous vous découragerez, et n'aurez pas l'énergie de mener les choses jusqu'au bout. Dieu bénit les fous.

L'ensemble des problèmes liés à la distribution des clefs est l'exemple même du cercle vicieux, puisque, avant que deux personnes échangent un secret (le message crypté), elles doivent déjà partager un secret (la clef).

Prenons Alice, Bernard et Ève, trois personnages imaginaires qui sont devenus des acteurs cryptographiques adoptés par tout le monde. Alice veut envoyer un message à Bernard, et Eve les espionne. Si Alice adresse des messages secrets à Bernard, elle utilise une clef pour crypter chacun d'eux. Elle est donc confrontée au problème de la distribution des clefs qu'elle doit faire parvenir à Bernard. Un moyen de le résoudre est qu'Alice et Bernard se rencontrent une fois par semaine et se communiquent alors suffisamment de clefs pour l'ensemble des messages qu'ils s'adresseront pendant les sept jours suivants. Échanger physiquement les clefs est un moyen sûr, mais peu commode, et si Alice ou Bernard tombe malade, le système s'effondre. Ils pourraient utiliser des coursiers ; ce serait plus onéreux et surtout moins sûr, mais au moins une partie du travail serait déléguée. Dans tous les cas, la distribution des clefs semble indispensable. Pendant deux cents ans ce fut un axiome cryptographique, une vérité indiscutable. Pourtant, il existe une expérience qui semblait défier cet axiome.

Imaginez qu'Alice et Bernard habitent un pays où le système postal est absolument amoral et où les employés de la poste lisent toutes les correspondances non closes. Un jour, Alice veut envoyer un message extrêmement personnel à Bernard. Elle le met dans une boîte en fer qu'elle ferme avec un cadenas et une clef. Elle envoie par la poste la

boîte verrouillée et garde la clef. Évidemment, lorsque la boîte parvient à Bernard, il ne peut l'ouvrir puisqu'il n'a pas la clef. Alice peut envisager de mettre la clef dans une autre boîte, de la verrouiller et de l'envoyer à Bernard, mais sans la clef de la seconde boîte il ne pourra l'ouvrir — et n'aura toujours pas accès à la clef de la première. La seule façon de tourner la question serait qu'Alice fasse faire une copie de sa clef et la donne à Bernard à l'avance. Jusqu'ici, c'est le même vieux problème habillé d'un nouveau scénario. Alice doit forcément donner à Bernard une copie de sa clef si elle veut enfermer quelque chose dans une boîte qu'il puisse seul ouvrir.

Maintenant passons au scénario suivant. Alice veut toujours envoyer un message à Bernard. Elle confie à nouveau son secret à un coffret en fer, le verrouille et l'envoie à Bernard. Lorsque le coffret lui parvient, Bernard ajoute son propre cadenas et renvoie la boîte à Alice. Alice reçoit donc un coffret muni maintenant de deux cadenas. Elle retire le sien, ne laissant que celui de Bernard pour fermer le coffret. Enfin, elle le retourne à Bernard. Et là est toute la différence : maintenant, Bernard peut ouvrir le coffret, puisqu'il n'est verrouillé que par son propre cadenas, dont il détient seul la clef.

Les implications de cette petite histoire sont énormes. Elle prouve qu'un message secret peut être acheminé sans risque entre deux personnes en se dispensant de l'échange de clef. Pour la première fois, nous voyons suggérer que cet échange n'est peut-être pas une nécessité absolue en cryptographie. Alice utilise sa propre clef pour crypter le message pour Bernard, qui le crypte à son tour selon sa clef personnelle et le renvoie. Quand Alice reçoit le message deux fois crypté, elle supprime son propre chiffrement et le retourne à Bernard, qui à son tour supprime son chiffrement et lit le message.

Il semble qu'on pourrait résoudre ainsi la question de la distribution des clefs, puisque le schéma à double chiffrement ne requiert pas cet échange. Pourtant, il reste un obstacle fondamental pour appliquer ce système où Alice chiffre, Bernard chiffre, Alice déchiffre, et Bernard déchiffre. Le problème est l'ordre dans lequel les chiffrements et déchiffrements sont exécutés. En principe, l'ordre du chiffrement et du déchiffrement est capital, et doit obéir à la maxime « dernier mis, premier enlevé ». Le matin, nous mettons nos chaussettes, puis nos chaussures, et le soir nous retirons nos chaussures avant nos chaussettes — impossible d'enlever les chaussettes avant les chaussures. Nous devons nous plier à la maxime « dernier mis, premier enlevé ». En

d'autres termes, le dernier chiffrement effectué devrait être le premier à être décrypté. Dans le scénario ci-dessus, Bernard était le dernier à chiffrer, son chiffrement aurait donc dû être décrypté le premier, alors que nous avons vu Alice supprimer son chiffrement d'abord, avant que Bernard touche au sien.

Quelques chiffres très élémentaires, tel le chiffre de César, sont si simples que l'ordre importe peu. Cependant, dans les années 70, il semblait que tout chiffrement efficace obéissait à la règle du « dernier mis, premier enlevé ». Si un message est chiffré avec la clef d'Alice, puis avec celle de Bernard, il doit alors être déchiffré avec la clef de Bernard avant d'être déchiffré avec la clef d'Alice. L'enchaînement est crucial, même avec un chiffre de substitution monoalphabétique. Imaginons qu'Alice et Bernard aient chacun leur clef, comme on le verra ci-dessous, et regardons ce qui se passe lorsque la chronologie n'est pas respectée. Alice utilise sa clef pour crypter le message pour Bernard, et Bernard crypte ce message déjà chiffré de nouveau avec sa propre clef. Alice utilise sa clef pour effectuer un déchiffrement partiel et Bernard utilise la sienne pour terminer le déchiffrement.

Clef d'Alice

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
H	F	S	U	G	T	A	K	V	D	E	O	Y	J	B	P	N	X	W	C	Q	R	I	M	Z	L

Clef de Bernard

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C	P	M	G	A	T	N	O	J	E	F	W	I	Q	B	U	R	Y	H	X	S	D	Z	K	L	V

Message	v	o	i	s	m	o	i	à	m	i	d	i
Crypté avec la clef d'Alice	R	B	V	W	Y	B	V	H	Y	V	U	V
Crypté avec la clef de Bernard	Y	P	D	Z	L	P	D	O	L	D	S	D
Décrypté avec la clef d'Alice	M	P	J	Y	Z	P	J	L	Z	J	C	J
Décrypté avec la clef de Bernard	c	b	i	r	w	b	i	y	w	i	a	i

Ce résultat n'a pas de sens. Pourtant, vous pouvez vérifier par vous-même que si l'ordre des déchiffrements était inversé et que Bernard déchiffre avant Alice, le résultat donnerait bien le message d'origine. Mais si l'ordre est tellement important, pourquoi le système des cadenas marchait-il si bien dans l'anecdote des boîtes ? La réponse est que l'ordre importe peu dans ce cas. Je peux mettre vingt cadenas sur une

boîte et les défaire dans n'importe quel ordre, la boîte finira par être ouverte. Malheureusement, les systèmes de chiffrement sont beaucoup plus susceptibles que les cadenas sous ce rapport.

Bien que le système du coffret aux deux cadenas ne puisse s'appliquer à la cryptographie, Diffie et Hellman s'en inspirèrent pour chercher une méthode qui contournerait le problème de la distribution de clefs. Ils passèrent des mois à chercher une solution. Chaque idée aboutissait à un échec, mais ils agissaient en bons fous, et persévéraient. Ils concentrèrent leur recherche sur diverses *fonctions* mathématiques. Une fonction est n'importe quelle opération qui transforme un nombre en un autre nombre. Par exemple *doubler* est une fonction, puisque cette opération transforme le 3 en 6, ou le 9 en 18. De plus, nous pouvons envisager toutes les formes de chiffrement informatique comme des fonctions, puisqu'elles transforment un nombre — le texte clair — en un autre nombre, le texte chiffré.

La plupart des fonctions mathématiques sont réversibles, puisqu'elles sont aussi simples à défaire qu'à faire. *Doubler* est ainsi réversible puisqu'il est facile de retrouver le nombre d'origine à partir de son double. Si nous savons que le résultat du doublement est 26, il est enfantin de déduire que le nombre d'origine est 13.

Diffie et Hellman n'étaient pas intéressés par ces fonctions réversibles. Leur centre d'intérêt était les fonctions à sens unique. Comme leur nom le suggère, ces fonctions sont faciles à appliquer, mais très difficiles à inverser : elles sont virtuellement *non-irréversibles*. Voyons à nouveau un exemple du quotidien. Mélanger de la peinture jaune et de la peinture bleue pour obtenir du vert est une fonction à sens unique, puisqu'il est facile de mélanger les peintures et impossible de retrouver les couleurs d'origine. Une autre fonction à sens unique est de casser un œuf, car il vous est impossible ensuite de le reconstituer.

L'arithmétique modulo, parfois appelée à l'école *arithmétique de l'horloge*, est un domaine des mathématiques riche en fonctions à sens unique. Dans l'arithmétique modulo, les mathématiciens considèrent un ensemble fini de nombres arrangés en boucle, un peu comme les nombres sur une horloge. La [figure 64](#) montre une horloge pour un modulo 7 (ou mod 7) qui a seulement 7 nombres de 0 à 6. Pour effectuer $2 + 3$, nous partons de 2 et nous avançons de 3 places pour arriver à 5, ce qui donne la même réponse que l'arithmétique normale. Pour faire $2 + 6$,

nous partons de 2 et avançons de 6 places, mais cette fois nous avons effectué un tour complet sur la boucle et nous atteignons le 1, qui n'est pas le résultat habituel en arithmétique. Ces résultats peuvent s'exprimer ainsi :

$$2 + 3 = 5 \pmod{7} \text{ et } 2 + 6 = 1 \pmod{7}$$

L'arithmétique modulo est relativement simple, et nous l'utilisons tous les jours lorsque nous parlons de l'heure. S'il est 9 heures maintenant, et que nous avons un rendez-vous dans 8 heures d'ici, nous pouvons dire que notre rencontre aura lieu à 5 heures de l'après-midi, plutôt qu'à 17 heures. Nous avons calculé mentalement $9 + 8 \pmod{12}$. Imaginons le cadran de l'horloge, regardons le 9, puis tournons de 8 places, et nous arrivons à 5 :

$$9 + 8 = 5 \pmod{12}$$

Plutôt que de visualiser des horloges, les mathématiciens appliquent souvent la recette suivante pour abréger les calculs de modulo. Effectuons d'abord le calcul en arithmétique normale. Ensuite, pour connaître le résultat en $\pmod{x}$, divisons la réponse normale par x et notons le reste. Ce reste constitue la réponse en $\pmod{x}$. Pour trouver la réponse à $11 \times 9 \pmod{13}$, nous procédons comme suit :

$$\begin{aligned} 11 \times 9 &= 99 \\ 99 : 13 &= 7, \text{ reste } 8 \\ 11 \times 9 &= 8 \pmod{13} \end{aligned}$$

Les fonctions effectuées en arithmétique modulo tendent à se comporter de manière erratique, ce qui les transforme parfois en fonction à sens unique. Cela devient évident lorsqu'une fonction simple en arithmétique normale est comparée à la même fonction en arithmétique modulo. Dans la première, la fonction sera à double sens et aisément inversible. Dans la seconde, elle sera à sens unique et difficilement inversible. Prenons par exemple la fonction 3^x . Cela veut dire : prendre un nombre (x), puis multiplier 3 par lui-même x fois pour trouver le nouveau nombre. Si $x = 2$, effectuons cette opération :

$$3^x = 3^2 = 3 \times 3 = 9$$

Autrement dit, la fonction transforme 2 en 9. En arithmétique ordinaire, plus la valeur de x croît, plus le résultat croît. Si l'on nous donnait le résultat de l'opération, il nous serait assez facile de revenir en arrière et de déduire le nombre d'origine. Si le résultat est 81, on peut en déduire que $x = 4$, puisque $3^4 = 81$. Si nous nous trompons et croyons que $x = 5$, nous trouverons que $3^5 = 243$, ce qui nous prouve que notre valeur attribuée à x était trop grande. Bref, même si nous nous trompons, nous pouvons retrouver l'exacte valeur de x et effectuer à l'envers la fonction.

En arithmétique modulo, cette même fonction ne se comporte pas si raisonnablement. Imaginons que l'on nous dise que 3^x en modulo 7 = 1, et que l'on nous demande de trouver la valeur de x . Aucune valeur ne nous vient à l'esprit, car nous sommes peu familiers, pour la plupart, avec l'arithmétique modulo. Nous pouvons supposer que $x = 5$ et chercher le résultat de $3^5 \pmod{7}$. Le résultat donnera 5, ce qui est trop élevé puisque nous cherchons un résultat égal à 1. Nous pouvons être tentés de réduire la valeur de x et d'essayer à nouveau. Mais nous irons dans la mauvaise direction puisque la réponse exacte est $x = 6$.

En arithmétique normale, nous pouvons essayer des nombres et sentir si nous brûlons ou si nous gelons. Le contexte de l'arithmétique modulo n'offre pas de prises utiles, et inverser les fonctions est bien difficile. Souvent, le seul moyen pour inverser une fonction en modulo est de constituer une table en calculant la fonction avec diverses valeurs attribuées à x , jusqu'à ce que l'on tombe sur la bonne solution. Le [tableau 25](#) montre les résultats obtenus en appliquant plusieurs valeurs à la fonction, à la fois en arithmétique normale et en arithmétique modulo. Si établir une telle table est un peu fastidieux lorsqu'on travaille sur d'assez petits nombres, cela devient extrêmement pénible avec une fonction comme $453^x \pmod{21\,997}$. C'est un exemple classique de fonction à sens unique, car je peux attribuer une valeur à x et calculer le résultat de la fonction, mais si je vous donne un résultat, disons 5 787, vous aurez une immense difficulté à inverser la fonction et à trouver quel x j'avais déterminé. Il ne m'a fallu que quelques secondes pour effectuer mon calcul, mais il vous en coûtera des heures pour établir une table et trouver l' x que j'avais choisi.

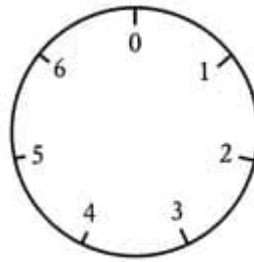


Fig. 64 L'arithmétique modulo s'effectue sur un ensemble fini de nombres, qu'on peut représenter comme des chiffres sur le cadran de l'horloge. Dans le cas montré ici, nous pouvons effectuer $6 + 5$ en module 7 en partant de 6 et en tournant de cinq espaces, ce qui nous amène à 4.

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
$3^x \pmod{7}$	3	2	6	4	5	1

Tableau 25 Valeurs de la fonction 3^x calculées en arithmétique normale (ligne 2) et arithmétique modulo (ligne 3). La fonction est croissante régulièrement en arithmétique normale, mais est erratique en arithmétique modulo.

Après deux années consacrées à l'arithmétique modulo et aux fonctions à sens unique, la fantaisie de Hellman commença à se révéler payante. Au printemps 1976, il eut l'idée d'une stratégie résolvant le problème de l'échange de clefs. En une demi-heure de gribouillage frénétique, il prouva qu'Alice et Bernard pouvaient convenir d'une clef sans se rencontrer, Hellman rendait ainsi caduc un axiome qui avait fait la loi pendant des siècles. Son idée reposait sur une fonction à sens unique de forme $Y^x \pmod{P}$. D'abord, Alice et Bernard se concertaient sur les valeurs attribuées à Y et P . À peu près toutes les valeurs sont possibles, avec cependant quelques restrictions, telles que : P doit être premier et Y inférieur à P . Ces valeurs ne sont pas secrètes, aussi Alice peut-elle téléphoner à Bernard et suggérer, disons, que $Y = 7$ et $P = 11$. Même si la ligne téléphonique n'est pas sûre et que la malveillante Ève écoute la conversation, c'est sans importance, comme nous allons le voir. Alice et Bernard sont maintenant convenu de la fonction à sens unique $7^x \pmod{11}$. À cet instant, ils peuvent entamer le processus visant à établir une clef secrète sans se rencontrer. Comme ils travaillent en parallèle, j'expose leurs actions en deux colonnes dans le [tableau 26](#).

Ayant suivi les étapes du [tableau 26](#), nous voyons que, sans se rencontrer, Alice et Bernard ont défini la même clef, qu'ils peuvent utiliser pour chiffrer un message. Par exemple, ils peuvent utiliser leur nombre, 9, comme clef pour un chiffrement en DES (le DES utilise en vérité des nombres beaucoup plus grands comme clef, et le processus

décrit dans le [tableau 26](#) serait effectué avec des nombres beaucoup plus importants, afin d'en tirer une clef de DES suffisamment conséquente). En appliquant le schéma d'Hellman, Alice et Bernard ont pu s'accorder sur une clef, sans avoir à se rencontrer et à se la murmurer à l'oreille. Le plus remarquable est que la clef secrète a été fixée en échangeant des informations sur une ligne téléphonique banale. Mais si Ève avait espionné cette ligne, alors elle connaîtrait sûrement elle aussi la clef ?

Examinons le schéma d'Hellman du point de vue d'Ève. Si elle écoute la conversation, elle ne connaît que les éléments suivants : que la fonction est $7^x \pmod{11}$, qu'Alice envoie $\alpha = 2$ et que Bernard envoie $\beta = 4$. Pour trouver la clef, elle doit faire ce que fait Bernard, c'est-à-dire transformer α en la clef en connaissant la valeur de B , ou ce que fait Alice, c'est-à-dire transformer β en la clef en connaissant A . Mais Ève ne connaît la valeur ni de A ni de B puisque Alice et Bernard n'ont pas échangé ces nombres et les ont gardés secrets. Ève est dans l'impasse. Elle n'a plus qu'un espoir : en théorie, elle devrait pouvoir tirer A de α , puisque α était la conséquence de l'insertion de A dans une fonction, fonction qu'Ève connaît. Ou bien

	Alice	Bernard
<i>1^{re} étape</i>	Alice choisit un nombre, disons 3, et le garde secret.	Bernard choisit un nombre, disons 6, et le garde secret.
	Nous appelons son nombre A .	Nous appelons son nombre B
<i>2^e étape</i>	Alice applique 3 à la fonction à sens unique et obtient un résultat de $7^A \pmod{11}$: $7^3 \pmod{11} = 343 \pmod{11} = 2$	Bernard applique 6 à la fonction à sens unique et obtient un résultat de $7^B \pmod{11}$: $7^6 \pmod{11} = 117\,649 \pmod{11} = 4$
<i>3^e étape</i>	Alice appelle le résultat de ce calcul α , et envoie son résultat, 2, à Bernard	Bernard appelle le résultat de ce calcul β , et envoie son résultat, 4, à Alice.

L'échange Normalement ceci devrait être un point crucial, puisque Alice et Bernard échangent de l'information, ce qui donne à Ève la possibilité d'espionner et d'apprendre le contenu de cette communication. Toutefois, il se trouve qu'Ève peut écouter sans que cela affecte la sécurité finale du système. Alice et Bernard peuvent utiliser la même ligne téléphonique qu'ils avaient employée pour fixer les valeurs de Y et de P , et Ève peut intercepter les deux nombres échangés, 2 et 4. Ces nombres ne sont pas la clef et peu importe qu'Ève les connaisse.

<i>4^e étape</i>	Alice prend le résultat de Bernard et calcule le résultat de $\beta^A \pmod{11}$:	Bernard prend le résultat d'Alice et calcule le résultat de $\alpha^B \pmod{11}$:
	$4^3 \pmod{11} = 64 \pmod{11}$ $=9$	$2^6 \pmod{11} = 64 \pmod{11}$ $=9$

La clef Miraculeusement, Alice et Bernard obtiennent à la fin le même nombre, 9. C'est la clef !

Tableau 26 La fonction à sens unique est $Y^x \pmod{P}$. Alice et Bernard ont attribué des valeurs à Y et P , et se sont entendus sur une fonction à sens unique $7^x \pmod{11}$.

elle pourrait tirer B de β , puisque β était la conséquence de l'insertion de B dans une fonction, que là encore Ève connaît. Malheureusement pour Ève, la fonction est à sens unique, et s'il est facile pour Alice de transformer A en α , et pour Bernard de transformer B en β , il est bien difficile pour Ève d'inverser le procédé, surtout si les nombres sont très grands.

Bernard et Alice ont juste échangé l'information nécessaire pour établir une clef, et cette information était insuffisante pour qu'Ève trouve cette clef. Par analogie avec le schéma d'Hellman, imaginons un chiffrement qui, d'une manière ou d'une autre, utilise une couleur comme clef. D'abord, assurons-nous que tout le monde, Alice, Bernard et Ève dispose d'un pot de trois litres contenant un litre de peinture jaune. Si Alice et Bernard veulent s'entendre sur une clef secrète, chacun d'eux ajoute un litre de sa propre couleur dans son pot. Alice peut ajouter

une teinte particulière de pourpre, alors que Bernard ajoutera du cramoisi. Chacun envoie son pot à l'autre. Alice prend le mélange de Bernard et ajoute un litre de sa couleur secrète. Bernard prend le mélange d'Alice et ajoute un litre de sa couleur secrète. Les deux pots sont maintenant de la même couleur, puisqu'ils contiennent chacun un litre de jaune, un litre de pourpre et un litre de cramoisi. C'est cette couleur précisément des deux pots où les mélanges ont été opérés qui constituera la clef. Alice ne sait pas quelle couleur Bernard a ajoutée et Bernard ne sait pas quelle couleur Alice a ajoutée, mais ils ont le même contenu tous les deux à la fin. Pendant ce temps, Ève est furieuse. Même si elle a intercepté les pots intermédiaires, elle ne peut en tirer la couleur finale des pots, qui est la clef. Elle aura pu voir la couleur du pot contenant du jaune mélangé à la couleur secrète de Bernard, lorsqu'il était acheminé vers Alice, et elle aura pu voir la couleur du pot contenant du jaune mélangé à la couleur secrète d'Alice lorsqu'il était acheminé vers Bernard, mais pour trouver la clef elle a vraiment besoin de connaître les couleurs secrètes originales de Bernard et d'Alice. Évidemment, elle ne peut déduire ces couleurs secrètes simplement en regardant les pots. Même si elle prélève un échantillon sur l'un des mélanges de peinture, elle ne pourra en séparer les couleurs pour retrouver la couleur secrète, car le mélange des peintures est une fonction à sens unique.

Hellman eut cette illumination alors qu'il travaillait chez lui durant la nuit, et lorsqu'il eut terminé ses calculs, il était trop tard pour appeler Diffie et Merkle. Il dut attendre le lendemain matin pour faire part de sa découverte aux deux seules personnes au monde qui avaient cru qu'une solution au problème de la distribution des clefs était possible. « C'est à moi que la muse a parlé, dit Hellman, mais nous avons posé les fondations ensemble. » Diffie reconnut immédiatement le pouvoir de cette avancée : « Marty expliqua son système d'échange de clef dans toute son agaçante simplicité. En l'écoutant, je sentis que cette notion effleurait mon esprit depuis un certain temps, mais n'avait jamais tout à fait pris corps. »

Le schéma d'échange de clef de Diffie-Hellman-Merkle permet à Alice et Bernard d'établir un secret dans une conversation publique. C'est l'une des découvertes les plus contraires à l'intuition jamais faites dans l'histoire de la science, et elle obligea le monde de la cryptographie à réviser les règles du chiffrement. Diffie, Hellman et Merkle exposèrent leur découverte en juin 1976 lors de la Conférence nationale

d'informatique, et stupéfièrent l'auditoire, composé d'experts en cryptologie. L'année suivante, ils prirent un brevet. Depuis Alice et Bernard n'ont plus à se rencontrer pour échanger une clef. Alice appelle simplement Bernard au téléphone, échange avec lui un couple de nombres ; ils établissent leur clef secrète et peuvent alors chiffrer leur message.

Certes l'échange de clef Diffie-Hellman-Merkle représentait un gigantesque bond en avant, mais le système n'était pas parfait ; il présentait un inconvénient inhérent. Imaginons qu'Alice habite Hawaï, et qu'elle veuille envoyer un *e-mail* à Bernard à Istanbul. Bernard dort probablement à ce moment-là, mais Alice peut envoyer son *e-mail* n'importe quand, il attendra dans l'ordinateur jusqu'à ce que Bernard se réveille. Pourtant, si Alice veut crypter son message, elle a besoin de fixer la clef avec Bernard, et pour échanger leurs nombres, il serait préférable qu'Alice et Bernard soient en ligne en même temps. En fait, Alice doit attendre le réveil de Bernard. Ou bien, elle peut lui transmettre la partie de l'échange de clef qui est la sienne et attendre douze heures la réponse de Bernard pour que la clef soit fixée et qu'Alice puisse, si elle ne dort pas à son tour, chiffrer et envoyer son message. L'échange de clef de Hellman annihile l'instantanéité de *l'e-mail*.

Hellman avait renversé un des piliers de la cryptographie et prouvé qu'Alice et Bernard n'avaient pas besoin de se rencontrer pour convenir d'une clef secrète. Ensuite, quelqu'un devrait simplement arriver avec un schéma plus efficace pour que le problème de la distribution des clefs soit tout à fait surmonté.

Naissance de la cryptographie à clef publique

Mary Fisher n'a pas oublié la première fois où Whitfield Diffie l'a invitée à sortir avec lui : « Je savais qu'il était passionné par la recherche spatiale, aussi j'ai proposé que nous allions assister à un lancement. Whit me dit qu'il partait justement ce soir-là pour voir décoller le Skylab, nous avons donc roulé toute la nuit et sommes arrivés sur place à 3 heures du matin. L'oiseau était sur la piste d'envol, comme on disait alors. Whit avait un coupe-file de journaliste, mais pas moi. Lorsqu'on me demanda mon accréditation et qui j'étais, Whit répondit : "Ma femme." C'était le 16 novembre 1973. » Ils se marièrent effectivement par la suite, et, les premières années, Mary soutint son mari dans ses méditations cryptographiques. Diffie était toujours payé sur contrat de recherche, ce qui ne procurait qu'un maigre salaire. Mary, pourtant archéologue de formation, prit un emploi chez British Petroleum pour joindre les deux bouts.

Pendant que Martin Hellman élaborait sa méthode d'échange des clefs, Whitfield Diffie travaillait sur une approche tout à fait différente du problème. Il traversait souvent des périodes de réflexions stériles et, un jour de 1975, il dit à Mary, qu'il n'était qu'un scientifique raté qui n'arriverait jamais à rien. Il lui conseilla même de chercher quelqu'un d'autre. Mary lui répondit qu'elle avait une foi totale en ses capacités, et deux semaines plus tard, Diffie avait une idée brillante.

Il se rappelle encore comment elle lui vint subitement, pour ensuite presque s'effacer : « Je suis descendu au rez-de-chaussée pour prendre un Coca, et j'ai presque oublié mon idée. Je me souvenais que j'avais pensé à quelque chose d'intéressant, mais je ne pouvais me rappeler quoi. Soudain, cela me revint et je ressentis une véritable décharge d'adrénaline tant j'étais excité. Pour la première fois, j'étais convaincu d'avoir découvert quelque chose de vraiment valable en matière de cryptographie. Tout ce que j'avais fait auparavant me semblait n'être que du bricolage. » On était au milieu de l'après-midi et Mary n'était pas rentrée. « Whit attendait à la porte, se souvient-elle. Il m'annonça qu'il avait quelque chose à me dire et son expression était bizarre. J'entrai et il dit : "Assieds-toi, s'il te plaît, je veux te parler. Je crois que j'ai fait une grande découverte. Je sais que je suis la première personne à avoir fait

cela.” Pour moi, le monde s’arrêta de tourner à cet instant. J’avais l’impression de jouer dans un film à Hollywood. »

Diffie avait concocté un nouveau type de chiffre, qui incorporait ce qu’on appelle une *clef asymétrique*. Jusqu’ici, toutes les techniques de chiffrements décrits dans ce livre ont été *symétriques*, ce qui signifie que le procédé de déchiffrement est simplement l’inverse du chiffrement. La machine Enigma utilise une clef définissant un certain ajustement pour le chiffrement du message, et le destinataire utilise une machine identique avec le même ajustement pour le déchiffrer. De même, le chiffrement DES utilise une clef pour opérer les seize tours de brouillage, et le déchiffrement DES utilise la même clef pour exécuter seize tours en sens inverse. Emetteur et récepteur utilisent la même clef pour crypter et décrypter, leur relation est symétrique. Dans un système à clef asymétrique, au contraire, comme le nom le suggère, la clef de chiffrement et la clef de déchiffrement ne sont pas les mêmes. Dans un chiffrement asymétrique, si Alice connaît la clef de chiffrement, elle peut crypter le message mais pas le décrypter. Pour le décrypter, elle a besoin de la clef de déchiffrement. Cette différence entre les deux clefs constitue la spécificité du chiffre asymétrique.

Il faut préciser que si, à ce moment, Diffie avait bien conçu le concept général d’un chiffre asymétrique, il n’avait pas un seul exemple concret à proposer. Le concept à lui seul était pourtant révolutionnaire. Si les cryptographes mettaient au point un véritable chiffre asymétrique opérationnel, les conséquences en seraient considérables pour Alice et Bernard. Alice pourrait créer sa propre paire de clefs : une clef de chiffrement et une clef de déchiffrement. Si nous tenons le chiffre asymétrique pour une forme de chiffrement numérique, alors la clef de chiffrement d’Alice est un nombre, et sa clef de déchiffrement un autre nombre. Alice garde secrète sa clef de déchiffrement qu’on appelle donc *clef privée*. Elle peut par ailleurs diffuser sa clef de chiffrement de façon à ce que tout le monde y ait accès, c’est pourquoi on l’appelle communément *clef publique*. Si Bernard veut envoyer un message à Alice, il consulte sa clef publique qui figurera sur une liste, comme sur un annuaire de téléphone. Bernard se sert de cette clef publique pour crypter son message, qu’il envoie à Alice. Celle-ci, pour le décrypter, utilise sa clef de déchiffrement privée. Si Charles, David ou Édouard veulent également envoyer un message à Alice, ils peuvent se procurer sa clef publique mais seule Alice détient la clef privée nécessaire pour déchiffrer les messages.

Le grand avantage de ce système est de supprimer la navette que demandait l'échange de clefs chez Diffie-Hellman-Merkle. Bernard n'a pas besoin d'attendre qu'Alice lui donne une information pour crypter, il n'a qu'à appliquer sa clef publique. Alice n'a pas à passer cette clef secrètement à Bernard : bien au contraire, elle peut maintenant afficher sa clef publique à l'intention de toute personne qui voudrait l'utiliser. Car si tout le monde connaît sa clef publique, personne, et donc pas Ève, ne peut décrypter les messages chiffrés grâce à cette clef, puisqu'il faut alors une autre clef. En fait, lorsque Bernard a chiffré un message avec la clef publique d'Alice, même lui ne peut pas le déchiffrer. Seule Alice, qui possède la clef privée, en a le pouvoir.

Cela est exactement le contraire du traditionnel chiffre symétrique, pour lequel Alice devait faire de grands trajets pour remettre la clef de déchiffrement à Bernard. Alice et Bernard devaient prendre d'innombrables précautions afin que cette clef, la même pour chiffrer et pour déchiffrer, ne tombe pas entre les mains d'Ève. Ce qui était à la base du problème de l'échange des clefs.

Revenons à notre analogie avec les cadenas. N'importe qui peut fermer un cadenas en appuyant dessus, mais seule la personne qui a la clef peut l'ouvrir. Le verrouillage (le chiffrement) est facile, tout le monde peut le faire, mais le déverrouillage (le déchiffrement) ne peut être effectué que par le possesseur de la clef. Savoir fermer le cadenas ne nous apprend pas comment l'ouvrir. Poussons la comparaison : imaginons qu'Alice dessine un cadenas et une clef. Elle garde pour elle la clef, mais fabrique des centaines d'exemplaires du cadenas qu'elle envoie à des bureaux de poste à travers le monde. Si Bernard veut lui envoyer un message, il le met dans une boîte, va au bureau de poste local et demande un cadenas d'Alice, puis cadenasse la boîte. Désormais, il ne peut plus l'ouvrir, mais lorsqu'Alice la recevra elle pourra l'ouvrir en se servant de sa clef unique. Le cadenas que l'on ferme en cliquant simplement dessus est parfaitement semblable à la clef de chiffrement publique, puisque tout le monde a accès au cadenas et peut sceller un message dans une boîte. La clef du cadenas joue le même rôle que la clef privée. Puisque seule Alice la détient, elle seule peut ouvrir le cadenas et prendre le message dans la boîte.

Le système semble simple lorsqu'on l'explique en termes de cadenas, mais il n'était pas évident de trouver une fonction mathématique qui fasse le même travail et qui puisse être incorporée dans un cryptosystème opérationnel. Pour transformer une idée géniale en une invention

applicable, il fallait trouver la fonction mathématique appropriée. Diffie envisagea un type particulier de fonction à sens unique, qui peut être inversée sous certaines conditions exceptionnelles. Dans le système asymétrique de Diffie, Bernard crypte le message en se servant de la clef publique, mais il ne peut le décrypter — c'est une fonction à sens unique. Toutefois Alice peut opérer le déchiffrement puisqu'elle a la clef privée, une information particulière qui lui permet d'inverser la fonction. Là encore les cadenas fournissent un bon exemple : cliquer le cadenas est une fonction à sens unique, car il est difficile en principe d'ouvrir le cadenas sans posséder quelque chose de particulier (la clef), cas où la fonction devient facile à inverser.

Diffie publia les grandes lignes de son idée au cours de l'été 1975, ce qui poussa d'autres scientifiques à se mettre à la recherche de la fonction requise pour le chiffre asymétrique. Au début, l'optimisme régna, mais à la fin de l'année personne n'avait trouvé. Plus les mois passaient, plus il semblait que cette fonction à sens unique particulière n'existait pas. L'idée de Diffie marchait-elle en théorie et pas en pratique ? L'équipe formée par Diffie, Hellman et Merkle avait pourtant révolutionné la cryptographie. Ils avaient persuadé le reste du monde qu'il y avait une solution au problème de l'échange des clefs, et avaient créé l'échange de clefs Diffie-Hellman-Merkle, un système imparfait mais applicable. Ils avaient aussi proposé le concept d'un chiffre asymétrique, un système parfait mais jusque-là inapplicable. Ils poursuivirent leurs recherches à l'université Stanford, cherchant toujours la fonction à sens unique qui rendrait utilisable le chiffre asymétrique. Ils ne réussirent pas à la trouver et c'est un autre trio de chercheurs qui y parvint, à cinq mille kilomètres de là, sur la côte Est des États-Unis.

« Premiers » suspects

« J'entrai dans le bureau de Ron Rivest, se souvient Leonard Adleman, et Ron avait en mains cet article. Il commença par dire : “Ces types de Stanford ont un de ces baratins.” Et je me rappelle avoir pensé : “C’est bon, Ron, mais je venais te parler d’autre chose.” Je n’étais pas du tout versé dans la cryptographie, et absolument pas intéressé par ce qu’il racontait. »

L'article qui excitait ainsi Ron Rivest était de Diffie et Hellman, et décrivait le concept du chiffre asymétrique. Rivest réussit à persuader Adleman que ce problème pouvait avoir des implications mathématiques intéressantes, et ils décidèrent de chercher ensemble la fameuse fonction à sens unique qui répondrait aux exigences d'un chiffre asymétrique. Adi Shamir se joignit à leur chasse. Tous trois étaient des chercheurs installés au huitième étage du Laboratoire d'informatique du MIT (*Massachusetts Institute of Technology*).

Rivest, Shamir et Adleman formaient une équipe parfaite. Rivest est un spécialiste en informatique doué d'une étonnante facilité à intégrer des idées nouvelles et à en faire des applications inattendues. Il se tenait en permanence au courant des dernières publications scientifiques qui lui inspirèrent quantité de tentatives bizarres et mirifiques pour trouver la fonction à sens unique après laquelle il courait. Cependant, chaque essai se révéla insatisfaisant d'une manière ou d'une autre. Shamir, autre scientifique de l'informatique, a un esprit brillant et pointu qui lui permet de pénétrer à travers l'enveloppe d'un problème et d'en viser le cœur. Lui aussi formula maintes idées concernant le chiffre asymétrique, mais lui aussi sans succès. Adleman, un mathématicien plein d'énergie, de rigueur et de patience, repérait généralement très vite les points faibles des idées de Shamir et Rivest, et les empêchait ainsi de perdre leur temps. Rivest et Shamir passèrent une année à élaborer des hypothèses qu'Adleman s'empressait de renverser. Le trio commençait à perdre espoir, ne comprenant pas que ce processus d'échecs répétés était un moment nécessaire de leur recherche qui les conduisait peu à peu d'un territoire mathématique stérile vers un terrain plus fertile. Au bout du compte, leurs efforts furent récompensés.

En avril 1977, Rivest, Shamir et Adleman passaient la fête de Pâques chez un étudiant, et ils avaient bien arrosé la soirée. Rivest, incapable de fermer l'œil, s'étendit avec un livre de mathématiques. Il ressassait la question qui le poursuivait depuis tant de semaines : pouvait-on générer un chiffre asymétrique ? Soudain, les brumes se dissipèrent autour de lui, et il eut une inspiration. Il passa la fin de la nuit à formaliser son idée, et à l'aube il avait rédigé tout un article. C'était Rivest qui avait fait la découverte, mais elle était issue de sa collaboration depuis un an avec Shamir et Adleman, et elle n'aurait pas pu se faire sans eux. Rivest mit la dernière main à l'article en y inscrivant les noms des auteurs par ordre alphabétique : Adleman, Rivest, Shamir.

Le lendemain matin, Rivest porta l'article à Adleman, qui lui appliqua ses procédés habituels pour le mettre en pièces, mais cette fois il n'y décela pas de faiblesse. Sa seule critique concerna la liste des auteurs : « J'ai demandé à Ron d'enlever mon nom de l'article, se rappelle Adleman. Je lui ai dit que c'était son invention, pas la mienne. Mais Ron refusa et nous nous disputâmes à ce propos. Nous sommes finalement convenus que je réfléchirais pendant la nuit, avant de décider ce que je voulais faire. Je revins le lendemain et suggérai à Ron de faire figurer mon nom en troisième position. Je me rappelle avoir pensé que cet article serait le moins intéressant que j'aurais jamais signé. » Adleman ne pouvait pas se tromper davantage. Le système RSA — acronyme de Rivest, Shamir, Adleman — allait devenir le chiffre le plus influent de la cryptographie moderne.



Fig. 65 Ronald Rivest, Adi Shamir et Leonard Adleman.

Avant d'entrer plus avant dans l'idée de Rivest, rappelons brièvement ce que les scientifiques cherchaient pour construire un chiffre

asymétrique :

(1) Alice doit créer une clef publique, qu'elle diffusera afin que Bernard (ou n'importe qui d'autre) puisse l'utiliser pour crypter les messages qu'il lui adressera. La clef publique étant une fonction à sens unique, il est virtuellement impossible pour qui que ce soit de l'inverser et de décrypter les messages reçus par Alice.

(2) Cependant, Alice a besoin de décrypter les messages qu'on lui envoie. Elle doit donc avoir une clef privée, quelque moyen spécifique qui lui permette d'inverser l'effet de la clef publique. Donc Alice (et Alice seule) est capable de décrypter les messages à elle adressés.

Au cœur du chiffre asymétrique de Rivest se trouve une fonction à sens unique basée sur le type des fonctions modulo décrites plus haut. La fonction à sens unique de Rivest peut être utilisée pour crypter le message. On introduit dans la fonction ce message qui, en fait, est un nombre, et le résultat est le texte chiffré, un autre nombre. Je ne décrirai pas en détail la fonction de Rivest (voir Annexe J), mais j'expliquerai un des aspects qui lui sont propres, appelé simplement N parce que c'est ce N qui rend la fonction réversible sous certaines conditions, et donc idéale pour être appliquée à un chiffre asymétrique.

N est important parce qu'il est le composant variable de la fonction à sens unique, ce qui entraîne que chaque personne peut choisir pour N une valeur différente, et personnaliser la fonction. Pour choisir sa valeur personnelle de N , Alice prend deux nombres premiers, p et q et les multiplie l'un par l'autre. Un nombre premier n'a pas de diviseur, hors lui-même et 1. Par exemple 7 est un nombre premier parce qu'aucun chiffre ne le divise sans qu'il y ait un reste. De même 13 est un nombre premier parce que seuls 1 et 13 le divisent sans laisser de reste. En revanche, 8 n'est pas un nombre premier, puisqu'on peut le diviser par 2 et par 4.

Alice pourrait ainsi choisir comme nombres premiers $p = 17\ 159$ et $q = 10\ 247$. Multiplier ces nombres l'un par l'autre donne :

$$N = 17\ 159 \times 10\ 247 = 175\ 828\ 273.$$

Le choix d'Alice pour N devient sa clef publique, elle peut l'imprimer sur sa carte de visite, la mettre sur Internet ou la publier dans un annuaire de clefs publiques avec toutes les autres valeurs de N appartenant à d'autres personnes. Si Bernard veut crypter un message pour Alice, il se

procure la valeur du N d'Alice (175 828 273) et l'insère dans la formule générale de la fonction à sens unique, elle aussi de notoriété publique. Bernard dispose maintenant d'une fonction à sens unique taillée sur mesure avec la clef d'Alice, qu'on peut appeler la fonction à sens unique d'Alice. Pour crypter un message pour Alice, il prend la fonction d'Alice, y insère le message, en note le résultat et l'envoie à Alice.

Jusque-là, le message crypté est en sécurité puisque personne ne peut le déchiffrer. Le message a été chiffré par une fonction à sens unique ; inverser cette fonction et décrypter le message sont, par définition, virtuellement impossibles. Pourtant, une question demeure : comment Alice peut-elle décrypter le message ? Pour lire les messages qu'on lui adresse, Alice doit avoir un moyen d'inverser la fonction à sens unique. Un élément doit lui permettre de décrypter le message. Heureusement pour Alice, Rivest a élaboré une fonction à sens unique qui peut être inversée par quelqu'un connaissant la valeur de p et de q , les deux nombres premiers qui ont été multipliés pour donner N . Bien qu'Alice ait dit à tout le monde que sa valeur pour N était 175 828 273, elle n'a pas révélé les valeurs de p et de q ; elle seule dispose donc de cette information nécessaire pour décrypter les messages.

Nous pouvons voir en N la clef publique, une information disponible pour n'importe qui, une information nécessaire pour crypter les messages destinés à Alice. Alors que p et q sont la clef privée, utilisable par Alice seulement, l'information indispensable pour décrypter ces messages.

Les modalités précises de l'utilisation de p et de q pour inverser la fonction à sens unique sont décrites dans l'Annexe J. Pourtant, il y a une question qui se pose immédiatement. Si tout le monde connaît N , la clef publique, alors n'est-il pas facile d'en déduire p et q , la clef privée, et de lire les messages d'Alice ? Après tout, N a été créé en partant de p et de q . En fait il se trouve que si N est assez grand, il est pratiquement impossible d'en déduire p et q , et c'est peut-être l'aspect le plus intéressant et le plus élégant du chiffre asymétrique RSA.

Alice a créé N en choisissant p et q et en multipliant l'un par l'autre. Le point fondamental est que cette action est en elle-même une fonction à sens unique. Pour démontrer l'irréversibilité de la multiplication de nombres premiers, prenons deux nombres premiers 9 419 et 1 933, et multiplions-les. Une machine à calculer fournit la réponse en quelques secondes : 18 206 927. Si, au contraire, on nous donne 18 206 927 en nous demandant de trouver les facteurs premiers (les deux nombres qui, multipliés l'un par l'autre, ont donné 18 206 927), cela prendra beaucoup

plus de temps. Si vous en doutez, réfléchissez à ceci : cela m'a pris dix secondes pour générer le nombre 1 709 023, mais il vous faudra, avec votre machine à calculer, presque tout un après-midi pour en sortir les facteurs premiers. Ce cryptosystème, le RSA, est une forme de la *cryptographie à clef publique*. Pour vérifier sa sécurité, mettons-nous à la place d'Ève, et essayons de saisir un message d'Alice à Bernard. Pour crypter son message, Alice consulte la clef publique de Bernard. Pour constituer sa clef publique, Bernard a choisi ses propres nombres premiers, p_B et q_B et les a multipliés l'un par l'autre pour obtenir N_B . Il a gardé secret p_B et q_B , qui forment sa clef privée, mais a rendu publique N_B qui est 408 508 091. Alice insère donc la clef publique de Bernard dans la fonction générale à sens unique de chiffrement, et crypte son message. Lorsque le message lui parvient, Bernard peut inverser la fonction et le décrypter, en utilisant les valeurs de p_B et q_B qui constituent sa clef privée. Entre-temps, Ève a intercepté le message. Sa seule chance de le décrypter est d'inverser la fonction à sens unique, ce qu'elle ne peut faire sans connaître p_B et q_B . Bernard a tenu secrets p_B et q_B mais Ève, comme tout le monde, sait que N_B est 408 508 091. Ève tente donc de déduire les valeurs de p_B et q_B en sortant les nombres qui, multipliés l'un par l'autre, peuvent donner 408 508 091, procédé appelé *factorisation*.

Combien de temps exactement faudra-t-il à Ève pour trouver les facteurs diviseurs de 408 508 091 ? Il y a plusieurs recettes pour essayer de factoriser N_B . Certaines sont plus rapides que d'autres, mais toutes exigent de vérifier si chaque nombre premier peut ou non diviser N_B sans laisser de reste. Par exemple, 3 est un nombre premier mais n'est pas un diviseur de 408 508 901 puisque 3 ne divise pas parfaitement 408 508 901. Ève passe donc au nombre premier suivant, le 5. Le 5 ne convient pas non plus, Ève passe au suivant, et ainsi de suite. Enfin elle arrive à 18 313, le 2 000^e nombre premier, qui est un facteur de 408 508 091. Ayant trouvé l'un des facteurs, il devient facile d'avoir l'autre, qui se révèle être 22 307. Avec une machine à calculer pouvant tester quatre nombres premiers à la minute, Ève aurait mis 500 minutes, soit plus de huit heures, pour identifier p_B et q_B . Autrement dit, Ève trouverait la clef secrète de Bernard et pourrait ainsi déchiffrer le message en moins d'un jour.

mathématiques interdisent tout raccourci. S'ils ont raison, le RSA semble sûr pour l'avenir immédiat.

Le grand avantage de la cryptographie à clef publique RSA est qu'elle en finit avec tous les problèmes associés aux chiffres traditionnels et à l'échange de clefs. Alice n'a plus à se soucier du transport de la clef pour Bernard, ni à s'inquiéter d'une interception d'Ève. En fait, peu importe à Alice que quelqu'un d'autre voie la clef publique — plus on est de fous, plus on rit — puisque cette clef ne sert qu'au chiffrement et non au déchiffrement, et qu'Alice peut la garder toujours sur elle.

RSA fut présenté pour la première fois en août 1977 dans un article signé par Martin Gardner et intitulé *A New Kind of Cipher that Would Take Millions of Years to Break*, dans sa rubrique de jeux mathématiques du *Scientific American*. Après avoir expliqué comment fonctionne la cryptographie à clef publique, Gardner proposait un concours à ses lecteurs. Il publiait un texte chiffré et donnait la clef publique utilisée pour son chiffrement :

$N =$ 114 381 625 757 888 867 669 235 779 976 146 612
010 218 296 721 242 362 562 561 842 935 706 935
245 733 897 830 597 123 563 958 705 058 989 075
147 599 290 026 879 543 541.

Le jeu consistait à factoriser N en p et q , et à utiliser ensuite ces nombres pour déchiffrer le message. Le prix était de cent dollars. Gardner n'avait pas la place pour expliquer en détail le RSA, il demandait donc aux lecteurs d'écrire au Laboratoire du MIT qui leur enverrait une note technique. Rivest, Shamir et Adleman furent étonnés de recevoir mille demandes. Ils n'y répondirent d'ailleurs pas immédiatement, craignant que la diffusion de leur idée ne compromette leurs chances d'obtenir un brevet. Lorsque cela fut fait, le trio organisa une réunion pour fêter l'événement. Professeurs et étudiants eurent droit à des pizzas et à de la bière, et furent invités aussi à mettre la note technique sous enveloppe pour les lecteurs du *Scientific American*.

Quant au concours de Gardner, il a fallu dix-sept ans pour que le chiffre soit brisé. En avril 1994, une équipe de six cents volontaires révéla les facteurs de N .

q = 3 490 529 510 847 650 949 147 849 619 903 898
133 417 764 638 493 387 843 990 820 577.

p = 32 769 132 993 266 709 549 961 988 190 834 461
413 177 642 967 992 942 539 798 288 533.

En utilisant ces valeurs comme clef privée, ils furent capables de déchiffrer le message. Celui-ci était une série de nombres, qui convertis en lettre donnèrent : *The magic words are squeamish ossifrage*. La factorisation avait été confiée à des volontaires appartenant à des pays aussi éloignés que l'Australie, l'Angleterre, les États-Unis et le Venezuela. Ils consacrèrent leurs loisirs à travailler sur des ordinateurs, chacun étant chargé d'une fraction du problème. Même en tenant compte de l'organisation considérable nécessitée par ces calculs en parallèle, certains lecteurs seront surpris que le système RSA ait été brisé en un temps si court, mais il faut noter que le concours portait sur une valeur de N relativement petite, de l'ordre de 10^{129} . Aujourd'hui, les utilisateurs de RSA prendraient une valeur beaucoup plus élevée pour protéger une information importante. Il est maintenant courant de crypter un message avec une valeur de N telle que tous les ordinateurs de la planète auraient besoin d'un temps plus long que l'âge de l'univers pour briser le chiffre.

Un autre historique de la cryptographie à clef publique

Au cours des vingt dernières années, Diffie, Hellman et Merkle sont devenus pour le monde entier les cryptologues qui ont inventé le concept de la cryptographie à clef publique, tandis que Rivest, Shamir et Adleman étaient crédités de la mise au point du système RSA, la meilleure application de cryptographie à clef publique. Pourtant, une révélation récente oblige à réécrire les livres d'histoire. Selon le gouvernement anglais, la cryptographie à clef publique aurait été inventée au *Government Communications Headquarters* (GCHQ) de Cheltenham, l'établissement top secret fondé sur les ruines de Bletchley Park après la Seconde Guerre mondiale. C'est une histoire d'une étonnante simplicité, avec des héros anonymes et une confidentialité imposée par l'État pendant des décennies.

L'histoire commence à la fin des années 60, lorsque l'armée anglaise commença à s'intéresser au problème de l'échange de clefs. Les états-majors prévoyaient que, avec la miniaturisation des radios et la réduction de leurs coûts, chaque soldat, dans les années 70, serait en contact radio constant avec son officier. Les avantages de cette communication universelle seraient considérables, mais les transmissions devraient être cryptées et le problème de l'échange de clefs serait insoluble. A cette époque, la seule forme de cryptographie était symétrique, une clef personnelle devrait donc être acheminée vers chaque membre du réseau de communication. Toute expansion de ce réseau serait limitée par le poids de l'échange de clefs. Début 1969, l'armée chargea James Ellis, l'un des cryptographes officiels anglais les plus en vue, de traiter le problème de l'échange de clefs.

Ellis était un personnage curieux, un peu excentrique. Il se vantait d'avoir parcouru la moitié du monde avant même d'être né, ayant été conçu en Angleterre, mais né en Australie. Encore bébé, il revint en Angleterre et grandit à Londres, dans le quartier de l'East End. À l'école, il s'intéressa surtout à la science, et alla étudier la physique à l'*Imperial College*, avant de rejoindre le Centre de recherches postales de Dollis Hill, où Tommy Flowers avait construit Colossus, le premier ordinateur destiné à briser les codes. Le département cryptographique de Dollis Hill

fut bientôt absorbé par le GCHQ et, le 1^{er} avril 1965, Ellis partit à Cheltenham pour intégrer le groupe de sécurité des communications électroniques (CESG) nouvellement créé. Impliqué dans des recherches touchant à la sécurité de l'État, il fut tenu par serment de garder le secret tout au long de sa carrière. Sa femme et sa famille savaient qu'il travaillait au GCHQ, mais elles n'étaient pas au courant de ses découvertes, et ne se doutaient même pas qu'il était l'un des plus remarquables décrypteurs du pays.

En dépit de ses qualités de décrypteur, Ellis ne fut jamais à la tête d'un important groupe de recherches au GCHQ. Il était brillant, mais imprévisible, introverti et peu adapté au travail en équipe. Son collègue Richard Walton se souvient : « C'était un travailleur plutôt bizarre, et il n'était pas vraiment intégré aux activités quotidiennes du GCHQ. Mais pour arriver avec de nouvelles idées, il était extraordinaire. Vous deviez parfois faire le tri parmi un tas de détrit, mais il innovait et s'attaquait toujours à ce qui était orthodoxe. Nous aurions été bien ennuyés si tout le monde au GCHQ avait été comme lui, mais nous pouvions supporter une proportion plus importante de ce type de personnage que n'importe quel autre organisme. Nous nous en sortions avec un certain nombre de types comme lui. »

Une des grandes qualités d'Ellis était sa soif de connaissances. Il lisait tous les journaux scientifiques sur lesquels il pouvait mettre la main, et ne jetait jamais rien. Pour des raisons de sécurité, les employés du GCHQ devaient enlever tous les papiers de leur bureau chaque soir et les placer dans des placards verrouillés, ce qui veut dire que les placards d'Ellis étaient pleins des publications les plus obscures qu'on puisse trouver. Il y gagna une réputation de gourou en cryptologie, et lorsque d'autres chercheurs se trouvaient face à un problème insoluble, ils frappaient à sa porte dans l'espoir que son originalité et ses vastes connaissances leur fourniraient une solution. C'est sans doute à cause de cette réputation qu'on lui demanda de se pencher sur le problème de l'échange des clefs.

Le coût de l'échange des clefs était déjà énorme, et constituait un facteur limitatif à toute expansion du chiffrement. Une simple réduction de 10 % sur le coût de la distribution des clefs entraînerait une baisse non négligeable pour le budget de la sécurité militaire. Pourtant, Ellis, plutôt que de bricoler des aménagements dans ce sens, préféra chercher tout de suite une solution plus radicale. « Il approchait toujours un problème en demandant : "Est-ce là réellement ce que nous voulons faire ?" dit

Walton. L'une des premières choses qu'il contesta fut la nécessité de partager des données secrètes — c'est-à-dire la clef. Aucun théorème ne dit que vous devez avoir un secret en commun. C'était donc quelque chose de contestable. »

Ellis commença par fouiller dans son trésor d'articles scientifiques. Plusieurs années plus tard, il se rappelait le moment où il découvrit que l'échange des clefs n'était pas un élément inévitable de la cryptographie.



Fig. 66 James Ellis.

L'événement qui me fit changer d'avis fut un rapport fait pendant la guerre pour Bell Téléphone par un auteur inconnu et qui décrivait une ingénieuse idée pour assurer la sécurité des communications téléphoniques. Il proposait que le récepteur couvre la voix de son correspondant par du bruit sur la ligne. Il pouvait ensuite supprimer ce bruit puisqu'il en était l'auteur et savait donc ce qui l'avait causé. Les désagréments de ce système empêchèrent son application, mais il présentait des caractéristiques intéressantes. La différence avec le chiffrement conventionnel est que, dans ce cas, le récepteur prend une part active dans le processus de chiffrement. L'idée était donc née.

« Bruit » est le terme appliqué à n'importe quel signal qui perturbe une communication. Il est habituellement engendré par des phénomènes naturels, et son trait le plus agaçant est d'intervenir absolument au hasard, ce qui veut dire que supprimer un bruit sur un message est très délicat. Si un système radio est bien conçu, le niveau de bruit est faible et le message est clairement audible, mais si le niveau de bruit est élevé et couvre le message, il n'y a pas moyen de le récupérer. Ellis suggéra que la destinataire — Alice — crée exprès du bruit, dont elle règle l'intensité avant de l'ajouter sur la ligne qui la relie à Bernard. Bernard peut alors envoyer son message à Alice et si Ève écoute la communication sur la ligne elle ne pourra pas comprendre le message couvert par le bruit. Ève sera incapable de séparer le bruit du message. La seule personne qui peut le faire est Alice, car elle connaît l'exacte nature du bruit, l'ayant elle-même causé. Ellis comprit que la sécurité était ainsi assurée sans échange d'aucune clef. La clef était le bruit, et seule Alice la connaissait.

Dans une note, Ellis précisait le cheminement de sa réflexion : « La question suivante était évidente. Pouvait-on faire la même chose avec un chiffrement ordinaire ? Pouvons-nous établir un message crypté sûr, lisible par son destinataire désigné sans échange préalable d'une clef ? Cette question me poursuivait dans mon lit une nuit, et la preuve d'une possibilité théorique m'apparut en quelques minutes. Nous avons un théorème d'existence. L'impensable était en fait possible. » (Un théorème d'existence montre qu'un certain concept est possible, mais il ne se soucie pas des particularités de ce concept.) Autrement dit, jusque-là, chercher une solution pour l'échange de clef illustre tout à fait

l'image de l'aiguille dans la botte de foin, avec en plus la possibilité que l'aiguille ne soit même pas dans le foin. Grâce au théorème d'existence, Ellis savait maintenant que l'aiguille était quelque part.

L'idée d'Ellis était très proche de celle de Diffie, Hellman et Merkle, mais il avait quelques années d'avance sur eux. Personne n'entendit parler des recherches d'Ellis puisqu'il était tenu au secret. Vers la fin 1969, il semble qu'Ellis se soit trouvé dans la même impasse que le trio de Stanford en 1975. Il était convaincu que la cryptographie à clef publique (ou chiffrement non secret, comme il l'appelait) était possible et il avait développé le concept de clefs publiques et clefs privées séparées. Il savait aussi qu'il devait trouver une fonction à sens unique particulière, qui puisse être inversée si le receveur possède une certaine indication. Malheureusement, Ellis n'était pas un mathématicien. Il essaya quelques fonctions mathématiques, mais s'aperçut vite qu'il ne progresserait pas plus loin tout seul.

Ellis révéla alors sa découverte à ses patrons. Leurs réactions sont encore classées confidentiel-défense, mais Richard Walton a accepté de me rapporter dans un entretien ce que furent les commentaires de l'époque. Assis avec son cartable entrouvert sur ses genoux, dissimulant des papiers derrière le rabat, il survola les documents.

Je ne peux vous montrer les papiers que j'ai ici, car ils portent encore de vilains mots comme TOP SECRET imprimés dessus. En gros, l'idée de James remonte jusqu'au grand patron, qui la confie, comme font les grands patrons, à des spécialistes pour qu'ils l'étudient. Ceux-ci établissent que ce que James avance est rigoureusement exact. En d'autres termes, ils ne peuvent balayer l'idée de ce type en la taxant de fantaisiste. D'un autre côté, ils ne voient pas comment mettre son idée en pratique. Ils sont à la fois impressionnés par l'ingéniosité de James et pas certains qu'on puisse en tirer quelque chose.

Pendant les trois années qui suivirent, les plus brillants cerveaux du GCHQ s'efforcèrent de trouver une fonction répondant aux besoins d'Ellis, mais n'y parvinrent pas. Puis, en septembre 1973, un nouveau mathématicien rejoignit l'équipe. Il s'agissait de Clifford Cocks, récemment diplômé de l'université de Cambridge où il s'était spécialisé

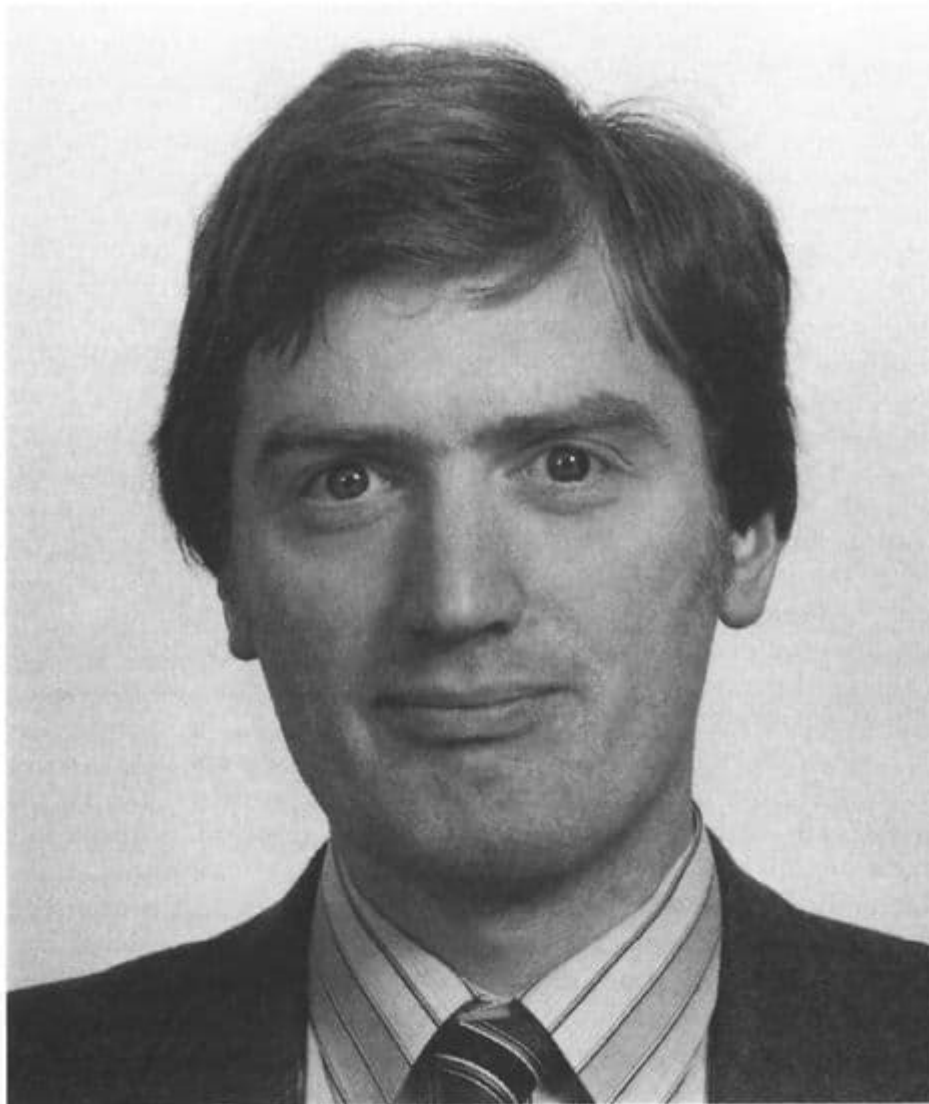
dans la théorie des nombres, une des formes les plus pures des mathématiques. Quand il arriva au GCHQ, il savait peu de chose sur le chiffrement et sur le monde discret de la communication militaire et diplomatique, aussi lui donna-t-on un mentor, Nick Patterson, pour le guider pendant ses premières semaines.

Après six semaines environ, Patterson parla à Cocks d'« une idée vraiment loufoque ». Il exposa la théorie d'Ellis d'un cryptosystème à clef publique, et ajouta que personne n'avait encore été capable de trouver une fonction mathématique adaptée à la demande. Patterson raconta cela à Cocks parce que c'était l'idée la plus excitante pour les cryptologues du lieu, et non parce qu'il attendait de lui qu'il essaie d'y répondre. Pourtant, Cocks se mit au travail le jour même : « Je n'avais rien à faire de particulier, alors je décidai de réfléchir à cette idée. Comme j'avais travaillé sur la théorie des nombres, j'étais familier des fonctions à sens unique, quelque chose que vous pouvez faire mais pas défaire. Les nombres premiers et la factorisation me semblèrent constituer un point de départ évident. » Cocks commençait à formuler ce qui serait plus tard connu comme le chiffre asymétrique RSA. Rivest, Shamir et Adleman découvrirent leur formule de chiffrement à clef publique en 1977, mais quatre ans auparavant le jeune diplômé de Cambridge avait suivi le même chemin. Cocks se souvient : « Du début à la fin, cela ne me prit pas plus d'une demi-heure. J'étais plutôt content de moi. J'ai pensé : "Oh ! c'est bien. On m'a posé un problème et je l'ai résolu." »

Cocks ne mesura pas tout à fait l'importance de sa découverte. Il ne savait pas que les meilleures têtes du GCHQ se confrontaient au problème depuis trois ans, et il n'avait pas du tout le sentiment d'avoir fait accomplir un pas décisif à la cryptographie. La naïveté de Cocks a dû participer à son succès car il put attaquer le problème avec confiance, au lieu d'être intimidé par lui. Cocks fit part de sa découverte à son mentor, Patterson, qui adressa un rapport à la direction. Cocks était novice et sans assurance, alors que Patterson connaissait la question et était plus armé pour répondre aux questions techniques qui ne manqueraient pas d'être soulevées.

Bientôt de parfaits inconnus commencèrent à venir voir Cocks, l'enfant prodige, et à le féliciter. L'un de ces inconnus était James Ellis, qui avait hâte de rencontrer l'homme qui avait fait de son rêve une réalité. Cocks ne saisissant toujours pas l'importance de ce qu'il avait

réalisé, ne prêta guère d'attention à cette rencontre, et aujourd'hui, vingt ans plus tard, il ne se souvient pas de la réaction d'Ellis.



[Fig. 67](#) Clifford Cocks.

Quand Cocks réalisa enfin ce qu'il avait fait, il pensa que sa découverte aurait déçu G.H. Hardy, l'un des grands mathématiciens anglais du début du siècle, qui, dans son ouvrage *The Mathematician's Apology* (1940), avait fièrement proclamé : « Les vraies mathématiques n'ont aucun effet sur la guerre. Personne n'a encore trouvé un objectif militaire qui serait dépendant de la théorie des nombres. » Par *vraies mathématiques*, il entendait mathématiques pures, comme la théorie des nombres qui était au centre du travail de Cocks. Hardy avait tort : les dédales de la théorie des nombres peuvent maintenant aider des généraux à établir secrètement leurs plans de bataille. En raison des implications militaires de son travail, Cocks, comme Ellis, ne put parler à personne en

dehors du GCHQ de ce qu'il avait fait. Travailler dans un organisme gouvernemental sous le sceau du secret lui interdisait d'informer ses parents ou ses anciens condisciples de Cambridge. La seule personne à laquelle il pouvait parler était Gill, sa femme, car elle travaillait elle aussi au GCHQ.

Si l'idée de Cocks constituait l'un des secrets potentiellement les plus importants du GCHQ, elle souffrait d'être en avance sur son temps. Cocks avait trouvé une fonction mathématique qui permettait la cryptographie à clef publique, mais il restait encore une difficulté pour appliquer le système. Le chiffrement par une clef publique nécessite un ordinateur beaucoup plus puissant qu'un chiffrement selon un chiffre symétrique comme DES. Au début des années 70, les ordinateurs étaient relativement primitifs et incapables de suivre le processus de chiffrement à clef publique dans un délai raisonnable. Aussi le GCHQ n'était-il pas en mesure d'exploiter la cryptographie à clef publique.

Au début de 1974, Cocks exposa son travail sur la cryptographie à clef publique à Malcom Williamson, qui avait récemment rallié le GCHQ en tant que cryptographe. Les deux hommes étaient de vieux amis. Ils s'étaient rencontrés au lycée de Manchester. Encore écoliers, en 1968, les deux garçons avaient représenté l'Angleterre aux olympiades de mathématiques en Union soviétique. Après avoir été ensemble à l'université de Cambridge, ils suivirent chacun leur route pendant deux ans, puis se virent de nouveau réunis au GCHQ. Depuis l'âge de onze ans, ils n'avaient cessé d'échanger des idées sur les mathématiques, mais la révélation par Cocks de la cryptographie à clef publique fut bien l'idée la plus bouleversante que Williamson eut jamais entendue. « Cliff m'expliqua son idée, rappelle Williamson, et je ne le crus pas vraiment. J'étais plein de doutes, car c'est très étrange de pouvoir faire cela. »



Fig. 68 Malcom Williamson.

Williamson essaya de prouver que Cocks avait fait une erreur et que la cryptographie à clef publique n'existait pas. Il vérifia les calculs, pour détecter une faute à la base. La cryptographie à clef publique semblait trop belle pour être vraie, et Williamson était tellement déterminé à trouver l'erreur qu'il rentra chez lui avec le problème. Les employés du GCHQ ne sont pas censés rapporter du travail à la maison, puisque tout ce qu'ils touchent est classé confidentiel et que leur domicile est un lieu vulnérable à l'espionnage. Mais le problème tournait dans la tête de Williamson, et il ne pouvait se retenir d'y penser. Au mépris des consignes, il rapporta donc ses papiers chez lui. Il passa cinq heures à chercher une faiblesse sans y parvenir : « Au lieu de cela, raconte-t-il, je trouvais une autre solution au problème de la distribution des clefs. » Williamson venait de trouver l'échange de clef de Diffie-Hellman-Merkle, à peu près en même temps que Martin Hellman. La première

réaction de Williamson est à l'image de sa tournure d'esprit cynique : « Ça a l'air formidable, pensai-je. Je me demande si je peux trouver une erreur là-dedans. Je crois que j'étais plutôt négatif, ce jour-là. »

En 1975, James Ellis, Clifford Cocks et Malcom Williamson avaient donc découvert tous les aspects fondamentaux de la cryptographie à clef publique, cependant tous se turent. Les trois Anglais durent voir leur découverte redécouverte par Diffie, Hellman, Merkle, Rivest, Shamir et Adleman, au cours des trois années suivantes. Curieusement, le GCHQ eut connaissance du RSA avant d'entendre parler de l'échange de clefs de Diffie-Hellman-Merkle, alors que, pour le monde extérieur, c'est cette formule d'échange de clefs qui apparut d'abord. La presse scientifique se fit l'écho des découvertes faites à Stanford et au MIT, et les chercheurs qui avaient pu publier leurs travaux dans les revues scientifiques devinrent célèbres dans la communauté des cryptologues. Un rapide regard sur Internet fait découvrir 15 pages de web seulement mentionnant Clifford Cocks et 1 382 pages concernant Whitfield Diffie. L'attitude de Cocks est admirablement réservée : « Vous ne travaillez pas dans ce domaine pour être célèbre. » Et Williamson est tout aussi calme : « Ma réaction fut : "Bon, c'est comme ça." La vie continuait. »



Fig. 69 Malcom Williamson (second à partir de la gauche) et Clifford Cocks (à l'extrême droite) arrivent aux olympiades de mathématiques de 1968.

Le seul regret de Williamson est que le GCHQ n'ait pas réussi à breveter la cryptographie à clef publique. Quand Cocks et Williamson avaient fait leurs premières découvertes, les chefs du GCHQ estimèrent que breveter était impossible pour deux raisons. La première était que pour demander un brevet, il fallait révéler tous les détails de leurs

travaux, ce qui était incompatible avec les règles du GCHQ. La seconde était que, dans les années 70, il n'était pas évident qu'on puisse breveter des algorithmes mathématiques. Williamson était prêt à publier et à s'opposer à la demande de brevet de Diffie-Hellman-Merkle, mais ses supérieurs ne le permirent pas. Ceux-ci ne prévoyaient pas la révolution informatique et le potentiel de la cryptographie à clef publique. Au début des années 80, les patrons de Williamson commencèrent à regretter leur décision, en voyant que le développement de l'informatisation et que l'Internet, encore embryonnaire, annonçaient que le RSA et l'échange de clef Diffie-Hellman-Merkle deviendraient des produits commerciaux promis à un immense succès. En 1996, la *RSA Data Security Inc.*, la compagnie qui gère les produits RSA, fut vendue 200 millions de dollars.

Bien que les travaux du GCHQ ne soient pas encore déclassifiés, un autre organisme était au courant des réalisations anglaises. Au début des années 80, l'*America's National Security Agency* connaissait les travaux de Cocks, Ellis et Williamson, et c'est probablement *via* la NSA que Whitfield Diffie entendit des allusions aux découvertes anglaises. En septembre 1982, Diffie décida d'aller voir si cette rumeur était fondée, et il partit avec sa femme pour Cheltenham, afin de s'entretenir en personne avec James Ellis. Ils se rencontrèrent dans un pub, et Mary fut frappée par le personnage étonnant qu'était Ellis :

Nous étions assis là, à bavarder, et soudain j'ai pris conscience qu'il était l'être le plus merveilleux que l'on puisse imaginer. L'étendue de ses connaissances mathématiques n'est pas un sujet dont je sois capable de témoigner, mais c'était un vrai seigneur, incroyablement modeste, une personne d'une grande générosité intellectuelle et très distinguée. Quand je dis distinguée, je ne veux pas dire démodée et poussiéreuse. Cet homme était un chevalier. C'était un homme bon, doté d'une vraie noblesse d'esprit.

Diffie et Ellis évoquèrent de nombreux sujets, depuis l'archéologie jusqu'aux rats dont la présence dans un tonneau améliore la qualité du cidre, mais à chaque fois que la conversation se rapprochait de la cryptographie, Ellis la faisait dériver. Au moment de partir, Diffie ne put résister plus longtemps à l'envie de poser à Ellis la question qui lui

brûlait les lèvres : « Dites-moi comment vous avez inventé la cryptographie à clef publique ? » Il y eut un long silence, puis Ellis murmura : « Eh bien, je ne sais pas dans quelle mesure je peux en parler. Disons simplement que vos amis et vous avez fait beaucoup plus que nous dans ce domaine. »

Bien que le GCHQ ait été le premier à découvrir la cryptographie à clef publique, cela n'enlève rien aux universitaires qui l'ont redécouverte. Ceux-ci ont été les premiers à comprendre les possibilités du chiffrement à clef publique, et ce sont eux qui ont mené à bien son application. De plus, il est possible que le GCHQ n'aurait jamais révélé ses travaux, bloquant ainsi un système de chiffrement qui allait permettre à la révolution informatique d'atteindre tout son développement potentiel. En fait, la découverte par les universitaires était tout à fait indépendante de la découverte du GCHQ, et du même niveau intellectuel. Le milieu universitaire est très loin du domaine de la recherche classée confidentiel-défense, et les universitaires n'ont pas accès aux outils et aux informations secrètes qui peuvent être tenus cachés dans le monde classifié. De l'autre côté, les chercheurs officiels, eux, ont accès à toute la littérature universitaire. On peut voir là une autre fonction à sens unique : l'information coule librement dans une direction, mais il est impossible d'envoyer de l'information en remontant le courant.

Au milieu des années 80, l'atmosphère changea au GCHQ, et la direction envisagea de rendre publics les travaux d'Ellis, de Cocks et de Williamson. Les mathématiques de la cryptographie à clef publique étaient désormais connues, et il n'y avait plus de raison pour garder le secret. Au contraire, les Anglais avaient avantage à révéler leur travail de pionniers. Comme le rappelle Richard Walton :

Nous flirtions avec l'idée de dire toute la vérité en 1984. Nous commencions à voir quels avantages retirerait le GCHQ d'être mieux connu. C'était l'époque où le marché de la sécurité officielle s'étendit au-delà des traditionnels domaines militaires et diplomatiques, et nous devions inspirer confiance à ceux qui n'avaient pas coutume de traiter avec nous. On était en pleine ère Thatcher, et nous essayions de contrer l'idée selon laquelle « l'État c'est mal, le privé c'est génial ». Nous

voulions donc publier un article, mais cette idée fut coulée par ce salaud de Peter Wright, qui écrivit Spycatcher. On avait chauffé notre direction générale pour obtenir son autorisation, lorsqu'il y eut tout ce foin autour de Spycatcher. Alors, l'ordre du jour fut « têtes basses, et vos chapeaux par-dessus ».

Peter Wright était un officier à la retraite des services de renseignements anglais, et la publication de son livre de mémoires, *Spycatcher*, fut source d'une grande gêne pour le gouvernement anglais. Il faudrait encore treize ans pour que le GCHQ soit enfin rendu public — vingt-huit ans après la découverte initiale d'Ellis. En 1997, Clifford Cocks mit la dernière main à un travail important (et non classifié) sur le RSA, qui pouvait intéresser un cercle plus large et dont la publication n'offrait aucun risque pour la sécurité. À la suite de quoi, il fut invité à présenter une communication à la conférence de l'Institut de mathématiques qui devait se tenir à Cirencester. La salle serait pleine de spécialistes de la cryptologie. Une poignée d'entre eux saurait que Cocks, qui allait commenter l'un des aspects du RSA, en était en fait l'inventeur méconnu. Il y avait un risque que quelqu'un pose une question embarrassante, du type : « Avez-vous inventé le RSA ? » Si une telle question survenait, selon la règle du GCHQ, Cocks devait nier son rôle dans l'établissement du RSA, ce qui l'obligeait à mentir sur un sujet absolument inoffensif. La situation était parfaitement ridicule et le GCHQ décida qu'il était temps de modifier sa politique. On permit donc à Cocks de commencer son intervention par un bref historique de la contribution du GCHQ dans la cryptographie à clef publique.

La conférence eut lieu le 18 décembre 1997. Après environ trois décennies de secret, Ellis, Cocks et Williamson recevaient la reconnaissance qu'ils méritaient. Malheureusement, James Ellis était mort un mois plus tôt, le 25 novembre 1997, à l'âge de soixante-treize ans. Ellis rejoignait ainsi la liste d'experts anglais du chiffrement dont les contributions n'avaient pu être saluées de leur vivant. La victoire de Charles Babbage sur le chiffre de Vigenère avait été tenue secrète parce que son travail avait une valeur incalculable pour les forces britanniques en Crimée. Au lieu de Babbage, c'est Friedrich Kasiski qui fut crédité de cette réussite. De même, Alan Turing fournit pendant la guerre une contribution inégalée, et cependant le secret d'État exigea que son travail sur Enigma ne soit pas divulgué.

En 1987, Ellis avait rédigé un document classé confidentiel qui rappelait sa contribution à la cryptographie à clef publique, et qui reflétait ses pensées sur le silence qui pèse sur les travaux des cryptologues. On y lit notamment :

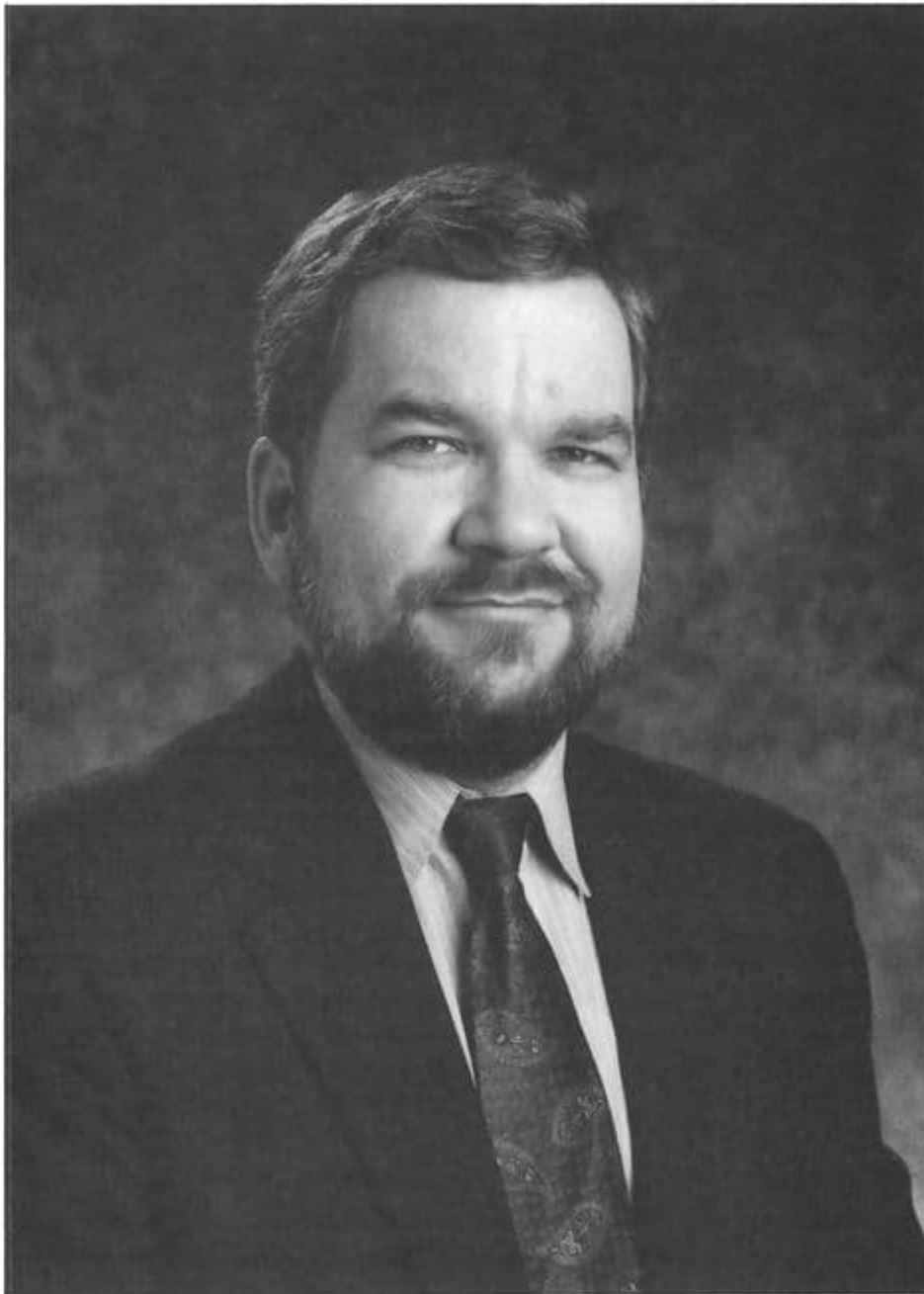
La cryptographie est une science peu ordinaire. La plupart des scientifiques cherchent à publier les premiers résultats de leurs travaux, parce que c'est à travers cette diffusion que ces travaux prennent toute leur valeur. Au contraire, la plus grande valeur en cryptographie est atteinte en dissimulant l'information à des adversaires potentiels. Aussi les cryptographes professionnels travaillent habituellement en cercle restreint pour se procurer mutuellement l'interaction nécessaire à la qualité des recherches, tout en restant protégé des concurrents. La révélation de ces secrets n'est généralement autorisée que dans l'intérêt de la vérité historique, et lorsqu'il est démontré qu'aucun bénéfice supplémentaire ne pourrait être tiré d'une prolongation de ce secret.

Pretty Good Privacy

Comme Whit Diffie l'avait prédit dès le début des années 70, nous sommes entrés maintenant dans l'âge de l'information — une ère post industrielle dans laquelle l'information est devenue le bien le plus précieux. L'échange informatisé fait désormais partie intégrante de notre société. Dix millions d'*e-mails* sont envoyés chaque jour et le courrier électronique est en passe de supplanter le courrier classique. L'Internet, qui n'en est encore qu'à ses débuts, a fourni une infrastructure nouvelle au marché, et le commerce électronique se répand. Les transferts de fonds électroniques entre banques véhiculent un flot financier constant, et l'on estime que, chaque jour, la moitié des matières premières mondiales sont traitées sur le réseau de la *Society for Worldwide Interbank Financial Telecommunication*. Les démocraties qui usent du référendum pratiqueront de plus en plus le vote électronique et les États se serviront d'Internet pour leur administration, par exemple en proposant des services comme les déclarations d'impôts électroniques.

Toutefois, la réussite de cet âge de l'information dépend de la capacité à protéger ces renseignements qui flottent autour du globe, et cette charge revient naturellement à la cryptographie. Le chiffrement sera le fournisseur de verrous et de clefs de cette nouvelle ère. Pendant deux mille ans, il n'a été vraiment indispensable que pour les gouvernants et les militaires, mais aujourd'hui il joue un rôle dans les affaires et demain le public s'en remettra à lui pour assurer la confidentialité de toutes les transmissions. Par chance, au moment où ces besoins se créent, on dispose de chiffrements efficaces. Le développement de la cryptographie à clef publique — et notamment le système RSA — a fourni aux cryptographes contemporains un net avantage dans leur perpétuel combat contre les cryptanalystes. Si la valeur de N est suffisamment grande, trouver p et q prend à Ève un temps considérable et le chiffre RSA se révèle en fait intouchable, mais surtout la cryptographie à clef publique n'est pas entravée par le problème de la distribution des clefs. Le RSA

garantit à nos plus précieuses informations des serrures presque infrangibles.



[Fig.70](#) Phil Zimmermann,.

Évidemment, toute technologie a son revers, la cryptographie comme les autres. Si le chiffre protège les échanges entre bons citoyens, il couvre également les messages des criminels et des terroristes. La police a souvent utilisé des écoutes pour rassembler des preuves dans des cas de crime organisé ou de terrorisme, mais elle n'aura plus cette possibilité si ces groupes utilisent des chiffres inattaquables. À l'aube du XXI^e siècle,

un dilemme fondamental se pose à la cryptographie : comment permettre au public et aux entreprises d'utiliser le chiffrement pour protéger la confidentialité de leurs tractations sans laisser en même temps les criminels user du chiffrement pour échapper aux recherches. Cette question est actuellement très débattue, et au centre de la discussion revient toujours l'histoire de Phil Zimmermann, un homme dont les tentatives pour répandre l'usage d'un chiffrement sûr ont semé la panique chez les experts américains de la sécurité et mis en cause l'efficacité de la *National Security Agency* (NSA), organisme au budget d'un milliard de dollars, provoquant même une enquête du FBI et celle d'un grand jury à son sujet.

Phil Zimmermann passa la moitié des années 70 à la Florida Atlantic University, où il étudia la physique et l'informatique. Une fois diplômé, il semblait destiné à une carrière sans à-coups dans l'industrie florissante de l'informatique, mais les événements politiques du début des années 80 bouleversèrent sa vie et, dès lors, il s'intéressa moins à la technologie des puces et davantage à la menace de guerre nucléaire. Son inquiétude venait à la fois de l'invasion soviétique en Afghanistan, de l'élection de Ronald Reagan à la présidence des États-Unis, de l'instabilité due à l'âge de Brejnev et aux tensions croissantes engendrées par la guerre froide. Il envisagea même de s'installer avec sa famille en Nouvelle-Zélande, pensant trouver là un des seuls lieux sur terre susceptible de rester habitable après un conflit nucléaire. Mais, à la veille de leur départ, lui et sa femme assistèrent à une conférence organisée dans le cadre de la campagne pour le gel des armements nucléaires. Plutôt que de s'enfuir, les Zimmermann décidèrent de rester et de mener le combat chez eux, en se portant au premier rang des activistes antinucléaires. Ils approchèrent les politiciens pour leur démontrer les dangers d'une politique de l'armement, et ils furent arrêtés dans le Nevada lors de manifestations, en même temps que Carl Sagan et quatre cents autres protestataires.

En 1988, Mikhaïl Gorbatchev initia la *perestroïka*, la *glasnost* et un relâchement de la tension Est-Ouest. Les angoisses de Zimmermann se dissipèrent un peu, mais il ne perdit pas son goût pour l'activisme politique, qu'il canalisa simplement dans une autre direction. Il concentra son attention sur la révolution informatique et la nécessité du chiffrement.

La cryptographie, écrit-il, avait toujours été une science obscure avec peu de retombées sur la vie quotidienne. Historiquement, elle avait toujours tenu un rôle particulier dans les communications militaires et diplomatiques. Mais à l'âge de l'information, la cryptographie a un rôle à jouer dans le pouvoir politique, en particulier dans les relations du pouvoir entre les gouvernants et la population. Elle a un rôle à jouer dans le droit à la confidentialité, la liberté d'expression, la liberté d'association, la liberté de la presse, la liberté qui protège de toute poursuite et arrestation injustifiées, la liberté qu'on vous laisse tranquille.

Ces vues peuvent sembler paranoïaques, mais selon Zimmermann, il y a, entre communication traditionnelle et communication électronique, une différence fondamentale qui entraîne des implications non négligeables pour la sécurité :

Autrefois, si le gouvernement voulait percer l'intimité de simples citoyens, il devait se donner du mal pour intercepter, déceler et lire une correspondance écrite, ou écouter et éventuellement enregistrer, des conversations téléphoniques. On peut comparer cela à attraper un poisson avec une ligne, un poisson à la fois. Heureusement pour la démocratie et la liberté, ce travail intensif d'espionnage n'est pas praticable à grande échelle. Aujourd'hui, le courrier électronique se substitue de plus en plus au courrier sur papier traditionnel, et bientôt ce sera peut-être la norme pour tout le monde, et non plus une nouveauté comme aujourd'hui. À l'inverse des lettres, les messages e-mail sont très simples à intercepter et à exploiter pour trouver d'utiles mots-clefs. Ceci peut être exécuté à grande échelle facilement, systématiquement, constamment et sans qu'on puisse le détecter. C'est comparable à la pêche au filet — et cela constitue une différence orwellienne quantitative et qualitative considérable pour la santé de la démocratie.

On peut illustrer cette différence entre courrier ordinaire ou électronique en imaginant qu'Alice veut envoyer des invitations pour son anniversaire et qu'Ève, qui n'a pas été invitée, veut savoir le lieu et la date de la réception. Si Alice utilise la méthode traditionnelle et poste ses lettres, il sera difficile pour Ève d'intercepter une invitation. Pour commencer, Ève ne sait pas où les invitations d'Alice ont été postées, puisque Alice peut le faire dans n'importe quelle boîte aux lettres de la ville. Son seul espoir d'intercepter une invitation est de se procurer l'adresse d'un ami d'Alice et d'infiltrer le bureau distributeur. Là, elle devra encore vérifier toutes les lettres manuellement. Si elle réussit à trouver une lettre d'Alice, elle l'ouvrira à la vapeur pour y chercher l'information qu'elle désire, et la remettra en état avant de lui laisser poursuivre sa route, afin de n'éveiller aucun soupçon.

La tâche d'Ève est considérablement plus facile si Alice envoie ses invitations par *e-mail*. Lorsque les messages sortent de l'ordinateur d'Alice, ils vont à un serveur local, entrée principale pour Internet ; si Ève est assez maligne, elle peut s'infiltrer dans ce serveur local sans bouger de chez elle. Les invitations porteront l'adresse *e-mail* d'Alice, et ce sera chose facile que d'installer un tamis électronique qui retiendra les *e-mails* portant l'adresse d'Alice. Une fois qu'une invitation a été trouvée, il n'y a pas d'enveloppe à ouvrir et donc aucun problème pour la lire. De plus, l'invitation peut continuer son chemin sans porter aucun signe de l'interception. Alice ignorera ce qui s'est passé. Toutefois, il existe un moyen d'empêcher Ève de lire les *e-mails* d'Alice : le chiffrement.

Plus de cent millions d'*e-mails* sont envoyés quotidiennement autour du monde, tous vulnérables à une interception. La technologie informatique a facilité la communication, mais elle offre aussi la possibilité de surveiller cette communication. Selon Zimmermann, les cryptographes ont le devoir de promouvoir l'usage du chiffrement pour protéger la vie privée de l'individu :

Un gouvernement futur pourra hériter d'une infrastructure technologique aménagée pour la surveillance, grâce à laquelle il suivra les gestes de ses opposants politiques, toute transaction financière, toute communication, tout e-mail, tout appel téléphonique. Tout peut être filtré, analysé, identifié automatiquement par la technique de reconnaissance de la voix, et enregistré. Il

est temps pour la cryptographie de sortir de l'ombre de l'espionnage et de l'armée, et de s'avancer en pleine lumière pour être adoptée par chacun d'entre nous.

En théorie, lorsque le RSA fut inventé en 1977, il offrait un antidote au scénario de *Big Brother* puisque les personnes privées pouvaient créer leurs propres clefs publiques et privées. Pourtant, en pratique, il y avait un problème majeur, car le processus du chiffrement RSA demandait un ordinateur d'une puissance bien supérieure à celle nécessitée par les formes des chiffrements symétriques, comme le DES. Dans les années 80, seuls l'État, l'armée et les grandes entreprises possédaient des ordinateurs suffisamment puissants pour effectuer le chiffrement RSA. La société fondée pour commercialiser le RSA, la *RSA Data Security Inc.*, développa ses produits uniquement à l'intention de ce marché.

Zimmermann, lui, estimait que tout le monde avait droit à la confidentialité offerte par le chiffrement RSA, et il appliqua son zèle politique à développer un produit qui permettrait aux masses d'y accéder. Il espérait tirer partie de son expérience en informatique pour créer un produit économique et efficace, n'exigeant que la capacité d'un ordinateur personnel courant. Il voulait aussi que sa version du RSA offre un abord particulièrement convivial, afin que l'utilisateur n'ait pas besoin d'être un expert en cryptographie pour l'appliquer. Il appela son projet *Pretty Good Privacy* ou PGP. Ce nom lui fut inspiré par *Ralph's Pretty Good Groceries* (« Les Joliment bonnes épiceries de Ralph »), entreprise qui finançait une des émissions préférées de Zimmermann, *Prairie Home Companion*, présentée par Garrison Keillor.

Travaillant chez lui à Boulder, Colorado, Zimmermann, petit à petit, fabriqua son logiciel de cryptement. Son objectif principal était d'accélérer le chiffrement RSA. Normalement, si Alice veut utiliser le RSA pour crypter un message destiné à Bernard, elle cherche sa clef publique et applique la fonction à sens unique RSA au message. Réciproquement, Bernard décrypte le texte chiffré en utilisant sa clef privée pour inverser la fonction à sens unique. Les deux processus demandent beaucoup de manipulations mathématiques ; chiffrement et déchiffrement peuvent, si le message est long, prendre plusieurs minutes sur un ordinateur personnel. Si Alice envoie cent messages par jour, elle ne peut pas passer plusieurs minutes à crypter chacun d'eux. Pour accélérer chiffrement et déchiffrement, Zimmermann employa un truc simple, qui utilisait le chiffrement asymétrique RSA en tandem avec le

bon vieux chiffrement symétrique. Le chiffrement symétrique traditionnel peut être aussi sûr que le chiffrement asymétrique et est beaucoup plus rapide à effectuer, mais il souffre du problème de l'envoi de clef. C'est là que le RSA vient à la rescousse, parce qu'il peut servir à crypter la clef symétrique.

Zimmermann conçut le scénario suivant. Si Alice veut envoyer un message crypté à Bernard, elle commence par le crypter avec un chiffre symétrique. Zimmermann suggérait de prendre un chiffre comme l'IDEA, qui ressemble au DES. Pour crypter avec l'IDEA, Alice doit choisir une clef et pour que Bernard décrypte le message, Alice, d'une façon ou d'une autre, doit passer la clef à Bernard. Alice résout ce problème en cherchant la clef publique de Bernard, qu'elle utilise pour crypter la clef IDEA. Alice finit donc par envoyer deux choses à Bernard : le message crypté avec le chiffre symétrique IDEA, et la clef IDEA cryptée avec le chiffre asymétrique RSA. À l'autre bout, Bernard utilise sa clef privée RSA pour décrypter la clef IDEA, et utilise ensuite la clef IDEA pour décrypter le message. Cela peut sembler compliqué, mais l'avantage est que le message, qui peut contenir une quantité importante d'informations, est crypté avec un chiffre symétrique rapide, et seule la clef IDEA, qui est relativement courte, est cryptée avec un chiffre asymétrique lent. Zimmermann prévoyait d'avoir cette combinaison de RSA et d'IDEA dans son produit PGP, mais voulait, pour offrir une interface conviviale à l'utilisateur, que celui-ci n'ait pas affaire à rentrer dans le détail de tous ces rouages.

Ayant, dans une large mesure, résolu le problème de la rapidité, Zimmermann apporta ensuite toute une série d'aménagements commodes. Par exemple, avant d'utiliser la partie RSA du PGP, Alice doit générer sa clef privée et sa clef publique personnelles. Créer une clef n'est pas une opération triviale, car elle demande de trouver une paire de nombres premiers géants. Pourtant Alice n'aura qu'à promener sa souris de manière erratique et le programme PGP fabriquera sa clef privée et sa clef publique — les mouvements de la souris introduisent un facteur aléatoire que PGP utilise pour assurer que chaque utilisateur ait sa propre paire distincte de nombres premiers et donc que sa clef privée et sa clef publique soient uniques. Après quoi, Alice n'a plus qu'à diffuser sa clef publique.

Par ailleurs, le PGP facilite la signature numérique d'un *e-mail*. D'habitude, l'*e-mail* ne porte pas de signature, ce qui rend impossible d'identifier l'authenticité d'un message électronique. Si Alice utilise un

e-mail pour envoyer une lettre d'amour à Bernard, elle la crypte normalement avec la clef publique de celui-ci, et lorsqu'il la reçoit, il la décrypte avec sa clef privée. Bernard est d'abord flatté, mais comment peut-il être sûr que la lettre est vraiment d'Alice ? La malveillante Ève a peut-être écrit l'*e-mail* et mis le nom d'Alice dessus. Sans une signature manuscrite, il n'y a pas de moyen évident pour vérifier l'auteur. Prenons un autre cas. Imaginons qu'une banque reçoive un *e-mail* d'un client qui donne l'ordre de transférer tous ses fonds sur un compte numéroté dans une banque des îles Caïman. Là encore, sans signature manuscrite, comment savoir si l'ordre émane vraiment du client ? L'*e-mail* peut avoir été écrit par un voleur essayant de faire virer de l'argent sur son compte personnel aux îles Caïman. Pour instaurer la confiance sur Internet, il est essentiel qu'il y ait une forme valable de signature numérique.

La signature digitale PGP est basée sur un principe déjà développé par Whitfield Diffie et Martin Hellman. Lorsqu'ils proposèrent l'idée de clefs publiques et de clefs privées différentes, ils comprirent que, outre la solution au problème de la distribution des clefs, leur système procurerait un mécanisme naturel pour générer des signatures électroniques. Nous avons vu dans le chapitre 6 que la clef publique sert au chiffrement et la clef privée au déchiffrement. En fait, on peut bouleverser le processus et utiliser la clef privée pour le chiffrement et la clef publique pour le déchiffrement. Ce mode de chiffrement est généralement inutilisé, car il offre peu de sécurité. Si Alice utilise sa clef privée afin de crypter un message pour Bernard, tout le monde peut le décrypter puisque tout le monde a la clef publique d'Alice. Toutefois, ce mode d'opération authentifie l'auteur, puisque si Bernard peut décrypter le message en utilisant la clef publique d'Alice c'est que le message a dû être crypté avec sa clef privée. Seule Alice possède cette clef privée, le message n'a donc pu être envoyé que par Alice.

En fait, si Alice veut envoyer une lettre d'amour à Bernard, elle a deux options. Ou elle crypte le message avec la clef publique de Bernard pour garantir la confidentialité, ou elle le crypte avec sa propre clef privée pour garantir l'authenticité. Si elle combine les deux options, elle peut garantir l'authenticité et la confidentialité. Il existe des procédés plus rapides, mais voici un moyen par lequel Alice peut envoyer sa lettre : elle commence par crypter le message en utilisant sa clef privée, puis crypte le texte chiffré obtenu avec la clef publique de Bernard. Nous pouvons nous représenter le message enfermé dans une première

coquille fragile, le chiffrement avec la clef privée d'Alice, puis dans une coquille extérieure solide, la clef publique de Bernard. Le texte chiffré qui en résulte ne peut être déchiffré que par Bernard, qui seul possède la clef privée nécessaire pour briser la dure coquille extérieure. Ayant déchiffré cette enveloppe extérieure, Bernard pourra facilement déchiffrer l'enveloppe intérieure avec la clef publique d'Alice. La coquille intérieure n'est pas là pour protéger le message, mais elle prouve que le message vient d'Alice, et non d'un imposteur.

À ce stade, envoyer un message PGP devient plutôt compliqué. Le chiffre IDEA est utilisé pour crypter le message, le RSA est utilisé pour crypter la clef IDEA et un autre niveau de chiffrement doit être ajouté si une signature digitale est nécessaire. Zimmermann parvint cependant à aménager son produit de façon que tout se fasse automatiquement, afin qu'Alice et Bernard n'aient pas à se soucier de mathématiques. Pour envoyer un message à Bernard, Alice écrira son *e-mail* et choisira une des options PGP dans un menu affiché sur l'écran de son ordinateur. Ensuite, elle tapera le nom de Bernard et PGP trouvera la clef publique de Bernard et fera automatiquement le chiffrement. En même temps, PGP effectuera les micmacs nécessaires pour la signature numérique du message. Lorsqu'il reçoit le message crypté, Bernard sélectionne l'option PGP, et PGP décrypte et authentifie l'auteur. Rien n'est original dans PGP (Diffie et Hellman avaient déjà pensé aux signatures numériques et d'autres cryptographes utilisaient une combinaison de chiffres symétrique et asymétrique pour accélérer le chiffrement), mais Zimmermann était le premier à réunir tout cela dans un logiciel de chiffrement facile à utiliser, et suffisamment efficace pour fonctionner sur un ordinateur personnel de puissance moyenne.

À la fin de l'été 1991, Zimmermann mettait la dernière main au PGP pour lui donner son aspect définitif. Deux problèmes demeuraient, dont aucun n'était technique. L'un des problèmes était que le RSA, qui est au centre du PGP, est un produit breveté, et la loi protégeant les brevets exigeait que Zimmermann obtienne une licence de la RSA Data Security Inc., avant de lancer son produit. Zimmermann décida d'ignorer ce problème. PGP n'était pas destiné à être un produit pour les transactions commerciales, mais plutôt pour les personnes privées ; il n'avait donc pas le sentiment d'empiéter sur le territoire de la RSA Data Security Inc. et espérait que la compagnie lui donnerait une licence gratuite le moment venu.

Un problème plus immédiat était le projet d'amendement anticriminalité émis par le Sénat américain en 1991, qui comportait la clause suivante : « Le sentiment du Congrès est que les fournisseurs de services de communications électroniques et les fabricants de matériel pour les communications électroniques devraient s'assurer que les systèmes de communication permettent au gouvernement d'obtenir une version claire des données, des voix et de tout autre communication lorsqu'une autorisation légale sera accordée. » Le Sénat s'inquiétait du développement de technologies digitales, comme les téléphones cellulaires, qui pourraient empêcher les représentants de la loi de procéder à des écoutes téléphoniques. Non content d'obliger les compagnies à garantir la possibilité des écoutes téléphoniques, le texte semblait aussi mettre en cause toute forme de chiffrement.

Une opposition concertée entre RSA Data Security Inc., l'industrie de la communication, et des groupes défenseurs des libertés civiles obtint l'abandon de l'article, mais on sentait bien que ce n'était qu'une victoire temporaire. Zimmermann craignait que, tôt ou tard, l'État tente de faire passer une loi qui rendrait illégal un chiffrement comme PGP. Il avait toujours pensé vendre PGP, mais maintenant il révisait ses options. Plutôt qu'attendre et voir le gouvernement interdire PGP, il jugea plus efficace de le rendre disponible à tout le monde avant qu'il ne soit trop tard. En juin 1991, il franchit un pas capital en demandant à un ami de faire figurer PGP sur un bulletin d'informations pour les utilisateurs du Net. Après tout, PGP n'est qu'un logiciel ; il pouvait donc être copié gratuitement par n'importe qui. PGP était maintenant lâché sur Internet.

Au début, PGP sema la perturbation chez les aficionados de la cryptographie. Ensuite, il fut exploité par un nombre grandissant d'internautes enthousiastes. Bientôt, les magazines d'informatique publièrent de brefs échos, puis de longs articles, sur le phénomène PGP. Graduellement, PGP envahissait jusqu'aux coins les plus retirés de la communauté informatique. Des associations pour les droits de l'homme commencèrent à crypter leurs documents avec PGP pour empêcher les documents de tomber dans les mains des régimes accusés d'atteintes aux libertés. Zimmermann recevait des *e-mails* le félicitant de son invention. « Il y a des groupes de résistance en Birmanie, dit Zimmermann, qui l'utilisent dans des camps d'entraînement dans la jungle. Ils disent que cela leur donne le moral, parce qu'avant l'arrivée de PGP, lorsque des documents étaient pris, cela entraînait l'arrestation, la torture et l'exécution de familles entières. » En 1991, le jour où Boris Eltsine

faisait sauter le bâtiment abritant le parlement à Moscou, Zimmermann reçut l'*e-mail* suivant envoyé de Lettonie : « Phil, je veux que vous sachiez : espérons que cela ne se produira pas, mais si jamais la dictature s'installait en Russie, votre PGP étant diffusé de la Baltique à l'Extrême-Orient il aidera les démocrates si nécessaire. Merci. »

Pendant que Zimmermann se faisait des admirateurs tout autour du monde, chez lui, en Amérique, il devenait la cible des critiques. La RSA Data Security Inc. avait décidé de ne pas lui accorder de licence gratuite et enrageait qu'on ait empiété sur son brevet. Même si Zimmermann avait mis PGP à la disposition du public sous la forme d'un logiciel gratuit, ce logiciel contenait le système RSA de cryptographie à clef publique et la RSA Data Security Inc. le taxa de piraterie. Zimmermann avait diffusé quelque chose qui appartenait à quelqu'un d'autre. La bataille autour du brevet se poursuivit pendant plusieurs années, et, à la même époque, Zimmermann rencontra un problème encore plus grave.

En février 1993, deux enquêteurs officiels lui rendirent visite. Après quelques questions préalables concernant l'atteinte à la protection du brevet, ils l'interrogèrent dans le cadre de l'accusation plus grave d'exportation illégale d'armement. Le gouvernement américain incluant les logiciels de chiffrement dans sa définition des munitions — au même titre que les missiles, les mitraillettes et les mortiers —, PGP ne pouvait pas être exporté sans une autorisation du Département d'État. Autrement dit, Zimmermann était accusé de trafic d'armes parce qu'il avait exporté PGP *via* Internet. Durant les trois années suivantes, il fut l'objet de l'enquête d'un grand jury et se retrouva poursuivi par le FBI.

Le chiffrement pour tous... ou non ?

L'enquête sur Phil Zimmermann et le PGP déclencha un débat sur les effets positifs et négatifs du chiffrement à l'âge de l'information. La diffusion de PGP obligea les cryptographes, les politiques, les défenseurs des libertés et les forces de l'ordre à s'interroger sur les implications d'un usage massif du chiffrement. Il y avait ceux qui, comme Zimmermann, pensaient que ce serait un bien, assurant aux individus la protection de leurs messages numériques. En face d'eux se dressaient ceux qui estimaient que le chiffrement généralisé constituait un danger pour la société, criminels et terroristes pouvant désormais communiquer impunément.

Le débat se poursuivit dans les années 90, et il n'est pas clos. La question fondamentale est de savoir si le gouvernement doit ou non légiférer sur la cryptographie. La liberté de chiffrement permettrait à tous, y compris les criminels, de se fier à leurs *e-mails*. D'un autre côté, restreindre l'usage de la cryptographie permettrait certes à la police de surveiller des criminels, mais lui permettrait aussi — à elle comme à d'autres — d'espionner le citoyen ordinaire. Au bout du compte, ce sont les peuples qui, à travers les gouvernements qu'ils éliront, décideront du rôle futur de la cryptographie. Ces pages sont destinées à exposer les deux points de vue. Il sera souvent fait référence aux diverses positions américaines et à leurs défenseurs, d'abord parce que l'Amérique est la patrie de PGP et ensuite parce que, quelle que soit la politique finalement adoptée en Amérique, elle aura des retombées sur celles des autres pays du monde.

L'opposition à l'élargissement de l'usage de la cryptographie est fondée sur le désir de *statu quo*. Pendant des décennies, toutes les polices du monde ont pratiqué des écoutes téléphoniques légales. Dès 1918, en Amérique, des enregistrements d'écoutes furent utilisés pour neutraliser des espions ennemis, et dans les années 20, ils se révélèrent utiles pour coincer des trafiquants d'alcool. L'idée que les écoutes téléphoniques constituaient un outil nécessaire à la défense de la légalité se renforça à la fin des années 60, lorsque le FBI s'aperçut que la mafia étendait son pouvoir dans le pays. Les défenseurs de l'ordre avaient beaucoup de peine à établir des charges contre les suspects, parce que l'organisation

criminelle menaçait tous ceux qui auraient pu témoigner contre elle et faisait régner la loi du silence. La police comprit que sa seule chance de trouver des preuves était d'utiliser des écoutes, et la Cour suprême se montra sensible à ses arguments. En 1967, on décida que la police pourrait recourir aux écoutes, sous réserve d'avoir obtenu une autorisation juridique.

Vingt ans plus tard, le FBI soutient toujours que « des écoutes téléphoniques légalement autorisées sont la seule technique d'investigation qui permette aux forces de l'ordre de lutter contre les drogues illégales, le terrorisme, les crimes de sang, l'espionnage et les mafias ». Or, ces écoutes deviendront inutile si les criminels ont accès au chiffrement. Un appel téléphonique fait sur une ligne numérique n'est rien de plus qu'un flot de nombres, et peut être crypté selon les techniques utilisées par les *e-mails*. Le PGPfone, par exemple, est l'un des nombreux produits capables de crypter des communications orales sur Internet.

Les mêmes défenseurs de l'ordre assurent que le chiffrement devrait être limité de façon à ce qu'ils puissent continuer leurs interceptions. La police a déjà rencontré des criminels qui se servaient de chiffres pour se protéger. Selon un expert juridique allemand, « les affaires brûlantes, comme les trafics d'armes ou de drogue, ne se règlent plus au téléphone, mais sont menées sous leur forme cryptée sur les réseaux de données internationaux ». Un officiel de la Maison-Blanche a signalé une même tendance inquiétante aux États-Unis, insistant sur le fait que « les membres des organisations criminelles comptent dans leurs rangs certains des meilleurs experts des systèmes informatisés et des chiffrements puissants ». Le cartel de Cali, par exemple, organise ses affaires de drogues au moyen de communications cryptées. Les défenseurs de la loi craignent donc qu'Internet couplé avec la cryptographie aide les criminels à communiquer, et ils s'inquiètent particulièrement des menées de ceux qu'on appelle les Quatre Cavaliers de l'Apocalypse — trafiquants de drogue, mafias, terroristes et pédophiles —, groupes qui bénéficieront le plus du chiffrement.

Criminels et terroristes cryptent également leurs plans et leurs archives. La secte Aum Shinrikyo, responsable de l'attaque par le gaz du métro de Tokyo en 1995, a utilisé le RSA pour crypter certains de ses documents. Ramsey Yousef, l'un des terroristes impliqués dans l'explosion du World Trade Center, avait sur lui des plans cryptés pour de futures actions terroristes. En dehors des organisations terroristes

internationales, des criminels plus ordinaires ont aussi recours à la cryptographie. En Amérique, un syndicat illégal de joueurs crypta ainsi ses comptes pendant quatre ans. Un rapport commandé par un organisme officiel américain, et rédigé par Dorothy Denning et William Baugh, estimait qu'il y avait à travers le monde cinq cents cas de criminalité faisant intervenir la cryptographie, et prédisait que ce nombre allait à peu près doubler chaque année.

À côté de la police domestique, il y a aussi des retombées pour la sécurité nationale. L'Agence américaine de sécurité nationale (la NSA) est chargée de recueillir des renseignements sur les nations ennemies en déchiffrant leurs communications. La NSA jouit d'un réseau international de postes d'écoutes, en coopération avec l'Angleterre, l'Australie, le Canada et la Nouvelle-Zélande, qui tous réunissent et partagent l'information. Le réseau inclut des sites comme la *Menwith Hill Signals Intelligence Base* dans le Yorkshire, la plus importante installation d'espionnage au monde. Une partie du travail de Menwith Hill se fait à l'aide du système *Echelon*, qui est capable de passer au crible *e-mails*, fax, Télex et appels téléphoniques pour y détecter certains mots précis. Echelon est fondé sur un lexique de mots suspects tels *Hezbollah*, *assassin* ou *Clinton* et le système est assez subtil pour reconnaître ces mots immédiatement. Echelon peut cocher des messages douteux pour leur faire subir un examen ultérieur, ce qui lui permet de surveiller les échanges de certains groupes politiques ou d'organisations terroristes. Évidemment, Echelon deviendrait caduc si tous les messages étaient sérieusement cryptés. Chacune des nations participant à Echelon perdrait une source considérable de renseignements sur les complots politiques et les attentats terroristes.

L'autre point de vue est soutenu par les défenseurs des libertés civiles, au sein desquels on trouve des groupes comme le *Center for Democracy and Technology* et l'*Electronic Frontier Foundation*. L'argumentation pro-chiffrement repose sur le fait que la confidentialité est un droit de l'homme fondamental, reconnu par l'article 12 de la Déclaration universelle des droits de l'homme : « Nul ne doit être soumis à des interventions arbitraires dans sa vie privée, sa famille, sa maison et sa correspondance, ni à des attaques touchant à son honneur et à sa réputation. Tous ont droit à la protection de la loi contre de telles interventions ou attaques. »

Les défenseurs des libertés estiment que l'usage le plus large du chiffrement est essentiel pour garantir le droit à la confidentialité — faute de quoi, selon eux, l'avènement de la technologie digitale, qui rend la surveillance beaucoup plus facile, marque le début d'une nouvelle ère pour les écoutes sauvages et les abus qu'elles entraînent inévitablement. Ils rappellent que les présidents Lyndon Johnson et Richard Nixon ont été convaincus d'avoir fait pratiquer des écoutes injustifiées et que le président John Kennedy avait ordonné des écoutes suspectes pendant le premier mois de sa présidence. Lors de discussions autour d'un projet de loi concernant les importations de sucre de la République dominicaine, Kennedy avait fait placer des micros chez plusieurs membres du Congrès, sous prétexte qu'il craignait qu'on ne les ait achetés. Pourtant, on ne trouva aucune preuve de pots-de-vin, et les enregistrements procurèrent seulement à Kennedy des informations utiles qui l'aiderent à faire passer sa loi.

Un des plus célèbres cas d'écoutes injustifiées durables concerne Martin Luther King, dont les conversations téléphoniques ont été surveillées pendant des années. En 1963, le FBI obtint par ce procédé un renseignement sur King qu'il livra au sénateur James Eastland pour qu'il l'exploite lors de débats sur les libertés individuelles. Plus généralement, le FBI rassembla des renseignements sur la vie privée de Martin Luther King, qu'on utilisa pour le discréditer. Des enregistrements de King racontant des histoires obscènes furent envoyés à sa femme et passés devant le président Johnson. Après l'attribution à King du prix Nobel, des détails embarrassants sur sa vie furent transmis à l'académie suédoise.

D'autres gouvernements se sont également rendus coupables d'abus d'écoutes téléphoniques. La Commission nationale de contrôle des interceptions de sécurité estime qu'il y a environ 100 000 écoutes illégales en France chaque année. Mais la plus grande attaque portée à la vie privée de tout un chacun est probablement le programme international Echelon. Echelon n'a pas à justifier ses interceptions, et ne s'attache pas à des individus en particulier. Sa moisson d'information se fait sans discrimination, à l'aide de récepteurs qui captent les télécommunications qui sont renvoyées par les satellites. Si Alice envoie un message transatlantique anodin à Bernard, il sera certainement intercepté par Echelon, et si le message se trouve contenir certains mots figurant dans le répertoire d'Echelon, il sera noté pour un examen ultérieur, au même titre que les messages de groupes extrémistes et

terroristes. Tandis que les tenants de la loi plaident que le chiffrement doit être interdit parce qu'il enlèverait toute efficacité à Echelon, les défenseurs des libertés estiment que le chiffrement est nécessaire justement pour rendre Echelon inefficace.

Lorsque les uns avancent que des chiffres sûrs empêcheront de confondre des criminels, les autres répondent que la protection de la vie privée est plus importante. Ces derniers ajoutent que le chiffrement ne sera d'ailleurs pas un obstacle à la défense de la légalité, parce que les écoutes sont rarement un élément crucial dans les enquêtes. En Amérique, en 1994, sur deux cent cinquante mille inculpations devant les tribunaux fédéraux, mille seulement ont été rendues possibles par des écoutes téléphoniques.

Parmi les avocats de la liberté cryptographique, on n'est pas surpris de trouver certains des inventeurs de la cryptographie à clef publique. Whitfield Diffie souligne que les personnes privées ont joui d'une totale confidentialité pendant une grande partie de notre histoire.

En 1790, quand la Déclaration des droits fut ratifiée, deux personnes pouvaient avoir une conversation privée (avec une sécurité que personne au monde ne pourrait avoir aujourd'hui) simplement en s'éloignant de quelques mètres de la route et en vérifiant que personne n'était caché dans les buissons. Il n'y avait pas de magnétophones, de microphones paraboliques, ou d'interféromètres laser rebondissant sur leurs verres de lunettes. Vous noterez que la civilisation a survécu. Beaucoup d'entre nous regardent cette période comme un âge d'or dans la culture politique américaine.

Et Ron Rivest, un des inventeurs du RSA, pense que restreindre la cryptographie serait imprudent :

C'est une bien misérable politique que de taper sans discrimination sur une technologie simplement parce que quelques criminels pourraient en tirer parti. N'importe quel citoyen américain peut s'acheter une paire de gants même si un cambrioleur peut s'en servir pour fouiller toute une maison sans laisser d'empreintes. La

cryptographie est une technologie de protection des données, comme les gants sont une technologie de protection des mains. [...] La première peut être frustrante pour les écoutes téléphoniques du FBI, et les seconds peuvent perturber les relevés d'empreintes du FBI. La cryptographie et les gants sont tous deux affreusement bon marché et faciles à se procurer. En fait, vous pouvez maintenant vous fournir en excellents logiciels de cryptographie sur Internet pour une somme inférieure au prix d'une paire de gants.

Les grands groupes industriels sont sans doute les meilleurs alliés des défenseurs de la cryptographie. Le commerce sur Internet en est encore à ses débuts, mais les ventes se développent rapidement. Vendeurs de livres, de CD et de logiciels ont ouvert la voie, suivis par les supermarchés, les compagnies de transport et bien d'autres entreprises qui s'engouffrent sur leurs traces. En 1998, un million d'Anglais ont utilisé Internet et acheté pour 400 millions de livres de produits — un chiffre qui quadruplera en 1999. Dans quelques années, le commerce sur Internet dominera le marché, à condition toutefois que les commerçants puissent fournir les moyens de la sécurité et de la confiance. Un commerce doit pouvoir garantir la confidentialité et la sécurité des transactions financières, et le seul moyen pour cela est d'employer un chiffrement efficace.

Actuellement, un achat sur Internet peut être protégé par la cryptographie à clef publique. Alice visite le site web d'une société et choisit un objet. Elle remplit alors un bulletin de commande qui lui demande son nom, son adresse et des précisions sur sa carte de crédit. La commande cryptée est transmise à la société qui peut seule la décrypter, car elle seule possède la clef privée nécessaire pour son décryptement. Tout ceci est fait automatiquement par le navigateur web d'Alice (par exemple Netscape ou Explorer) conjointement avec l'ordinateur de la société.

Comme toujours, la sécurité dépend de la taille de la clef. En Amérique, il n'y a pas de restrictions sur la longueur de la clef, mais les fabricants de logiciels américains ne sont pas autorisés à exporter ceux de leurs produits web qui permettent un chiffrement très sûr. Aussi les logiciels exportés dans le reste du monde ne peuvent manipuler que de courtes clefs et donc offrir une sécurité moyenne. En fait, si Alice, à

Londres, achète un livre à une société basée à Chicago, sa transaction est un milliard de milliards de milliards de fois moins sûre que la même transaction effectuée par Bernard, à New York, et la même société de Chicago. La transaction de Bernard est absolument sûre parce que son navigateur permet des chiffrements avec une clef plus grande, alors que la transaction d'Alice pourrait être déchiffrée par un individu déterminé. Heureusement, le coût du matériel nécessaire pour déchiffrer les spécifications de la carte de crédit d'Alice est beaucoup plus élevé que la limite autorisée de dépenses de la plupart des cartes de crédit, ce qui rend cette attaque peu rentable. Bref, si le commerce sur Internet est appelé à se développer, les consommateurs tout autour du monde doivent avoir une sécurité assurée, et les affaires ne tolèrent pas un chiffrement boiteux.

Le commerce réclame un chiffrement sûr pour une autre raison encore. Les grandes compagnies emmagasinent des quantités d'informations sur des bases de données informatisées, incluant des descriptions de produits, des indications sur leurs clients et des écritures comptables. Évidemment, ces compagnies veulent protéger cette information contre les pirates qui pourraient infiltrer l'ordinateur et dérober les renseignements. Cette protection peut être assurée par le chiffrement de l'information stockée, pour qu'elle ne soit accessible qu'aux employés possédant la clef de déchiffrement.

À l'heure actuelle, l'opinion populaire semble pencher pour la liberté de chiffrement, qui a été soutenue par certains médias et par deux films hollywoodiens récents. Début 1998, *Mercury Rising* racontait l'histoire d'un nouveau chiffre NSA, supposé infrangible, qui est déchiffré par inadvertance par un savant autiste de neuf ans. Alec Baldwin, agent de la NSA, organise l'assassinat de l'enfant, considéré comme dangereux pour la sécurité du pays. Heureusement, le gamin a Bruce Willis pour le protéger. La même année, Hollywood produisit *Enemy of the State*, qui traite d'un complot de la NSA pour assassiner un politicien qui défend un amendement favorable à un chiffrement fort. Le politicien est tué, mais un avocat, interprété par Will Smith, et un transfuge de la NSA, joué par Gene Hackman, finissent par traîner l'assassin devant les tribunaux. Les deux films donnent une image de la NSA plus sinistre encore que celle de la CIA, et dans bien des cas la NSA a effectivement endossé le rôle de gendarme des institutions.

Dans les derniers temps, une troisième option est apparue, qui propose un compromis. Pendant la dernière décennie, les cryptographes ont testé

le pour et le contre d'un schéma connu comme *l'escrow-key* — le séquestre des clefs. Le terme « séquestre » s'applique généralement à un arrangement par lequel une personne donne une certaine somme d'argent à une troisième personne, afin qu'elle puisse remettre cet argent à une deuxième personne dans certaines circonstances. Par exemple, un locataire peut déposer une garantie chez un notaire qui la versera au propriétaire si son bien est endommagé. En termes de cryptographie, *séquestre* signifie qu'Alice remettra une copie de sa clef à un tiers agréé, un intermédiaire indépendant et fiable, qui sera en mesure de transmettre cette clef privée à la police si celle-ci rassemble suffisamment de preuves qu'Alice est impliquée dans une affaire criminelle.

L'*American Escrowed Encryption Standard* fut conçu par le gouvernement américain et adopté en 1994. Son but était d'encourager l'adoption de deux cryptosystèmes, appelés *clipper* et *capstone*, destinés respectivement aux communications téléphoniques et aux communications électroniques. Pour utiliser clipper, Alice achètera un téléphone avec une puce pré-installée qui contiendra sa clef privée secrète. Au moment même où elle achète le téléphone, une copie de la clef privée contenue dans la puce sera coupée en deux morceaux, chaque moitié étant confiée à une autorité fédérale différente pour son stockage. Le gouvernement américain faisait valoir qu'Alice avait ainsi accès à un chiffrement sûr et que la confidentialité de ses communications ne serait enfreinte que si les forces de l'ordre pouvaient prouver aux deux organes officiels de séquestre qu'ils étaient fondés à demander sa clef privée.

Le gouvernement américain utilisa clipper et capstone pour son propre compte et les rendit obligatoires pour les sociétés travaillant avec lui. Les autres entreprises ou personnes privées étaient libres d'utiliser d'autres formes de chiffrement, mais le gouvernement espérait que clipper et capstone deviendraient peu à peu les systèmes favoris du pays. Ce ne fut pas le cas. Les défenseurs des droits civiques n'apprécièrent pas l'idée que les autorités fédérales disposent des clefs de tout le monde. Ils firent un rapprochement avec des clefs réelles et demandèrent ce que les gens penseraient d'un gouvernement qui aurait les clefs de toutes les maisons. Des experts en cryptographie firent remarquer qu'un seul employé indélicat pourrait miner tout le système en vendant des clefs au plus offrant. Et les entreprises s'inquiétèrent pour la confidentialité. Une entreprise européenne, par exemple, peut craindre que ses messages ne soient interceptés par des officiels américains qui pourraient livrer ces informations à des concurrents américains.

Malgré l'échec de *clipper* et *capstone*, certains gouvernements restent convaincus que le séquestre des clefs peut fonctionner, si les clefs sont bien à l'abri des tentatives criminelles et si des garanties sont données au public que le gouvernement n'abusera pas du système. Louis J. Freeh, directeur du FBI, déclara en 1996 : « Les représentants de la loi sont unanimement favorables à une politique de chiffrement équilibrée [...] Le séquestre des clefs n'est pas la seule solution, mais c'est une très bonne solution, car il répond aux besoins fondamentaux de la société en matière de confidentialité, de sécurité de l'information, de commerce électronique, de protection des personnes et de sûreté nationale. » Bien que le gouvernement américain ait fait marche arrière sur ses projets de séquestre, beaucoup pensent qu'il essaiera de les réintroduire dans l'avenir sous une autre forme. Ayant constaté le peu de succès d'un séquestre facultatif, il pourrait envisager un séquestre obligatoire. Pendant ce temps, les militants en faveur du chiffrement continuent leur lutte. « Les gens impliqués dans le débat sur la cryptographie, écrit le journaliste Neil Cukier, sont tous intelligents, honorables et favorables au séquestre. Mais aucun ne possède plus de deux de ces qualités à la fois. »

Le gouvernement pourrait choisir entre diverses options pour équilibrer les choses en fonction de chaque camp. Il est difficile de savoir quelle option sera retenue, car la politique actuelle concernant la cryptographie est fluctuante. Des événements nouveaux interviennent constamment dans le débat. En novembre 1998, le discours du Trône de la reine d'Angleterre annonçait une législation anglaise portant sur le marché digital. En décembre 1998, trente-trois nations signaient l'amendement Wassenaar limitant les exportations d'armement, qui couvre aussi les technologies cryptographiques puissantes. En janvier 1999, probablement sous la pression des milieux d'affaires, la France a abrogé ses lois concernant la cryptographie, jusqu'alors les plus restrictives en Europe de l'Ouest. En mars 1999, le gouvernement anglais a émis un document sur une proposition de charte du commerce électronique.

Dans les années à venir, nous allons sans doute assister encore à bien des tours et des détours sur les voies des politiques de la cryptographie. Un aspect de la cryptographie future semble pourtant certain, celui de la nécessité de l'authentification. Si Alice veut envoyer un *e-mail* sûr à son nouvel ami Zak, elle a besoin de la clef publique de Zak. Elle peut

demander à Zak de lui envoyer sa clef publique par la poste. Malheureusement, elle court le risque qu'Ève intercepte la réponse de Zak, la détruit et forge une nouvelle lettre dans laquelle elle enverra sa propre clef publique. Alice peut alors envoyer à Zak son *e-mail*, mais elle l'aura, sans le savoir, crypté avec la clef publique d'Ève. Si Ève peut intercepter cet *e-mail*, il lui sera facile de le déchiffrer. Un des problèmes de la cryptographie à clef publique est de savoir avec certitude si vous employez bien la clef publique exacte de votre correspondant. Des autorités d'authentification sont des organismes qui vérifient si telle clef publique appartient bien à telle personne. Un de ces organismes peut demander à rencontrer Zak en personne pour s'assurer que sa clef est enregistrée sans erreur. Si Alice fait confiance à cette autorité, elle peut obtenir d'elle la clef publique de Zak et être certaine que cette clef est la bonne.

J'ai expliqué comment Alice peut acheter des produits sur Internet en utilisant la clef publique d'une entreprise pour remplir le bon de commande. En réalité, elle ne le fera que si la clef publique a été validée par une autorité qui l'authentifie. En 1998, la première société d'authentification était *Verisign*, qui était devenue en quatre ans une affaire de 30 millions de dollars. Non contents de certifier des clefs publiques, ces organismes peuvent aussi garantir la validité de signatures digitales. En 1998, *Baltimore Technologies*, en Irlande, a authentifié les signatures digitales du président Bill Clinton et du Premier ministre Bertie Ahern. Ce qui leur a permis de signer numériquement un communiqué à Dublin.

Cela n'entraîne pas de risques pour la sécurité. On aura simplement demandé à Zak sa clef publique pour pouvoir la transmettre avec exactitude à ceux qui voudront lui envoyer des messages. Il y a d'autres sociétés qu'on appelle en anglais *trusted third parties* (TTP), en français tiers de confiance, qui fournissent un service plus discuté, appelé *key recovery*, le recouvrement des clefs. Imaginons un cabinet juridique qui protège tous ses documents en les cryptant avec sa clef publique propre, afin d'être seule à pouvoir les décrypter avec sa propre clef privée. Un tel système constitue une bonne mesure contre des pirates, mais que se passe-t-il si l'employé qui a la garde de la clef privée l'oublie, s'enfuit avec elle, ou est renversé par un autobus ? Les gouvernements encouragent la création de ces tiers agréés qui garderont des copies de toutes les clefs. Une entreprise qui perd sa clef privée pourra alors la retrouver auprès du tiers qu'elle aura choisi.

Évidemment, ce système est discutable car les tiers agréés auront à leur disposition les clefs privées, et pourront donc lire les messages de leurs clients. Ils doivent être dignes de confiance, sinon le système ne tient pas. Certains considèrent que ce n'est là qu'une nouvelle forme de séquestre et que les défenseurs de la loi pourront être tentés de forcer le tiers dépositaire à leur remettre la clef de son client si une enquête le demande. D'autres prétendent que ce dépôt fait partie de l'infrastructure nécessaire pour une cryptographie à clef publique.

Personne ne peut prédire quel rôle jouera ce tiers de confiance dans le futur, et personne ne peut prévoir avec certitude la forme que prendra la politique cryptographique dans dix ans. Je soupçonne pourtant que, dans le futur, les militants prochiffrement gagneront d'abord la bataille, surtout parce qu'aucun pays ne voudra appliquer des lois sur la cryptographie qui porterait tort au commerce électronique. Si cette politique se révèle être une erreur, il sera toujours possible de changer les lois. Devant une série d'attentats terroristes que des écoutes auraient peut-être pu éviter, les gouvernements verront l'opinion devenir favorable à la politique du séquestre. Tous les usagers de forts chiffrements seront tenus de déposer leurs clefs chez un agent agréé du séquestre, et toute personne qui enverra un message crypté avec une clef non déposée sous séquestre sera passible de poursuites. Si les condamnations sont suffisamment sévères, les défenseurs de la loi reprendront le contrôle des communications. Plus tard, si les gouvernements abusent de la confiance placée dans ce système de séquestre, le public réclamera un retour à la liberté cryptographique et le mouvement du balancier reviendra à sa place précédente. En vérité, il n'y a pas de raisons pour que nous ne changions pas de politique cryptographique en fonction des événements politiques, économiques et sociaux. Le facteur prépondérant viendra de ce que le public redoutera le plus, des criminels ou du gouvernement.

La réhabilitation de Zimmermann

En 1993, Zimmermann fit l'objet d'une enquête de la part d'un grand jury. Selon le FBI, il avait exporté des munitions, puisqu'il avait fourni à des nations ennemies et à des terroristes les outils dont ils avaient besoin pour échapper au contrôle du gouvernement américain. Plus l'enquête avançait, plus les cryptographes et les défenseurs des droits civiques se portaient au secours de Zimmermann, créant même un fonds de financement international pour payer ses avocats. En même temps, le fait d'être l'objet d'une enquête du FBI fit la promotion du PGP — un chiffrement si sûr qu'il faisait peur au FBI.

Pretty Good Privacy avait été diffusé à la hâte à ses débuts, et le produit n'avait pas été aussi peaufiné qu'il aurait pu l'être. Il y eut bientôt un concert de voix qui s'élevèrent pour réclamer une version révisée de PGP, mais visiblement Zimmermann n'était pas en position de continuer à travailler sur ce produit. Des ingénieurs européens commencèrent à reconstruire PGP. D'une manière générale, l'attitude des Européens envers le chiffrement était — et est encore — plus libérale, et il n'y avait aucune restriction à l'exportation d'une version européenne de PGP à travers le monde. De plus, le brevet RSA n'était pas protégé en Europe, puisqu'il n'avait été déposé que pour l'Amérique.

Au bout de trois ans, l'enquête du grand jury n'avait toujours pas conduit Zimmermann devant un tribunal. Le cas est rendu complexe par la nature de PGP et la manière dont il a été distribué. Si Zimmermann avait programmé PGP sur un ordinateur et l'avait envoyé à un régime ennemi, les poursuites contre lui auraient été simples, puisqu'il aurait été coupable d'avoir exporté un système de chiffrement prêt à l'emploi. De même, s'il avait exporté une disquette contenant le programme PGP, l'objet aurait pu être considéré comme du matériel cryptographique, et là encore le cas de Zimmermann serait clair. D'un autre côté, s'il avait fait imprimer le programme et l'avait exporté comme un livre, les charges contre lui ne seraient pas claires, parce qu'il aurait alors été considéré comme ayant exporté un savoir plutôt qu'un objet cryptographique. Pourtant, le matériel imprimé peut être scanné électroniquement et téléchargé, ce qui rend le livre aussi dangereux que la disquette. Ce qui se passa réellement fut que Zimmermann confia une copie de PGP à un

ami qui le programma simplement sur un ordinateur américain connecté à Internet. Après quoi, un régime hostile l'a peut-être, ou peut-être pas, utilisé. Zimmermann était-il vraiment coupable de l'exportation de PGP ? Aujourd'hui encore, les textes juridiques concernant Internet sont l'objet de discussions et d'interprétations. Au début des années 90, la situation était extrêmement vague.

En 1996, après trois ans d'enquête, le Bureau de l'attorney général américain abandonna ses poursuites contre Zimmermann. Le FBI comprit qu'il était trop tard. Le PGP s'était évadé sur l'Internet, et poursuivre Zimmermann n'y changerait rien. Un problème s'ajoutait à cela, et c'était le soutien apporté à Zimmermann par des institutions importantes comme les éditions du MIT (Massachusetts Institute of Technology) qui avait publié PGP sous la forme d'un livre de 600 pages. Le livre était distribué dans le monde entier, et poursuivre Zimmermann aurait entraîné de poursuivre MIT Press. Le FBI hésitait aussi à poursuivre une procédure dans laquelle il n'était pas certain que Zimmermann serait condamné. Un procès du FBI pouvait n'amener qu'un débat embarrassant sur le droit à la vie privée, qui entraînerait dans le public plus de sympathie encore pour un chiffrement universel.

Un autre grave souci de Zimmermann fut lui aussi résolu. Il finit par parvenir à un accord avec RSA et obtint une autorisation concernant l'application du brevet. PGP était enfin un produit légitime et Zimmermann un homme libre. L'enquête avait fait de lui un croisé de la cryptographie, et tous les directeurs commerciaux du monde doivent avoir envié la notoriété et la publicité gratuite que l'affaire avait offertes à PGP. Fin 1997, Zimmermann vendit PGP à *Network Associates* et devint l'un de ses dirigeants. Bien que PGP soit maintenant vendu aux entreprises commerciales, il est toujours disponible gratuitement pour les personnes qui n'ont pas l'intention d'en faire un usage commercial. Autrement dit, les gens qui veulent simplement exercer leur droit à la confidentialité peuvent toujours trouver PGP sur Internet sans payer.

Si vous voulez obtenir une copie de PGP, plusieurs sites Internet vous l'offrent, et vous les trouverez assez facilement. La source la plus sûre est sans doute à <http://www.pgpi.com/>, l'International PGP Home Page, où vous vous procurerez les versions américaine et internationale. Maintenant, je voudrais dégager ma responsabilité. Si vous choisissez d'installer PGP, à vous de vérifier si votre ordinateur est capable de le gérer, si le logiciel n'a pas de virus, et ainsi de suite. Vérifiez aussi que vous vivez dans un pays qui autorise l'usage de chiffrements forts. Enfin,

assurez-vous que vous prenez bien la version appropriée de PGP : des personnes vivant à l'extérieur des États-Unis ne doivent pas posséder la version américaine de PGP, parce qu'il y aurait viol des lois sur l'exportation. Seule la version internationale de PGP n'est soumise à aucune restriction.

Saut quantique dans le futur

Pendant deux millénaires, les créateurs de codes se sont évertués à protéger des secrets, et les briseurs de codes ont fait de leur mieux pour les découvrir. Cela a toujours été une lutte au corps à corps, avec des attaquants désarmés lorsque les concepteurs de code étaient les plus forts, et des inventeurs contraints de créer de nouvelles formes de chiffrement lorsque leurs systèmes précédents étaient compromis. L'invention d'une cryptographie à clef publique et le débat politique autour de l'usage d'une cryptographie forte nous amènent à l'époque actuelle, où il est clair que les cryptographes sont en train de gagner la guerre de l'information. Non seulement les codes d'aujourd'hui sont, de fait, indéchiffrables, mais le problème de distribution des clefs a été résolu. Selon Philip Zimmermann, nous vivons un âge d'or de la cryptographie : « Avec les moyens modernes, on peut coder en restant réellement hors de portée de toute forme connue de cryptanalyse. Et je pense que cet état de choses va durer. » L'avis de Zimmermann est partagé par William Crowell, directeur adjoint de la NSA, qui déclare : « À supposer que tous les ordinateurs personnels du monde — au nombre de 260 millions environ — soient mis au travail sur un seul message crypté selon PGP, il faudrait un temps estimé à 12 millions de fois l'âge de l'univers pour décrypter un seul message. »

Toutefois, l'expérience passée nous montre que chaque code réputé inviolable a, tôt ou tard, succombé à la sagacité des cryptanalystes. Le code de Vigenère fut appelé « *le chiffre indéchiffrable* », jusqu'à ce que Babbage en vienne à bout, et Enigma a été considéré comme invulnérable, avant que les Polonais n'en révèlent les faiblesses. Les analystes sont-ils donc au seuil d'une nouvelle révolution, ou est-ce Zimmermann qui a raison ? Il est toujours très risqué de prédire les développements futurs de n'importe quelle technologie, mais dans le cas des chiffrements, c'est particulièrement aventureux. Non seulement il nous faut deviner quelles découvertes interviendront dans le futur, mais aussi lesquelles ont déjà été faites, et sont restées cachées. L'histoire de

James Ellis et du GCHQ nous avertit qu'il peut y avoir des percées remarquables cachées sous le voile du secret d'État.

Dans ce dernier chapitre, nous verrons quelques-unes des idées futuristes qui peuvent améliorer ou détruire la confidentialité au XXI^e siècle. La première partie traitera de l'avenir de la cryptanalyse, et d'une idée en particulier qui pourrait permettre de briser tous les chiffrements actuels. La deuxième partie porte, elle, sur le projet le plus captivant, un système cryptographique qui aurait un potentiel suffisant pour garantir le secret absolu.

L'avenir de la cryptanalyse

En dépit de la puissance considérable de RSA et des autres chiffres modernes, les cryptanalystes sont encore capables de tenir un rôle éminent dans la collecte des renseignements. Leur succès est démontré par le fait qu'ils sont plus que jamais demandés. C'est ainsi que la NSA reste le premier employeur de mathématiciens au monde.

Il n'y a qu'une fraction des informations qui circulent autour du monde qui soit cryptée en toute sécurité. La plus grande partie est faiblement cryptée ou pas du tout. En effet, si le nombre d'abonnés à Internet augmente rapidement, rares sont ceux qui prennent les précautions adéquates en matière de secret. C'est pourquoi les organismes nationaux de sécurité, les représentants de la loi ou toutes les personnes à l'esprit curieux peuvent se procurer plus d'informations qu'ils n'en peuvent traiter.

Même si les usagers appliquent correctement le chiffre RSA, il reste quantité de renseignements que les briseurs de codes peuvent glaner sur les messages interceptés. Ils emploient toujours la vieille technique de l'analyse des flux ; à défaut de découvrir le contenu d'un message, ils peuvent en trouver l'auteur et le destinataire, ce qui en soi est déjà une information. Récemment s'est développée la *tempest-attack*, qui consiste à détecter les signaux électromagnétiques émis par les composants électroniques d'un ordinateur. En garant sa voiture devant la maison d'Alice, Ève peut utiliser un équipement détecteur approprié pour identifier chaque touche qu'Alice actionne sur son clavier, et ainsi intercepter le message avant qu'il soit crypté et envoyé. Elle pourrait également s'emparer d'autres informations, telles que des clefs. Pour se protéger de ces attaques, certaines compagnies fournissent un matériel d'écrantage à installer sur les murs de la pièce pour éviter toute émission électromagnétique. Aux États-Unis, il faut une licence gouvernementale pour se procurer ce matériel, ce qui dit assez que des organisations comme le FBI doivent faire un usage courant de cette surveillance.

Parmi les autres attaques, citons les *virus* et le *cheval de Troie*. Ève pourrait concevoir un virus qui infecte le logiciel PGP et s'installe tranquillement dans l'ordinateur d'Alice. Quand Alice utilisera sa clé privée pour décrypter un message, le virus pourrait se réveiller et en

prendre note. La fois suivante où Alice se connectera à Internet, le virus enverra subrepticement la clef à Ève, ce qui lui permettra de déchiffrer tous les messages envoyés par la suite à Alice. Le cheval de Troie, une autre astuce, consiste pour Ève à concevoir un logiciel de codage apparaissant comme normal, mais en réalité traître à son utilisateur. Par exemple, Alice pourrait croire qu'elle charge une copie authentique de PGP, alors qu'en réalité c'est une version *cheval de Troie*, version modifiée qui ressemble à l'authentique programme PGP, mais qui contient des instructions destinées à envoyer à Ève des copies en clair de toute la correspondance d'Alice. Comme le formule Phil Zimmermann : « N'importe qui pourrait modifier le logiciel et produire une imitation lobotomisée — un zombie en quelque sorte — de PGP, apparemment normale, mais qui accomplirait les ordres de son maître diabolique. Cette version *cheval de Troie* pourrait être diffusée largement et semblerait être de moi. Quelle trahison ! Vous devez tout faire pour vous procurer votre exemplaire de PGP d'une source absolument sûre, quoi qu'il en coûte. »

Une variante du cheval de Troie serait un logiciel de chiffrement entièrement nouveau, qui apparaîtrait comme sûr, mais qui en réalité contiendrait une sortie dérobée, permettant à ses créateurs de décrypter tous les messages émis. En 1998, un rapport de Wayne Matsen a révélé que la compagnie suisse Crypto AG avait établi de telles issues dans quelques-uns de leurs produits et avait procuré au gouvernement américain toutes précisions permettant de les exploiter. Les Américains étaient donc capables de lire les communications d'autres pays. C'est ainsi qu'en 1991 furent capturés les assassins de Chapour Bakhtiar, l'ancien premier ministre iranien en exil en France, grâce à l'interception et au déchiffrement clandestin des messages iraniens cryptés avec du matériel Crypto AG.

Bien que l'analyse des flux, les attaques en tempête, les virus, les chevaux de Troie offrent tous des moyens efficaces pour se procurer des informations, les cryptanalystes se rendent bien compte que leur vrai but est de casser le chiffre RSA, pierre angulaire du chiffrement moderne. Le chiffre RSA sert à protéger les plus importantes communications militaires, diplomatiques, commerciales ou judiciaires, qui sont au premier chef les messages que les officines de renseignement cherchent à déchiffrer. Pour vaincre le robuste système RSA, les cryptanalystes doivent faire une découverte majeure, soit technique, soit théorique.

Une percée théorique pourrait être un moyen fondamentalement nouveau pour trouver la clef privée d'Alice, définie par p et q , que l'on

trouve en factorisant la clef publique, N . L'approche normale consiste à essayer chaque nombre premier successivement pour voir s'il est diviseur de N , mais nous savons que ceci prend un temps déraisonnable. Les cryptanalystes ont essayé de trouver un raccourci, une méthode qui réduirait drastiquement le nombre d'étapes pour trouver p et q , mais jusqu'à présent toutes les tentatives pour développer une méthode rapide de factorisation ont échoué. En fait, les mathématiciens étudient la factorisation depuis des siècles, et les techniques modernes ne sont pas radicalement meilleures que les anciennes. Il se pourrait même que les lois des mathématiques interdisent tout simplement l'existence d'une méthode plus rapide.

Sans réel espoir d'une percée théorique, on en est réduit à chercher une innovation technologique. S'il n'y a aucune méthode pour réduire le nombre d'étapes nécessaires à une factorisation, alors les cryptanalystes ont besoin d'une technologie qui effectue ces étapes plus rapidement. Les puces de silicium continueront à gagner en vitesse dans les années qui viennent, à raison d'un doublement tous les dix-huit mois, mais ce n'est pas encore suffisant pour avoir un réel impact sur la vitesse de factorisation. Les cryptanalystes ont besoin d'une technologie des milliards de fois plus rapide que celle d'aujourd'hui, aussi se tournent-ils vers une forme radicalement nouvelle d'ordinateur, l'*ordinateur quantique*. Si les scientifiques pouvaient construire un tel instrument, celui-ci effectuerait les calculs à une telle vitesse qu'il ravalerait les superordinateurs modernes au rang de bouliers.

Le concept d'ordinateur quantique nécessite l'exposition de certains principes de la physique quantique, appelée aussi mécanique quantique. Au préalable, il est bon de se rappeler l'avertissement lancé à l'origine par Niels Bohr, un des pères fondateurs de la mécanique quantique : « Quiconque peut contempler la mécanique quantique sans avoir le vertige n'y a rien compris. » Autrement dit, il faut s'attendre à rencontrer ici quelques idées surprenantes.

Pour expliquer les principes du calcul quantique, il est utile de revenir à la fin du XVIII^e siècle et au travail de Thomas Young, ce savant anglais qui fit la première avancée dans le déchiffrement des hiéroglyphes égyptiens. Alors chargé de cours à l'Emmanuel College de Cambridge, Young se reposait souvent l'après-midi au bord de la mare aux canards située aux abords du collège. Un jour, selon la légende, il remarqua deux canards qui nageaient gaiement l'un à côté de l'autre, et observa que les

deux sillages laissaient des rides qui interagissaient entre elles et formaient un curieux dessin. Les deux suites de vagues s'estompaient derrière les deux canards, et là où une crête de vague causée par l'un d'eux rencontrait le creux d'une vague venue de l'autre, il en résultait une zone d'eau calme. Le sommet et le creux s'annulaient mutuellement. Par ailleurs, lorsque deux crêtes de vagues arrivaient au même point simultanément, il en résultait une vague encore plus grosse, et si c'étaient deux creux de vagues, il en résultait un creux plus profond encore. Il en fut fasciné, particulièrement parce que les canards lui rappelaient une expérience sur la nature de la lumière qu'il avait menée en 1799.

Dans ses expériences précédentes, la lumière arrivait sur une plaque comportant deux fentes verticales étroites comme il est montré sur la figure 71 (a). Sur un écran placé derrière le plan des fentes, Young s'attendait à voir deux raies lumineuses, projetées par les fentes. Au lieu de cela, il remarqua que la lumière se dispersait en éventail au sortir des deux fentes et formait sur l'écran une alternance de franges lumineuses et de franges sombres. Ces rayures de lumière sur l'écran l'avaient intrigué, mais il croyait être désormais en mesure de l'expliquer complètement, d'après ce qu'il avait vu sur la mare aux canards.

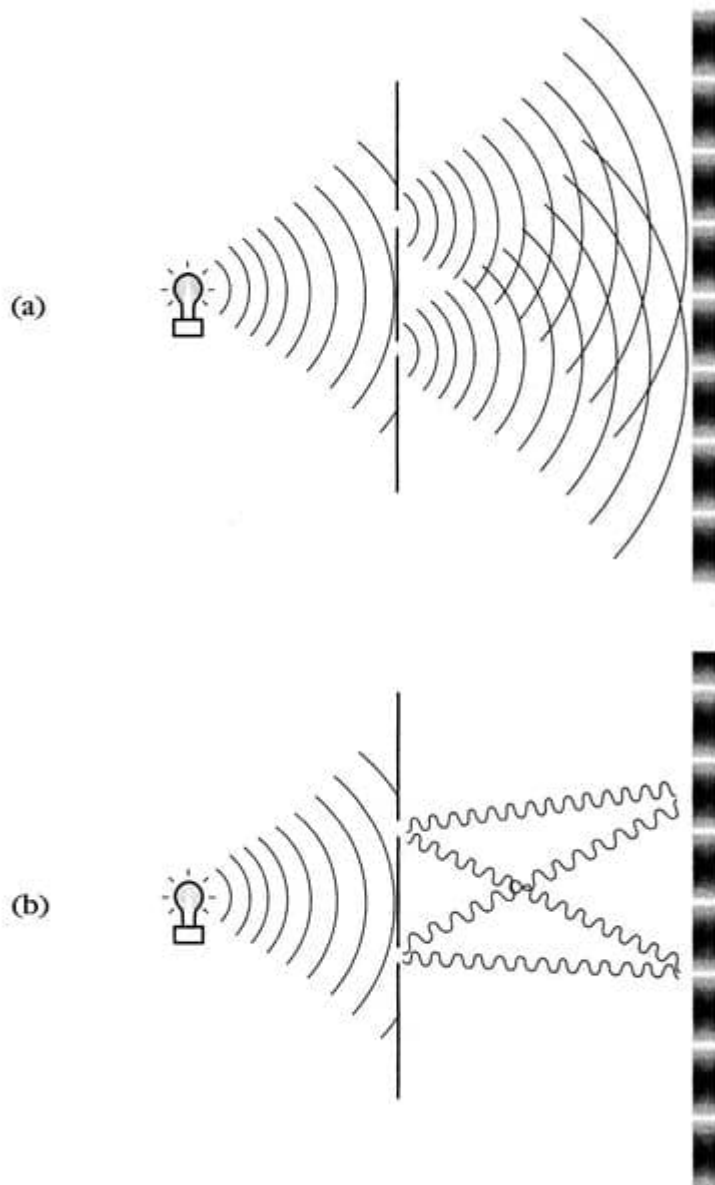


Fig. 71 Dispositif des fentes de Young, vue de dessus. Le diagramme (a) montre la lumière se déployant en éventail à la sortie des deux fentes dans la plaque, interagissant et créant un dessin de rayures sur l'écran. Le diagramme (b) montre comment des vagues distinctes interagissent. Si un creux rencontre une crête sur l'écran le résultat est une rayure sombre. Si deux creux (ou deux crêtes) se rencontrent sur l'écran, elles donnent une raie claire.

Young commença par supposer que la lumière était une sorte d'ondulation. D'où l'analogie des ondes lumineuses émanant des deux fentes avec les ondes de surface derrière les deux canards. De plus, les bandes lumineuses et obscures sur l'écran étaient causées par ces mêmes interactions qui amenaient les ondes aquatiques à former des sommets élevés, des creux plus profonds et des zones de calme. Young pouvait se représenter des points sur l'écran où un creux rencontre un sommet avec pour résultat une annulation et une raie sombre, et des points de l'écran où la rencontre de deux sommets se renforçant formaient une raie

brillante, comme on le voit sur la figure 71 (b). Ce sont les canards de l'Emmanuel College qui firent pénétrer Thomas Young plus avant dans la vraie nature de la lumière, et il finit par publier *La Théorie ondulatoire de la lumière*, un classique impérissable parmi les publications de physique.

Nous savons aujourd'hui que la lumière se comporte effectivement comme une onde, mais également comme une particule. La perception de la lumière comme une onde ou une particule dépend des circonstances, et c'est cette ambiguïté qui est connue comme la dualité onde-corpuscule. Nous n'en dirons pas plus sur la dualité, si ce n'est que la physique moderne décrit un faisceau de lumière comme un ensemble innombrable de particules individuelles — les photons — qui manifestent des propriétés ondulatoires. L'expérience de Young nous montre donc un flot de photons passant à travers les fentes, et interagissant de l'autre côté de l'écran.

Jusque-là, il n'y aurait rien de particulièrement étrange dans cette expérience. Cependant, les techniques modernes permettent aux physiciens de la reproduire en utilisant un filament de lampe si faible qu'il émet les photons un par un. Si les photons sont produits, par exemple, à un rythme de un par minute, alors chacun d'eux voyage seul vers la plaque, passe à travers l'une des deux fentes et parvient finalement sur l'écran. Bien que nos yeux ne soient pas assez sensibles pour voir des photons individuellement, on peut les observer avec un détecteur approprié, et en l'espace de quelques heures nous pourrions construire un schéma d'ensemble des points d'impact des photons sur l'écran. Avec un seul photon à la fois à travers les fentes, nous ne nous attendons pas à voir le réseau de franges observé par Young, parce que ce phénomène semble dériver du passage de deux photons à travers une fente et interagissant entre eux de l'autre côté de la plaque. Cependant, pour quelque raison extraordinaire, on obtient ce réseau de franges claires et sombres même avec des photons individuels, exactement comme s'ils avaient interagi.

Ce résultat bizarre défie le sens commun. Impossible de décrire le phénomène par les lois classiques de la physique, celles qui expliquent le comportement des objets de tous les jours. La physique classique peut expliquer les orbites des planètes ou la trajectoire d'un boulet de canon, mais elle est incapable de décrire pleinement le monde du vraiment petit, tel que la trajectoire d'un photon. Pour expliquer des phénomènes impliquant des photons, les physiciens ont donc recours à la théorie

quantique, une explication du comportement des objets au niveau microscopique. Cependant, même les théoriciens quantiques ne peuvent s'entendre sur l'interprétation de la bi-fente de Young. Ils tendent à se répartir en deux camps, chacun avec sa propre interprétation.

Le premier camp met en avant l'idée de *superposition*. Les superpositionnistes commencent par établir que, du photon, nous ne connaissons que deux choses certaines : il a quitté le filament et il atteint l'écran. Tout le reste est un mystère complet, y compris le fait de savoir si le photon est passé par la fente de gauche ou celle de droite. Et puisque le cheminement exact du photon est inconnu, les superpositionnistes adoptent le point de vue très spécial qu'il est passé par les deux simultanément, ce qui lui permettrait alors d'interférer avec lui-même et de créer les rayures observées sur l'écran. Mais comment *un* photon peut-il passer par *deux* fentes ?

Les superpositionnistes imaginent quelque chose comme ce qui suit. Si nous ne savons pas ce que fait une particule, alors elle est autorisée à faire simultanément tout ce qui est possible. Dans le cas du photon, nous ne savons pas s'il est passé à gauche ou à droite, alors nous supposons qu'il est passé par les deux côtés simultanément. Chaque possibilité est appelée *état*, et puisque le photon possède les deux possibilités, on dit alors qu'il est dans une *superposition d'états*. Nous savons qu'un photon a quitté le filament et nous savons qu'un photon a frappé l'écran de l'autre côté de la plaque, mais entre les deux il a en quelque sorte explosé en deux photons fantômes qui sont passés à travers les deux fentes. Cela peut paraître stupide, mais au moins cela explique le réseau de franges qui résulte de l'expérience de Young réalisée avec des photons individuels. En comparaison, la vue classique démodée est que le photon est passé par l'une des deux fentes, sans que nous sachions laquelle. C'est en apparence bien plus sensé que la vue quantique, mais malheureusement incapable d'expliquer le résultat observé.

Erwin Schrödinger, prix Nobel de physique en 1933, inventa une parabole connue sous le nom de *Chat de Schrödinger*, souvent invoquée pour expliquer le concept de superposition. Imaginons que nous plaçons un chat dans une boîte. Il y a deux états possibles pour le chat, mort ou vivant. Initialement, nous savons que le chat est dans un état bien défini, car nous pouvons voir qu'il est vivant. À ce point, le chat n'est pas dans une superposition d'états. Ensuite, nous plaçons une fiole de cyanure dans la boîte et fermons le couvercle. Nous entrons maintenant dans une période d'ignorance, parce que nous ne pouvons voir ni mesurer l'état du

chat. Est-il encore vivant ou a-t-il trébuché sur la fiole de cyanure et perdu la vie ? Traditionnellement, nous dirions que le chat est soit mort soit vivant, sans pouvoir décider. Au contraire, la théorie quantique dit que le chat est dans une superposition d'états — il est à la fois mort et vivant, il satisfait toutes les possibilités. La superposition ne se produit que lorsque nous perdons la trace d'un objet, et c'est une façon de décrire un objet pendant une période d'ambiguïté. Quand nous ouvrons la boîte à la fin, nous pouvons voir si le chat est vivant ou mort. L'action de regarder le chat le contraint à être dans un état particulier, et c'est à ce moment précis que la superposition disparaît.

Pour les lecteurs qui se sentent mal à l'aise avec la superposition, il y a un second camp quantique qui fait une autre interprétation de l'expérience de Young. Malheureusement, cette interprétation est tout aussi bizarre que la précédente. L'interprétation dite des *univers parallèles*, revient à dire que, en quittant le filament, le photon a deux options — passer par la fente de gauche, ou par la fente de droite —, à partir de quoi l'univers se divise en deux univers, avec dans l'un le photon passant par la fente de gauche, dans l'autre le photon passant par celle de droite. Ces deux univers interfèrent de quelque manière l'un avec l'autre, ce qui justifie le réseau de franges. Les tenants des univers parallèles pensent que, toutes les fois qu'un objet a la possibilité d'entrer dans l'un quelconque de plusieurs états possibles, l'univers se divise en une multitude d'univers, en sorte que chaque option se déroule dans un univers différent. On a donné à cette prolifération d'univers le nom de *multivers*.

Que l'on adopte le parti de la superposition ou celui des univers parallèles, la théorie quantique est une philosophie troublante. Néanmoins, elle s'est imposée comme la théorie scientifique la plus fructueuse et la plus efficace jamais conçue, aussi bien adaptée pour expliquer l'expérience des franges de Young que quantité d'autres phénomènes. Seule la théorie quantique permet aux physiciens de calculer les conséquences des réactions nucléaires dans les centrales électriques. Seule la théorie quantique peut expliquer les miracles de l'ADN, ou le rôle des molécules dans les réactions chimiques, et seule la théorie quantique permet de concevoir le laser qui lit les CD sur votre stéréo. Que nous le voulions ou non, nous vivons dans un monde quantique.

De toutes les conséquences technologiques de la théorie quantique, la plus importante est sans doute l'ordinateur. Exterminateur de la sécurité

de tous les chiffrements modernes, l'ordinateur quantique ouvrirait aussi une ère nouvelle de l'informatique. L'un des pionniers de l'informatique, le physicien britannique David Deutsch, commença à imaginer ce concept en 1984, lors d'un colloque consacré à la théorie de l'informatique. C'est en écoutant une des conférences du colloque qu'il mit le doigt sur quelque chose qui avait été négligé jusque-là. Il était, en effet, tacitement entendu que les calculateurs fonctionnaient selon les lois de la physique classique, mais Deutsch acquit la conviction qu'ils devaient plutôt obéir à la mécanique quantique, plus fondamentale.

Les ordinateurs courants opèrent à un niveau que l'on peut qualifier de macroscopique, où les deux domaines ne se distinguent pratiquement pas. Il était dès lors sans importance que les scientifiques aient généralement conçu les ordinateurs selon la physique classique. Mais au niveau microscopique, les deux physiques divergent, et la mécanique quantique a force de loi. Au niveau microscopique, les lois quantiques révèlent pleinement leur étrangeté, et un ordinateur conçu pour exploiter ces lois se comporterait de façon radicalement nouvelle. Après le colloque, Deutsch rentra chez lui et commença à refondre la théorie des ordinateurs selon la nouvelle physique. Il décrivit sa vision d'un ordinateur quantique dans un article publié en 1985, expliquant en particulier en quoi il différerait d'un ordinateur classique.

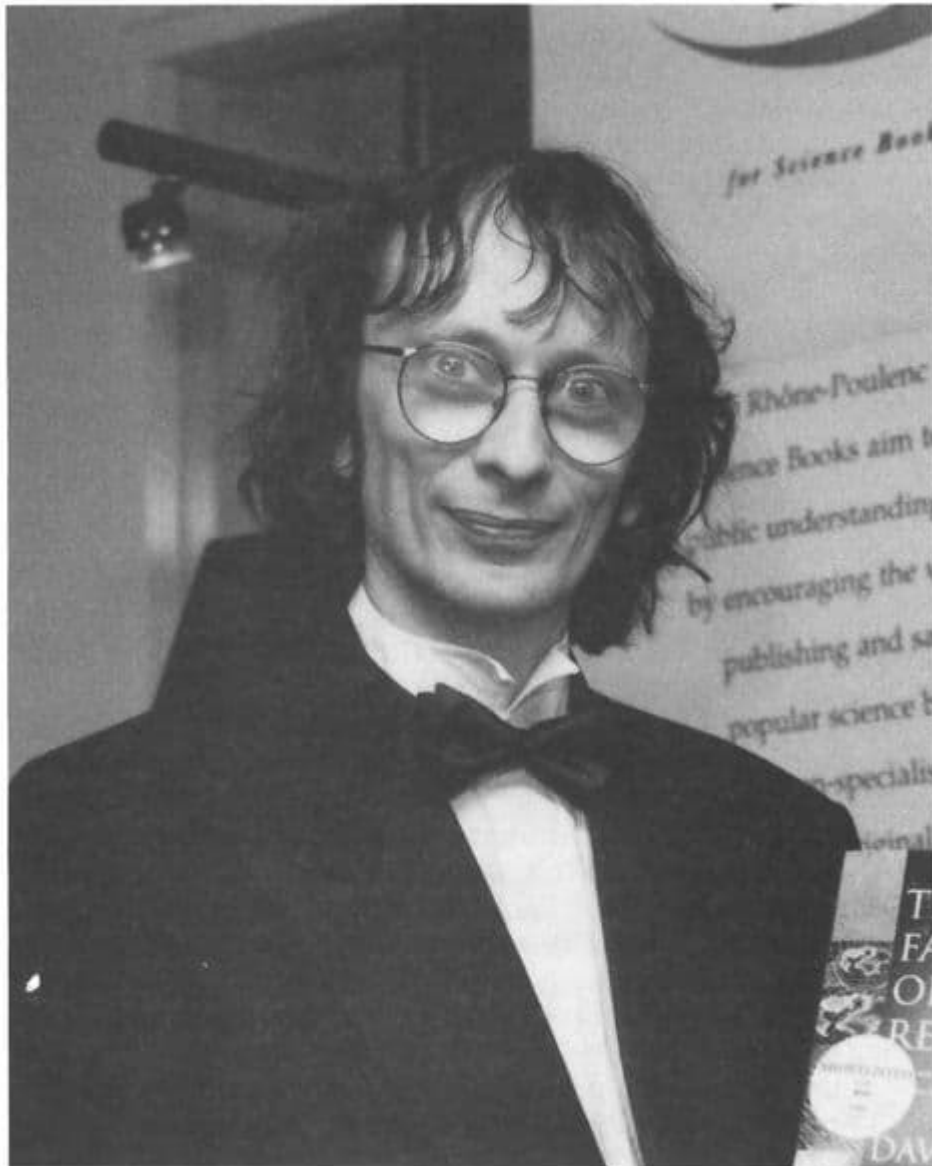


Fig. 72 David Deutsch.

Imaginez que vous ayez deux variantes d'une même question. Pour répondre aux deux questions avec un ordinateur classique, l'opérateur aurait à introduire la première question, attendre la réponse, puis à poser la seconde variante et attendre la réponse. En d'autres termes, un ordinateur banal ne peut poser qu'une question à la fois, et s'il y a deux questions possibles, il doit les traiter l'une après l'autre. Au contraire, avec un ordinateur quantique, les deux questions pourraient être incorporées dans une superposition d'états quantiques et, par là, être posées simultanément — et la machine elle-même entrerait alors dans une superposition de deux états, un par question. Ou, pour suivre l'interprétation des univers parallèles, la machine entrerait dans deux univers, et répondrait à chaque variante de la question dans des univers

différents. Quelle que soit l'interprétation, l'ordinateur quantique peut traiter les deux questions en même temps.

Pour comprendre et apprécier la puissance d'un ordinateur quantique, comparons ses performances à celles d'un ordinateur traditionnel sur un problème précis. Soit le problème qui consiste à trouver un nombre dont le carré et le cube épuisent tous les chiffres de 0 à 9 une fois et une fois seulement. Par exemple, si nous testons le nombre 19, alors $19^2 = 361$ et $19^3 = 6\,859$. Le nombre 19 ne convient pas puisque son carré et son cube n'incluent que les chiffres suivants : 1,3,5,6,6,8,9, c'est-à-dire que les chiffres 0,2,4,7 sont manquants et que le chiffre 6 est répété.

Pour résoudre ce problème avec un ordinateur traditionnel, l'opérateur aurait à adopter la démarche suivante. Entrer le nombre 1 et le faire tester par l'ordinateur. Une fois que celui-ci a fait les calculs nécessaires, il déclare si, oui ou non, le nombre 1 répond au critère. Ce n'est pas le cas de 1, donc l'opérateur entre 2 et effectue un nouveau test, et ainsi de suite, jusqu'à ce que le nombre approprié soit finalement trouvé. Il s'avère que la réponse est 69, puisque $69^2 = 4\,761$ et $69^3 = 328\,509$, ce qui contient effectivement la totalité des dix chiffres. En vérité, 69 est le seul nombre à satisfaire au critère.

Il est clair que cette procédure est longue, car l'ordinateur ne peut tester qu'un nombre à la fois. S'il faut une seconde pour un nombre, il mettra 69 secondes pour parvenir au résultat. L'ordinateur quantique, lui, donnerait la réponse en moins d'une seconde.

L'opérateur commence par représenter les nombres de façon appropriée aux capacités de l'ordinateur quantique. L'une des façons de représenter les nombres est de le faire en termes de particules en rotation. Beaucoup de particules fondamentales ont un mouvement de rotation propre ou *spin* qui peut se faire vers l'est (sens inverse des aiguilles d'une montre) ou vers l'ouest (sens des aiguilles d'une montre), un peu comme un ballon de basket tournant sur la pointe d'un doigt. Une particule tournant vers l'est représente le 1, tandis qu'une particule tournant vers l'ouest représente le 0. D'où il apparaît qu'une succession de particules en rotation est capable de représenter une succession de 1 et de 0, soit un nombre en écriture binaire. Par exemple, sept particules, tournant respectivement dans les sens est, est, ouest, est, ouest, ouest, ouest, représentent à elles toutes le nombre binaire 1101000, qui est l'équivalent du nombre 104 en écriture décimale. Selon leurs *spins*, une

combinaison de sept particules peut représenter tout nombre entre 0 et 127.

Avec un ordinateur traditionnel, l'opérateur entrerait une séquence de *spins* particulière, telle que ouest, ouest, ouest, ouest, ouest, ouest, est, qui représente 0000001, soit plus simplement le nombre décimal 1. L'opérateur attendrait alors que l'ordinateur teste le nombre pour voir s'il remplit les conditions mentionnées. Puis, l'opérateur entrerait 0000010, une séquence de *spins* représentative du nombre 2, et ainsi de suite. Comme précédemment, il faudrait entrer les nombres un par un, ce qui prend du temps. Avec un ordinateur quantique, l'opérateur a une manière différente, beaucoup plus rapide, d'entrer les nombres.

Parce que chaque particule est fondamentale, elle obéit aux lois quantiques. Tant qu'elle n'est pas soumise à une observation, elle peut entrer dans une superposition d'états, ce qui veut dire qu'elle tourne dans les deux directions en même temps, et qu'elle représente simultanément 0 ou 1. Autrement dit, nous pouvons imaginer la particule comme entrant dans deux univers : un dans lequel elle tourne vers l'est et représente 1, l'autre où elle tourne vers l'ouest et représente 0.

La superposition est obtenue de la façon suivante. Imaginons que nous soyons en mesure d'observer une des particules et que celle-ci tourne vers l'ouest. Pour changer le *spin*, on enverrait une impulsion d'énergie assez puissante pour la réorienter vers l'est. Ou alors, si nous envoyons une impulsion plus faible, certaines fois, au hasard, la particule changera de *spin*, et d'autres fois, elle n'en changera pas. Jusque-là, nous avons supposé la particule bien en vue tout le temps, et donc nous avons été capables de suivre son évolution. Au contraire, si la particule tournant vers l'ouest est placée dans une boîte hors de notre vue, et si nous envoyons une faible impulsion, il n'y a aucune façon de savoir si son *spin* tourne dans un sens ou dans l'autre. La particule entre dans une superposition d'états est et ouest, tout comme le chat entrait dans une superposition d'états mort et vivant. En prenant sept particules tournant vers l'ouest, en les mettant dans une boîte, et en donnant sept impulsions, on met les sept particules dans des états superposés.

Les sept particules en superposition représentent effectivement toutes les combinaisons possibles de *spins* vers l'est et vers l'ouest. Elles représentent simultanément 128 états différents ou 128 nombres différents. L'opérateur rentre les sept particules dans l'ordinateur, pendant qu'elles sont dans cet état superposé. L'ordinateur fait son calcul comme s'il testait 128 nombres simultanément et, en une seconde,

délivre le nombre 69 qui remplit le critère imposé. L'opérateur obtient 128 calculs pour le prix d'un.

L'ordinateur quantique défie le sens commun. Si l'on ignore les détails pour un moment, on peut le concevoir de deux façons différentes, selon l'interprétation que l'on préfère. Certains physiciens le voient comme une seule entité qui effectue 128 calculs simultanément. D'autres le voient comme 128 entités, chacune dans son univers distinct, et n'effectuant qu'un seul calcul. Le calcul quantique est une technologie du clair-obscur.

Les 1 et les 0 sur lesquels opèrent les ordinateurs traditionnels sont appelés des *bits*, abréviation anglaise de « chiffres binaires ». Puisque l'ordinateur quantique traite des 1 et des 0 qui sont dans une superposition quantique, on appelle ceux-ci des bits quantiques, ou *qubits* (que l'on prononce cubits). L'avantage est encore plus évident lorsqu'on considère des particules en plus grand nombre. Avec 250 particules en rotation, ou 250 qubits, on peut représenter un peu plus de 10^{75} combinaisons, c'est-à-dire plus que le nombre total de particules dans l'univers. S'il était possible de réaliser cet état de superposition avec 250 particules, alors un ordinateur quantique pourrait effectuer 10^{75} calculs simultanés, tout cela en l'espace d'une seconde.

L'exploitation des effets quantiques pourrait donner naissance à des ordinateurs d'une puissance inimaginable. Malheureusement, quand Deutsch eut la vision d'un tel ordinateur quantique au milieu des années 80, personne ne voyait comment y donner suite et créer une vraie machine solide et pratique. Les scientifiques ne savaient pas construire quoi que ce soit qui calcule avec des *spins* dans une superposition d'états. Un des grands obstacles était de maintenir une telle superposition pendant tout le calcul. Une superposition n'existe que tant qu'elle n'est pas observée, et une observation dans son sens le plus général peut provenir de toute interaction avec un objet quelconque extérieur à la superposition. Un atome égaré interagissant avec un des *spins* amènerait l'effondrement de la superposition dans un état unique, et l'échec du calcul sous sa forme quantique.

Un autre problème était que les scientifiques, ignorant comment programmer un ordinateur quantique, ne pouvaient non plus deviner de quels calculs il serait capable. Cependant, en 1994, Peter Shor, des Laboratoires Bell AT&T, dans le New-Jersey, réussit à définir un programme utilisable par un ordinateur quantique. La grande nouvelle

pour les cryptanalystes fut que son programme définissait une série d'étapes qui pouvaient être suivies pour factoriser un nombre géant, c'est-à-dire exactement ce qu'il fallait pour casser le code RSA. Quand Martin Gardner avait posé son énigme RSA dans le *Scientific American*, il avait fallu plusieurs mois à six cents ordinateurs pour factoriser un nombre de 129 chiffres. Le programme de Shor permettait, lui, de factoriser un nombre un million de fois plus grand en un millionième de ce temps. Malheureusement, Shor ne put faire la démonstration de son programme de factorisation parce qu'il n'existait encore rien qui ressemblât à un ordinateur quantique.

Puis, en 1996, arriva la découverte d'un autre programme très puissant par Lov Grover, lui aussi de Bell Labs. Son programme permet de scruter une liste à une vitesse incroyable, ce qui ne semble pas particulièrement intéressant, jusqu'à ce qu'on réalise que c'est juste ce qu'il faut pour casser le chiffre DES, c'est-à-dire chercher la bonne clef dans la liste de toutes les clefs possibles. Un ordinateur conventionnel capable de tester un million de clefs à la minute mettrait plus de mille ans, là où l'ordinateur quantique muni du programme de Grover trouverait la clef en moins de quatre minutes.

Ce n'est que pur accident si les deux premiers programmes destinés au calcul quantique étaient exactement ce que les cryptanalystes auraient placé au premier rang de leur liste de souhaits. Mais si les programmes de Shor et de Grover avaient déclenché un immense optimisme parmi les briseurs de codes, il s'ensuivit une grande frustration, car on n'avait aucune machine pour faire tourner ces programmes. On ne peut être surpris que le fin du fin en technologie du déchiffrement ait aiguisé les appétits d'organisations telles que l'Agence des projets de recherche avancée de la Défense américaine (DARPA) et le laboratoire national de Los Alamos, qui mettent tous leurs moyens à tenter de fabriquer des composants capables de manipuler des qubits, de la même façon que des puces de silicium manipulent les bits. Bien qu'une quantité d'avancées récentes aient relevé le moral des chercheurs, il faut bien admettre que la technologie est encore dans l'enfance. En 1998, Serge Haroche, de l'université Paris VI, dissipa l'idée que nous n'étions qu'à quelques années d'un véritable ordinateur quantique. Il déclara que cela revenait à construire laborieusement le premier étage d'un château de cartes, en prétendant que les 15 000 étages suivants ne seraient plus ensuite qu'une formalité.

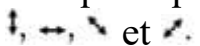
Seul le temps dira si et quand les problèmes de construction d'un ordinateur quantique pourront être surmontés. D'ici là, nous ne pouvons que spéculer sur l'impact qu'il aurait dans le monde de la cryptographie. Depuis les années 70, les concepteurs de codes ont pris nettement l'avantage sur les briseurs de codes, grâce à des chiffrements tels que DES ou RSA.

Ce qui semble certain, c'est que le développement d'un ordinateur quantique pleinement opérationnel mettrait en péril notre intimité ; il détruirait le commerce électronique et le concept de sécurité nationale. Il mettrait en danger la stabilité du monde. Le pays, quel qu'il soit, qui y parviendra le premier aura la capacité d'écouter les communications de ses citoyens, de lire les intentions de ses rivaux commerciaux, et de connaître les pensées de ses ennemis. L'ordinateur quantique présente donc un danger potentiel pour l'individu, pour le commerce international et pour la sécurité globale.

La cryptographie quantique

Pendant que les cryptanalystes attendent l'arrivée de l'ordinateur quantique, les cryptographes travaillent sur leur propre technologie miracle, un cryptosystème qui rétablirait la confidentialité face à la puissance terrifiante de ces nouvelles machines. Cette nouvelle forme de chiffrement est fondamentalement différente de tout ce que nous avons rencontré précédemment, car elle offre l'espoir d'une confidentialité totale. En d'autres termes, ce système serait sans défaut et garantirait une sécurité absolue pour l'éternité. De plus, ce système est fondé sur les concepts quantiques, ceux-là mêmes qui sont à la base de l'ordinateur quantique. Il en ressort que la mécanique quantique, qui sous-tend le principe capable de casser tous les chiffres existants, est aussi au cœur d'un nouveau chiffre inviolable appelé *cryptographie quantique*.

L'histoire de la cryptographie quantique remonte à une idée curieuse développée à la fin des années 60 par Stephen Wiesner, alors étudiant à l'université Columbia. La malchance de Wiesner fut de lancer une idée à ce point en avance sur son temps que personne ne la prit au sérieux. Il se rappelle encore la réaction de ses supérieurs : « Je n'ai eu aucun soutien de mon patron de thèse. Il n'y a jamais cru. J'ai parlé de cette idée à plusieurs autres personnes, mais elles prenaient une mine ahurie, et retournaient bien vite à leurs affaires. » Ce que Wiesner leur proposait, c'était le concept étrange de *monnaie quantique*, qui rendait impossible toute contrefaçon.

La monnaie quantique de Wiesner est profondément ancrée dans la physique des photons. Un photon qui se propage dans l'espace vibre comme on le voit sur la figure 73 (a), où quatre photons se déplacent dans le même sens, mais avec des directions de vibration — ou polarisations — différentes. Une ampoule électrique émet des photons de toute polarisation, c'est-à-dire que certains d'entre eux vibrent horizontalement, d'autres verticalement, et d'autres enfin suivant tous les angles possibles entre les deux. Pour simplifier, nous supposons que les photons n'ont que quatre polarisations possibles, que nous marquerons par :  et .

En plaçant un filtre Polaroid sur le trajet des photons, on peut garantir que le faisceau émergent de lumière ne contient que des photons

polarisés dans la même direction. Jusqu'à un certain point, on peut concevoir le filtre Polaroid comme une grille, et les photons comme des allumettes envoyées au hasard sur les barreaux. Seuls les photons ayant le bon angle de polarisation passeront à travers la grille sans altération, et les photons polarisés perpendiculairement seront bloqués.

Malheureusement, l'analogie avec les allumettes cesse d'être valable pour des photons polarisés en diagonale. Alors que de vraies allumettes ainsi orientées seraient bloquées par une grille verticale, ce n'est pas nécessairement le cas pour des photons. En effet, des photons polarisés en diagonale sont dans un état d'ambiguïté quantique lorsqu'ils sont confrontés à un filtre vertical. Le résultat est que la moitié des photons, au hasard, sont bloqués par le filtre, et que l'autre moitié passe, et que ceux qui sont passés ressortent avec une polarisation verticale ! La figure 73 (b) montre huit photons devant un filtre Polaroid vertical, et 73 (c) ne montre que les quatre ayant franchi le filtre avec succès. Tous ceux qui avaient une polarisation verticale sont passés ; ceux à polarisation horizontale sont restés bloqués. Enfin, la moitié des photons à polarisation diagonale sont passés.

C'est cette aptitude à arrêter certains photons qui explique le fonctionnement des lunettes de soleil à verres polarisants. En fait, vous pouvez démontrer l'effet des filtres Polaroid en faisant l'expérience avec des lunettes de soleil Polaroid. Enlevez d'abord un verre, et fermez cet œil de façon à regarder avec l'autre œil à travers le verre restant. Naturellement, le paysage paraît très sombre du fait que ce verre arrête beaucoup des photons qui autrement auraient atteint votre œil. À cet instant, tous les photons qui vous parviennent ont la même polarisation. Maintenant, regardez à travers les deux verres en plaçant le verre démonté devant l'autre, et en le faisant tourner lentement. Dans une certaine position, le second verre Polaroid n'aura aucun effet sur la lumière qui vous parvient, parce que son orientation est la même que celle du verre fixe. Si vous tournez alors le verre libre de 90° , tout va devenir complètement noir. Dans cette configuration, sa polarisation est à 90° de celle du verre fixé sur les lunettes, si bien que tout photon qui passe à travers le premier est arrêté par le second. Si, à partir de là, vous tournez le verre libre de 45° , vous obtenez une situation intermédiaire où les deux filtres sont partiellement désorientés, et la moitié des photons qui passent à travers le premier verre passera à travers le verre fixe.

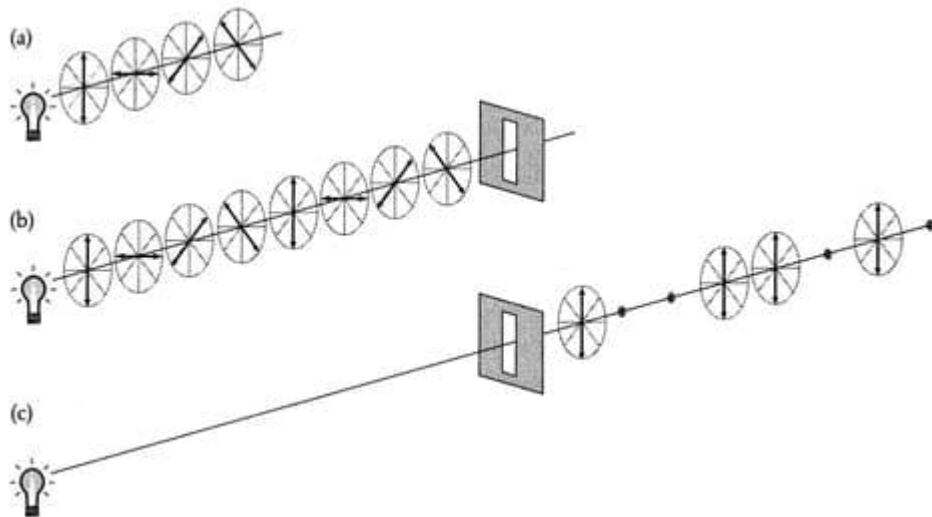


Fig. 73 (a) Bien que les photons puissent vibrer dans n'importe quelle direction de polarisation, nous ne considérons pour simplifier que quatre polarisations. (b) La lampe a émis huit photons, vibrant dans les quatre directions choisies, qui se dirigent vers le filtre Polaroid. (c) De l'autre côté du filtre, la moitié seulement des photons ont survécu. Les photons polarisés verticalement sont passés, mais pas les photons polarisés horizontalement. Des photons polarisés verticalement, un sur deux est passé et se retrouve à la sortie polarisé verticalement.

Wiesner projeta d'utiliser la polarisation des photons pour faire une monnaie infalsifiable. Son idée était que les billets de banque devraient contenir chacun 20 pièges ou *trappes à photons*, des petites puces capables de capturer et de retenir un photon. Il suggéra que les banques utilisent quatre films Polaroid orientés de quatre façons différentes (↕, ↔, ↘, ↗)↔, pour remplir les 20 trappes avec une séquence de 20 photons polarisés, différente sur chaque billet. Par exemple, la [figure 74](#) montre un billet avec la séquence de polarisations (↘, ↕, ↗, ↗, ↔, ↕, ↕, ↘, ↕, ↘, ↔, ↔, ↗, ↔, ↘, ↗, ↔, ↗, ↕, ↕). Les polarisations sont affichées ici sur la figure, mais en réalité elles doivent rester cachées. Chaque billet porte imprimé aussi le numéro de série traditionnel — B2801695E sur le dollar de l'illustration. La banque émettrice peut identifier chaque billet d'après la séquence de polarisations et le numéro de série, et doit garder en mémoire une table complète des correspondances entre les deux.

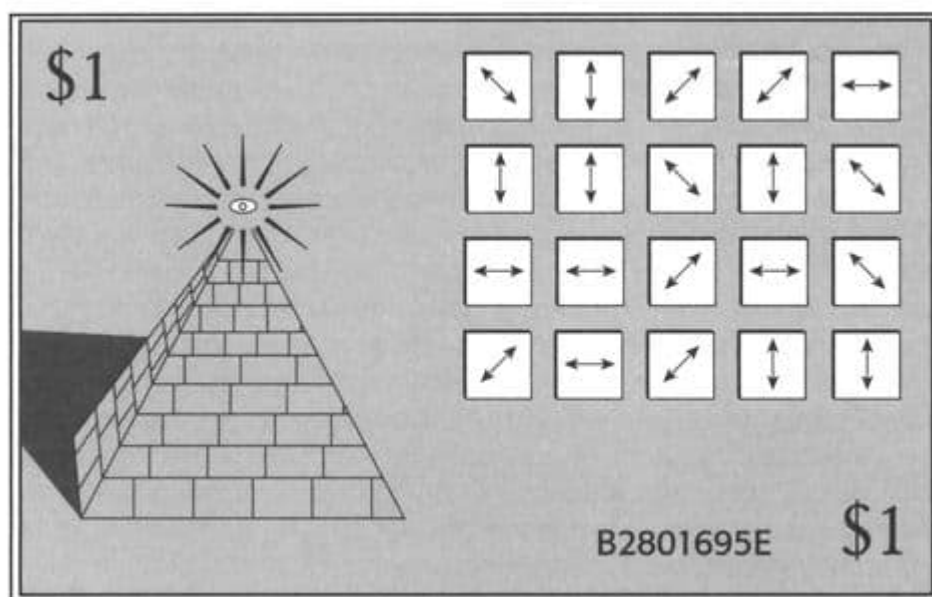


Fig. 74 La monnaie quantique de Stephen Wiesner. Chaque billet est unique par son numéro de série et par ses 20 trappes à photons, dont le contenu est un mystère. Ces trappes contiennent des polarisations de photons variées, dont la banque connaît la séquence, mais pas le contrefacteur éventuel.

Le faussaire est maintenant confronté à un sérieux problème : il ne peut pas se contenter de fabriquer un billet qui porte un numéro de série arbitraire et une séquence de polarisations quelconque dans les trappes, parce que, une telle association étant absente du fichier de la banque, le billet serait détecté comme un faux... Pour créer un faux, le contrefacteur doit partir d'un vrai billet, mesurer d'une façon quelconque les 20 polarisations, et faire alors un double en recopiant le numéro de série et en garnissant les trappes à photons de façon appropriée. Mais on sait qu'il est difficile de mesurer des polarisations, et si notre homme ne sait pas les mesurer avec justesse, il ne peut pas escompter fabriquer un faux billet vraisemblable.

Pour appréhender la difficulté de mesurer une polarisation de photon, il faut s'interroger sur le processus de mesure lui-même. Pour tenter de découvrir la polarisation du photon piégé dans une trappe particulière, on placera devant la trappe un filtre Polaroid orienté selon une direction, disons la verticale $\updownarrow$. Rappelons qu'un photon polarisé $\updownarrow$ passe avec certitude et qu'un photon polarisé $\leftrightarrow$ est arrêté avec certitude, mais qu'un photon polarisé diagonalement, que ce soit à 45° ($\nearrow$) ou à 135° ($\nwarrow$) a 50 % de chances de passer, 50 % de chances d'être arrêté.

Si un photon traverse le filtre, la seule conclusion certaine sera que sa polarisation n'était pas horizontale. Il pouvait avoir à l'origine une polarisation soit verticale, soit à 45° , soit à 135° . Si le photon ne franchit

pas le filtre, on peut seulement conclure que sa polarisation n'était pas verticale, mais cela laisse les trois options : $\rightarrow$, $\searrow$, ou $\swarrow$. Dans tous les cas, la réponse est ambiguë.

Cette situation d'impasse est inhérente à la physique des photons. C'est l'un des aspects du principe d'incertitude, un concept développé dans les années 20 par le physicien allemand Werner Heisenberg. Il a traduit cette proposition hautement technique en un énoncé très simple : « Par principe, nous ne *pouvons* connaître le présent dans tous ses détails. » Cela ne vient pas d'un équipement de mesure insuffisant, ou de mauvaise qualité. Heisenberg déclare simplement qu'il est impossible de mesurer simultanément avec précision tous les paramètres d'un objet. Dans notre exemple, nous ne pouvons connaître l'état exact des photons piégés dans les trappes. Le principe d'incertitude est une autre conséquence bizarre de la théorie quantique.

La monnaie quantique de Wiesner reposait sur le fait que la contrefaçon est un processus en deux temps : d'abord, lire le vrai billet avec une exactitude parfaite, et ensuite le reproduire. En incorporant des photons dans la composition du billet, Wiesner rendait impossible sa lecture, et par là élevait une barrière devant la contrefaçon.

Un faussaire naïf pourrait croire que, si lui est incapable de mesurer la polarisation des photons dans les trappes, la banque en est, elle aussi, incapable. Il pourrait essayer de fabriquer des faux en garnissant les trappes à photons avec une séquence arbitraire de polarisations. Cependant, la banque a les moyens de vérifier quels billets sont authentiques. Elle regarde le numéro de série, puis consulte son tableau de correspondance pour voir quelle devrait être la séquence de polarisations des photons piégés. Puisqu'elle connaît le résultat, elle peut orienter correctement le filtre Polaroid devant chaque trappe et faire une mesure. Si c'est un faux billet, les polarisations arbitraires choisies par le faussaire se traduiront par certains résultats incorrects, et la contrefaçon sera dévoilée. Par exemple, si la banque avait choisi un filtre t pour mesurer ce qui devrait être un photon polarisé t , et qu'elle trouve que le filtre bloque le photon, alors elle sait que le faussaire a rempli une trappe avec le mauvais photon. Si, au contraire, le billet se révèle vrai, alors la banque regarnit les pièges à lumière avec les photons appropriés, et remet le billet en circulation.

En résumé, le faussaire ne peut mesurer les polarisations dans un vrai billet parce qu'il ne connaît pas le contenu de chaque trappe, et donc ne sait pas comment orienter son filtre Polaroid pour faire le sondage

approprié. La banque est dans la situation contraire, puisque c'est elle qui a choisi les polarisations.

La monnaie quantique est une idée brillante, mais totalement irréaliste. Pour commencer, les ingénieurs n'ont pas encore mis au point la technologie du piégeage et de la conservation des photons polarisés. Même si cette technologie existait, elle serait bien trop coûteuse à mettre en œuvre. Il faudrait compter environ un million de dollars par billet. Mais bien qu'impraticable, la monnaie quantique appliquait la théorie quantique d'une façon imaginative. Aussi, malgré le manque d'encouragement de son directeur de thèse, Wiesner soumit-il un article à une revue scientifique ; il fut rejeté. Même chose avec trois autres revues. Selon Wiesner, ils ne comprenaient tout simplement pas la physique de la chose.

Il semble qu'une seule personne ait partagé l'enthousiasme de Wiesner pour le concept de monnaie quantique : son vieil ami Charles Bennett, étudiant en même temps que lui à Brandeis University. À l'âge de trois ans, Bennett voulait déjà être chercheur. En rentrant à la maison, sa mère vit un jour sur la cuisinière une casserole en train de bouillir qui contenait un étrange ragoût. Heureusement, elle ne se risqua pas à le goûter, car c'étaient les restes d'une tortue de mer que le jeune Bennett faisait bouillir dans l'alcali pour détacher la chair des os et obtenir ainsi un parfait squelette de tortue. Au lycée, son intérêt se déplaça de la biologie vers la biochimie, et, en entrant à Brandeis, il décida d'opter pour la chimie. En fin d'études, il se spécialisa dans la chimie physique, puis continua par de la recherche en physique, en mathématiques, en logique et enfin en informatique.



[Fig. 75](#) Charles Bennett.

Connaissant la vaste gamme d'intérêts de Bennett, Wiesner se dit qu'il pourrait apprécier la monnaie quantique, et lui communiqua une copie de son article refusé. Bennett fut fasciné par le concept et le considéra comme une des plus belles idées jamais formulées. Pendant une dizaine d'années, il relut de temps en temps le manuscrit, se demandant si l'on pouvait transformer une idée si ingénieuse en quelque chose d'utilisable. Au début des années 80, devenu chercheur permanent au laboratoire Thomas J. Watson d'IBM, il y pensait encore.

Il exposa un jour ce concept de monnaie quantique à Gilles Brassard, un informaticien de l'université de Montréal, avec qui il avait collaboré sur plusieurs sujets de recherche, et ils en discutèrent maintes fois les subtilités. Petit à petit, il leur apparut que l'idée de Wiesner pouvait avoir des retombées en cryptographie et ils se demandèrent ce qui arriverait si un message crypté était représenté et transmis par une suite de photons polarisés.

Bennett et Brassard commencèrent à concocter un système basé sur le principe suivant. Supposons qu'Alice souhaite envoyer à Bernard un message crypté composé d'une suite de 0 et de 1, qu'elle représente par des photons polarisés. Elle a deux façons possibles d'associer des polarisations à 1 et 0. Selon le premier schéma, appelé linéaire ou schéma-+, elle envoie $\uparrow$ pour représenter 1, et $\leftrightarrow$ pour représenter 0. Selon le deuxième schéma, appelé diagonal ou schéma-x, elle représente 1 par $\nearrow$, et 0 par $\searrow$. Pour envoyer un message binaire, elle passe de l'un à

l'autre schéma de façon imprévisible. Ainsi, le message 1101101001 serait transmis de la façon suivante :

Message	1	1	0	1	1	0	1	0	0	1
Schéma	+	x	+	x	x	x	+	+	x	x
Transmission	↑	↗	↔	↗	↗	↘	↑	↔	↘	↗

Alice transmet le premier 1 en utilisant le schéma-+, et le second 1 avec le schéma-x. C'est bien un 1 qui est transmis les deux fois, mais il est représenté par des polarisations différentes dans les deux cas.

Si Ève veut intercepter ce message, elle doit identifier les polarisations de chaque photon, tout comme le faussaire avait à identifier les polarisations dans les pièges à photons du billet de banque. Pour mesurer les polarisations, Ève doit décider comment orienter à chaque fois son filtre Polaroid. Mais elle ne peut savoir quel schéma Alice va utiliser pour chaque photon, donc son choix sera fait au hasard et va tomber faux une fois sur deux. En conséquence, elle ne peut avoir une connaissance complète du message transmis.

Une façon plus simple d'imaginer le dilemme d'Ève est de considérer qu'elle dispose de deux détecteurs Polaroid. Le détecteur-+ est capable de reconnaître sans ambiguïté des photons polarisés horizontalement et verticalement, mais n'est pas capable d'identifier des photons à polarisation diagonale, et les interprète faussement comme des photons polarisés verticalement et horizontalement. De son côté, le détecteur-x est capable de reconnaître sans ambiguïté des photons polarisés diagonalement, mais ne peut identifier des photons polarisés horizontalement et verticalement, et les interprète faussement comme des photons polarisés diagonalement. Par exemple, si elle utilise le détecteur-x pour identifier le premier photon, qui est ↑, elle va l'interpréter comme ↗ ou ↘. Malgré cette erreur, si elle l'interprète comme ↗, tout va bien, car ↗ aussi représente 1, mais si elle l'interprète comme ↘, c'est une faute car ↘ représente 0. Pour aggraver les choses, elle n'a qu'une seule chance de mesurer la polarisation du photon. Un photon est indivisible, si bien qu'elle ne peut le diviser en deux pour le faire passer par les deux détecteurs.

Ce système semble avoir plusieurs avantages : Ève ne peut être sûre de bien capter le message crypté, et elle n'a donc aucune chance de le déchiffrer. Cependant, il souffre d'un défaut sérieux et apparemment insurmontable, c'est que Bernard est dans la même position qu'Ève, dans

la mesure où il n'a aucun moyen de savoir quel schéma de polarisation Alice utilise pour chaque photon, et donc lui aussi va interpréter faussement le message. La solution est évidemment qu'Alice et Bernard conviennent du schéma de polarisation qu'ils utiliseront pour chaque photon. Dans l'exemple ci-dessus, Alice et Bernard auraient en commun une liste, ou clef, qui se lit + x + x x x + + x x. Mais nous voilà ramenés au vieux problème de la distribution des clefs : d'une façon ou d'une autre, Alice doit transmettre en sécurité à Bernard sa liste de schémas de polarisation.

Bien sûr, Alice pourrait crypter sa liste en utilisant un chiffre à clef publique tel que RSA, et la transmettre à Bernard. Cependant, imaginons une époque où RSA aurait été cassé, peut-être à la suite du développement de puissants ordinateurs quantiques. Le système de Bennett et Brassard se doit d'être autonome et de ne pas reposer sur le chiffre RSA. Pendant des mois, Bennett et Brassard essayèrent de contourner le problème de la distribution de la clef. En 1984, ils se trouvaient sur le quai de la gare de Croton-Harmon, non loin du laboratoire d'IBM Thomas J. Watson. Ils attendaient le train qui devait ramener Brassard à Montréal, et tuaient le temps à discuter des soucis et des ennuis d'Alice, Bernard et Ève. Si le train était arrivé quelques minutes plus tôt, ils se seraient dit au revoir, sans avoir avancé sur le chemin de la distribution de la clef. Au lieu de cela, dans une illumination soudaine, ils inventèrent la cryptographie quantique, la forme la plus parfaite de cryptographie jamais conçue.

La recette de la cryptographie quantique impose trois étapes préparatoires. Bien que ces étapes n'impliquent pas l'envoi d'un message crypté, elles permettent l'échange sans risque de la clef qui sera utilisée plus tard pour crypter un message.

1^{re} étape. Alice commence par transmettre une séquence aléatoire de 1 et de 0 (des bits), à partir d'un choix arbitraire de schémas de polarisations linéaires (horizontales ou verticales) et diagonales. La [figure 76](#) montre une telle séquence de photons se dirigeant vers Bernard.

2^e étape. Bernard doit identifier les polarisations de ces photons. N'ayant aucune idée du choix fait par Alice pour chacun d'eux, il alterne au hasard entre son détecteur-+ et son détecteur-x. Tantôt, c'est le bon détecteur, tantôt c'est le mauvais. Si Bernard utilise le mauvais détecteur,

il va interpréter faussement le photon d'Alice. Le [tableau 27](#) couvre toutes les possibilités. Par exemple, à la ligne supérieure, Alice utilise le schéma linéaire pour envoyer 1, et donc transmet $\uparrow$; Bernard, utilisant le bon détecteur, détecte $\uparrow$ et note 1, qui est correct. À la ligne suivante, Alice fait la même chose, mais Bernard utilise le mauvais détecteur. Il peut alors détecter soit $\nearrow$, soit $\searrow$, ce qui l'amène à écrire soit 1 (résultat correct), soit 0 (résultat faux).

3^e étape. À ce point, Alice a envoyé une suite de 1 et de 0, et Bernard a détecté les uns correctement, les autres incorrectement. Pour clarifier les choses, Alice téléphone à Bernard sur une ligne ouverte ordinaire, et lui dit quel schéma de polarisation elle a employé pour chaque photon, mais pas comment elle a polarisé chaque photon. Ainsi, elle pourrait annoncer que le premier photon a été envoyé en utilisant le filtre linéaire, mais elle ne révélerait pas si elle a envoyé $\uparrow$ ou $\leftrightarrow$. Bernard signale alors à Alice à quelles occasions il a fait le bon choix de polarisation. Dans ces cas-là, il a, sans doute possible, déterminé la polarisation correcte et noté correctement 1 ou 0. Finalement, Alice et Bernard décident d'oublier tous les photons pour lesquels Bernard avait fait le mauvais choix, et se restreignent à ceux pour lesquels il avait fait le bon choix pour le détecteur. En pratique, ils ont ainsi généré une nouvelle séquence de bits, constituée exclusivement des mesures correctes de Bernard. Cette étape est tout entière illustrée dans le tableau situé au bas de la [figure 76](#).

Ces trois étapes ont permis à Bernard et à Alice de convenir d'une série de chiffres binaires, tels que la séquence 11001001 montrée sur la [figure 76](#). La propriété fondamentale de cette séquence est d'être arbitraire, parce qu'elle provient de la séquence initiale d'Alice, qui elle-même était arbitraire. De plus, les occasions où Bernard utilise le bon détecteur sont aléatoires. La séquence convenue n'est donc pas un message, mais peut être utilisée comme une clef. La véritable procédure de chiffrement sûr peut enfin commencer.

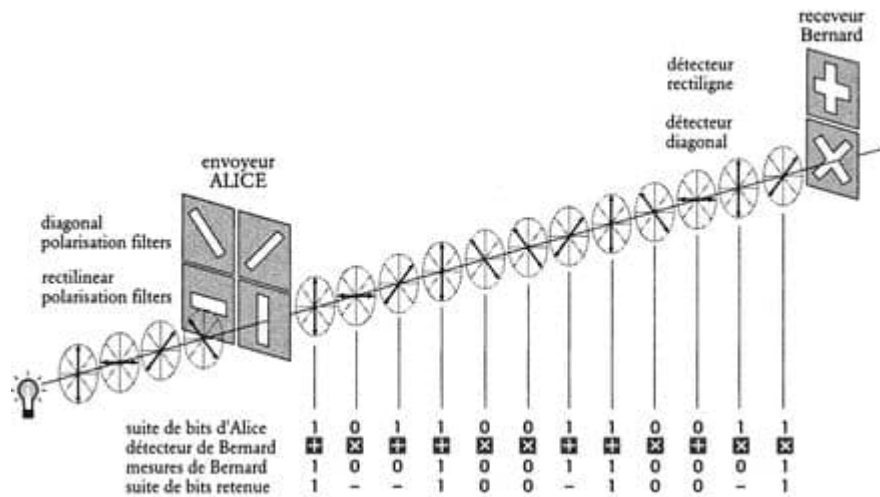


Fig. 76 Alice transmet une suite de 1 ou de 0 à Bernard. Chaque 1 et chaque 0 est représenté par un photon polarisé, selon un schéma de polarisation linéaire (horizontal/vertical) ou diagonal.

Bernard absorbe chaque photon en utilisant son détecteur linéaire ou son détecteur diagonal. Il choisit le bon détecteur pour le photon le plus à gauche, et l'interprète correctement comme un 1. Mais il choisit le mauvais détecteur pour le photon suivant. Par accident, il l'interprète comme un 0, ce qui est juste, mais ce bit est néanmoins écarté plus tard, parce que Bernard n'est pas assuré de l'avoir déterminé correctement.

Cette séquence aléatoire convenue peut servir de clef dans un chiffre jetable. Au chapitre 3, on a décrit comment une suite aléatoire de lettres ou de nombres, la *clef-une fois*, pouvait engendrer un chiffre absolument incassable. Le seul problème avec la clef-une fois était la difficulté de diffuser en toute sécurité la suite aléatoire, mais le tour d'adresse de Bennett et Brassard résoud le problème. Alice et Bernard sont convenus d'une clef unique, et les lois de la mécanique quantique interdisent à Ève de l'intercepter efficacement. Il est temps maintenant de se mettre dans la position d'Ève et de voir pourquoi elle est incapable d'intercepter la clef.

Schéma d'Alice	Chiffre binaire d'Alice	Envoi d'Alice	Détecteur de Bernard	Détecteur est-il valide	Détection par Bernard	Chiffre binaire de Bernard	Ce chiffre est-il correct
+	1	↑	+	Oui	↑	1	Oui
			x	Non	↗ ↘	1 0	Oui Non
	0	↔	+	Oui	↔	0	Oui
			x	Non	↗ ↘	1 0	Non Oui
x	1	↗	+	Non	↑ ↔	1 0	Oui Non
			x	Oui	↗	1	Oui
	0	↘	+	Non	↑ ↔	1 0	Non Oui
			x	Oui	↘	0	Oui

Tableau 27 : Options de la 2^e étape de l'échange de photons entre Alice et Bernard. Polarisation linéaire (+). Polarisation diagonale (x)

Tandis qu'Alice transmet les photons polarisés, Ève essaie de les identifier, mais elle ne sait pas si elle doit utiliser le détecteur- + ou le détecteur-x. Une fois sur deux en moyenne, elle fera le mauvais choix. C'est exactement la situation de Bernard qui, lui aussi, fait le mauvais choix une fois sur deux. Cependant, après la transmission, Alice dit à Bernard quelle orientation de détecteur il aurait dû utiliser pour chaque photon et ils tombent d'accord pour ne garder que les photons qui ont été identifiés alors que le détecteur avait la bonne orientation. Ceci n'aide pas pour Ève qui, pour la moitié de ces photons, aura utilisé la mauvaise orientation, et ainsi aura interprété faussement certains des photons qui constituent la clef finale.

On peut penser la cryptographie quantique en termes d'un paquet de cartes plutôt que de photons polarisés. Toute carte à jouer a une valeur et une couleur — valet de cœur ou six de trèfle — et nous voyons habituellement la valeur et la couleur en même temps. Supposons que nous ne puissions voir que la valeur ou la couleur, mais pas les deux. Alice extrait une carte du paquet, et doit décider quoi choisir, de la valeur ou de la couleur. Supposons qu'elle choisisse la couleur, qui est pique, ce

qu'elle note. Il se trouve que la carte est le quatre de pique, mais Alice sait seulement que c'est pique. Elle transmet alors la carte sur le canal pneumatique. A ce moment, Ève essaie d'identifier la carte, mais choisit de mesurer sa valeur, qui est quatre. Quand la carte arrive à Bernard, celui-ci décide d'observer sa couleur, qui est toujours pique, et il la note. Plus tard, Alice appelle Bernard et lui demande s'il a vu la couleur, ce qu'il a fait, si bien qu'Alice et Bernard possèdent une chose en commun — tous les deux avaient le mot pique écrit sur leur carnet. Au contraire, Ève a écrit quatre sur son carnet de notes, ce qui ne lui sert à rien.

Ensuite, Alice tire une autre carte — le roi de carreau — mais, là encore, elle ne peut en déterminer qu'une seule propriété. Cette fois, elle décide que ce sera la valeur : roi. Quand la carte atteint Bernard, il regarde la couleur, qui est carreau. Après cela, Alice appelle Bernard et lui demande s'il a mesuré la valeur de la carte, mais il doit admettre qu'il a fait un mauvais pari, et qu'il a mesuré la couleur. Cela ne gêne pas Alice et Bernard, car ils peuvent ignorer cette carte complètement, et recommencer avec une autre carte extraite au hasard du paquet. Dans ce dernier cas, Ève avait deviné juste et mesuré la même chose qu'Alice — la valeur roi —, mais la carte a été éliminée, parce que Bernard ne l'avait pas mesurée correctement. Ainsi Bernard n'a pas à s'inquiéter de ses fautes, puisqu'Alice et lui peuvent les ignorer, alors qu'Ève est prisonnière de ses fautes. En s'envoyant plusieurs cartes, Alice et Bernard peuvent s'entendre sur une séquence de valeurs et de couleurs qui vont servir de point de départ à une sorte de clef.

La cryptographie quantique permet à Alice et Bernard de convenir d'une clef, qu'Eve ne peut intercepter sans commettre d'erreurs. Mais elle offre un avantage supplémentaire : elle donne à Alice et Bernard le moyen de découvrir si Ève est en train de les espionner. La présence d'Ève sur la ligne se remarque parce que, chaque fois qu'elle observe un photon, elle risque de l'altérer, et ces altérations sont perceptibles pour Alice et Bernard.

Imaginons qu'Alice envoie $\nearrow$, et que Ève le mesure avec le mauvais détecteur, le détecteur-+. En fait, ce détecteur force le photon $\nearrow$ à sortir soit comme $\uparrow$, soit comme $\leftrightarrow$, car c'est le seul moyen de sortir du détecteur d'Ève. Si Bernard mesure le photon transformé avec son détecteur-x, il peut détecter soit $\nearrow$, qui est le photon envoyé par Alice, soit $\nwarrow$, ce qui serait une mesure fausse. C'est un problème pour Alice et Bernard, parce que, Alice ayant envoyé un photon polarisé diagonalement et Bernard ayant utilisé le bon détecteur, ce dernier aurait

cependant produit un résultat faux. En bref, si Ève a choisi le mauvais détecteur, elle va *tordre* certaines polarisations de photons, et cela va mener Bernard à des erreurs, même lorsqu'il utilise le bon détecteur. Ces erreurs peuvent être vérifiées par Alice et Bernard en faisant un rapide test d'erreurs.

On procède à ce test d'erreurs après les trois étapes préliminaires, au terme desquelles Alice et Bernard devraient avoir une suite identique de 1 et de 0. Imaginons qu'ils aient établi une séquence de 1 075 chiffres binaires. Une façon pour Alice et Bernard de vérifier si leurs séquences respectives sont en accord serait pour Alice d'appeler Bernard et de lui lire sa séquence complète. Mais si Eve espionne, elle est en mesure d'intercepter la clef tout entière. Vérifier la clef entière n'est donc pas raisonnable, et en plus c'est inutile. À la place, Alice va prendre seulement 75 de ses bits au hasard et ne tester que ceux-là. Si Bernard est d'accord avec ces 75 bits, il est hautement improbable qu'Ève ait espionné pendant la première transmission des photons. La probabilité de la présence d'Ève sur la ligne sans affecter les résultats de Bernard est inférieure à un milliardième. Puisque ces 75 bits ont été ouvertement discutés par Alice et Bernard, ils sont écartés et la clef — est réduite de 1 075 à 1 000 chiffres binaires. Si, au contraire, Alice et Bernard voient une différence entre leurs 75 bits, ils sauront qu'Ève était sur la ligne. Ils devront jeter la totalité du chiffre, passer sur une autre ligne et tout recommencer.

En résumé, la cryptographie quantique est un système qui assure la sécurité d'un message en rendant difficile pour Ève de lire avec exactitude une communication entre Alice et Bernard. De plus, si Ève essaie d'écouter, Alice et Bernard peuvent détecter sa présence. Donc, la cryptographie quantique permet à Alice et Bernard d'échanger et de s'entendre sur un chiffre jetable en parfaite confidentialité, et de s'en servir ensuite de clef pour crypter un message. La procédure se compose donc de cinq étapes :

- (1) Alice envoie à Bernard une série de photons, et Bernard les détecte.

- (2) Alice indique à Bernard à quelles occasions il a adopté la bonne orientation, sans lui dire ce qu'aurait dû être le résultat, si bien que la conversation peut être captée sans dommage.

(3) Alice et Bernard écartent les mesures que Bernard a faites incorrectement, et ne retiennent, pour définir une clef jetable, que les bonnes mesures.

(4) Alice et Bernard testent l'intégrité de leurs échanges en vérifiant quelques-uns des bits.

(5) Si la vérification donne des résultats satisfaisants, ils peuvent utiliser la clef pour crypter un message ; si la vérification révèle des erreurs, ils savent que les photons ont été captés par Ève, et ils doivent tout recommencer.

Quatorze ans après que l'article de Wiesner sur la monnaie quantique avait été refusé par les journaux scientifiques, voilà qu'il inspirait un système de communication d'une sécurité absolue. Aujourd'hui installé en Israël, Wiesner est soulagé que son œuvre soit reconnue : « En revenant en arrière, je me demande si j'en aurais fait grand-chose. Les gens m'ont accusé d'être un lâcheur, pour n'avoir pas insisté davantage pour publier mon idée — ils ont un peu raison —, mais j'étais encore étudiant à l'époque et je manquais de confiance en moi. Et d'ailleurs, personne ne semblait intéressé par la monnaie quantique. »

Les cryptographes accueillirent la cryptographie quantique de Bennett et Brassard avec enthousiasme, même si les expérimentateurs objectaient que l'idée, bonne en théorie, serait expérimentalement un échec. Ils pensaient que la difficulté de manipuler des photons individuels empêcherait de monter *un* tel système. Bennett et Brassard, eux, étaient convaincus que la cryptographie quantique pouvait être mise en œuvre. Ils avaient une telle foi en leur système qu'ils ne se souciaient même pas de tenter l'expérience. Comme Bennett le dit une fois : « Cela ne sert à rien d'aller au Pôle Nord si vous savez qu'il est là. »

Cependant, le scepticisme croissant incita finalement Bennett à démontrer que le système pouvait effectivement marcher. En 1988, il commença à rassembler les éléments nécessaires à un montage de cryptographie quantique, et engagea un jeune chercheur, John Smolin, pour l'y aider. Après une année d'efforts, ils étaient prêts à tenter d'envoyer le premier message protégé par la cryptographie quantique. Tard dans la soirée, ils se retirèrent dans le laboratoire protégé de toute lumière, dans un environnement entièrement noir, à l'abri de tout photon indésirable qui viendrait interférer avec l'expérience. Après un dîner consistant, ils étaient prêts pour une longue nuit de travail autour de

l'appareil. Ils s'étaient donné pour but d'envoyer des photons polarisés dans la pièce, et de les analyser avec un polariseur-+ et un polariseur-x. Un ordinateur baptisé Alice contrôlait la transmission des photons, et un autre, baptisé Bernard, décidait quel détecteur devait être utilisé pour analyser chaque photon.

Après des heures de réglage, vers 3 heures du matin, Bennett fut témoin du tout premier échange de cryptographie quantique. Alice et Bernard s'arrangeaient pour envoyer et recevoir des photons, ils discutaient les schémas de polarisation utilisés par Alice, ils éliminaient les photons que Bernard avait détectés avec le mauvais analyseur et ils s'entendaient sur un chiffre jetable constitué des autres photons. « Il n'y avait aucun doute que cela devait marcher, rappelle Bennett. Le seul échec pouvait provenir de mains trop malhabiles pour monter l'expérience. » L'expérience de Bennett avait démontré que deux ordinateurs, Alice et Bernard, pouvaient communiquer dans une confidentialité totale. C'était un résultat historique, bien que les deux ordinateurs ne fussent séparés que de trente centimètres.

Depuis l'expérience de Bennett, le défi a été de mettre au point un système de cryptographie quantique capable de transmettre sur des distances significatives. Ce n'est pas une mince affaire, car les photons voyagent mal. Si Alice transmet un photon polarisé par voie aérienne, les molécules d'air vont interagir, changer la polarisation, ce qui n'est pas admissible. La fibre optique est un meilleur milieu de transmission. En 1995, des chercheurs de l'université de Genève ont réussi à monter un système de cryptographie quantique qui fonctionne sur une fibre optique qui rejoint Genève à Nyon, sur une longueur de 23 km.

Plus récemment, des scientifiques du Laboratoire national de Los Alamos (Nouveau-Mexique) ont repris les expériences dans l'air. Le but est de créer un système qui pourrait fonctionner par voie de satellites. Si on pouvait y parvenir, ce serait la sécurité globale absolue. Jusqu'à présent, le groupe de Los Alamos n'a réussi à transmettre dans l'air que sur une distance de 1 km.

Les experts de la sécurité se demandent maintenant combien de temps il faudra pour que la cryptographie quantique entre dans le domaine de la technologie. Pour l'instant, la cryptographie quantique n'offre pas d'avantage particulier, parce que le chiffre RSA fournit déjà un procédé de cryptage incassable en pratique. Cependant, si les ordinateurs

quantiques deviennent une réalité, alors le RSA et les autres chiffres modernes seront obsolètes, et la cryptographie quantique s'imposera comme une nécessité. La question réellement importante est de savoir si la cryptographie quantique arrivera à temps pour nous sauver de l'inquisition des ordinateurs quantiques, ou s'il faudra traverser une période sans confidentialité, entre le développement de l'ordinateur quantique et l'avènement de la cryptographie quantique. Pour l'instant, la cryptographie est en avance. L'expérience suisse avec les fibres optiques démontre qu'il serait possible d'établir une ligne cryptographique interbanques parfaitement sûre à l'intérieur d'une même ville. À dire vrai, il serait actuellement possible de construire un tel lien entre la Maison-Blanche et le Pentagone. Peut-être y en a-t-il déjà un ?

La cryptographie quantique marquerait la victoire définitive des concepteurs de codes sur les casseurs de codes. La cryptographie quantique est un système de cryptage inattaquable. Cela peut sembler une affirmation exagérée, au vu des déclarations semblables qui ont été faites par le passé. À des moments différents des deux derniers millénaires, les codeurs ont cru que le chiffre monoalphabétique, puis le polyalphabétique, puis les machines à chiffrer telles qu'Enigma étaient incassables. Dans chacun de ces cas, les cryptographes ont été démentis, parce que leurs certitudes étaient basées sur le fait que la complexité des chiffres surpasserait l'intelligence et les moyens techniques des cryptanalystes à un moment de l'histoire. Après coup, nous voyons qu'il était inévitable que les cryptanalystes trouvent le moyen de briser chacun des codes, ou développent une technologie qui le fasse à leur place.

Cependant, la sécurité qu'offre la cryptographie quantique est d'une nature différente de toutes les autres. La cryptographie quantique n'est pas seulement incassable en pratique, elle est incassable dans l'absolu. La théorie quantique dit qu'il est impossible pour Ève de lire avec exactitude la clef à usage unique établie entre Alice et Bernard. Ève ne peut même pas tenter d'intercepter cette clef sans qu'Alice et Bernard s'aperçoivent d'une tentative d'espionnage. En réalité, si un message protégé par la cryptographie quantique devait jamais être déchiffré, cela voudrait dire que la théorie quantique est défectueuse, ce qui aurait des implications dévastatrices pour les physiciens ; ils seraient forcés de reconsidérer leur appréhension du monde jusqu'au niveau le plus fondamental.

Si des systèmes de cryptographie quantique peuvent être mis au point pour opérer sur de longues distances, l'évolution des codes secrets

cessera. La quête de la confidentialité sera parvenue à son terme. La technologie pourra garantir des communications sûres aux gouvernements, aux militaires, aux hommes d'affaires, ainsi qu'au public. La question est de savoir si on autorisera ou non l'usage de cette technologie. Comment les gouvernements régleront-ils la cryptographie quantique, de façon à enrichir l'âge de l'information sans protéger les criminels ?

Le Concours du Chiffre

Le concours du chiffre vous offre l'opportunité de tester vos talents de décrypteur. Il comporte dix étapes. La première est un chiffrement monoalphabétique assez simple ; les suivantes vous entraîneront à travers l'histoire de la cryptographie. La deuxième étape comporte un texte crypté selon l'un des chiffres les plus anciens, et la dixième applique l'une des formes les plus modernes de chiffrement. En principe, chaque étape sera plus difficile que la précédente. A la publication de ce livre un prix de 10 000 livres anglaises était offert au premier concurrent qui viendrait à bout de cette épreuve.

La solution finit par être découverte le 7 octobre 2000, après un an et un mois de recherches par les déchiffreurs de codes du monde entier, tant amateurs que professionnels.

Le Concours reste partie intégrante de ce livre. Même s'il n'y a plus de prix à remporter, j'encourage fortement les lecteurs à déchiffrer les messages. Les dix étapes étaient conçues pour croître en difficulté, bien que beaucoup de déchiffreurs aient trouvé l'étape 3 plus difficile que l'étape 4. Les chiffres utilisés dans chaque étape sont différents et progressent dans l'histoire ; les premiers chiffres sont anciens, faciles à décrypter, tandis que les dernières étapes utilisent des chiffrements modernes et requièrent beaucoup plus d'efforts. En résumé, les étapes de 1 à 4 sont du niveau d'un amateur, celles de 5 à 8 d'un enthousiaste, et les 9 et 10 sollicitent une grande expérience dans la matière.

Si vous voulez en savoir plus sur les coulisses du Concours du Chiffre, vous pouvez visiter mon site web (www.simonsingh.com), qui présente de nombreuses informations et un lien avec un compte-rendu rédigé par les gagnants du Concours, Fredrik Almgren, Gunnar Andersson, Torbjorn Granlund, Lars Ivansson et Staffan Ulfberg. Le compte-rendu est excellent, mais soyez avertis qu'il contient des solutions — tout comme certains éléments du site — que vous n'aurez peut-être pas envie de voir dévoilées.

Le propos essentiel du Concours du Chiffre était de stimuler les lecteurs, de les intéresser à la cryptographie et au déchiffrement. Le fait que des milliers de personnes aient relevé le défi est profondément satisfaisant. Le Concours est officiellement terminé, mais j'espère qu'il continuera à susciter de l'intérêt parmi les nouveaux lecteurs qui voudront tester leurs talents de déchiffreurs.

Bonne chance,

Simon Singh.

Étape 1 : Simple chiffre de substitution monoalphabétique

XT AXJ BTRJMTJ, MQQMUVVXTJ GXR NCBWJR N'UTX LMBT
N'PCLLX XJ BGR XAVBDBVXTJ, XT IMAX NU AMTNXGMFVX, RUV
GX QGMJVX NU LUV NU QMGMBR VCEMG. GX VCB DBJ AXJJX
QMVJBX NX LMBT KUB XAVBDMBJ. MGCVR GX VCB APMTWXM NX
ACUGXUV, RXR QXTRXXR G'XIIVMEXVXTJ, GXR SCBTJUVXR NX
RXR VXBTR RX NXGBXVXTJ XJ RXR WXT'CUZ RX PXUVJXVXTJ
G'UT G'MUJVX. GX VCB AVBM MDXA ICVAX QCUV IMBVX DXTBV
GXR LMWBABXTR, GXR APMGNXXTR XJ GXR MRJVCGCWUXR. GX
VCB QVBJ GM QMVCGX XJ NBJ MUZ RMWXR NX FMFEGCTX : JCUJ
PCLLX KUB GBVM AXJJX XAVBJUVX XJ LX IXVM ACTTMBJVX RCT
XZQGBAMJBCT VXDJBVM GM QCUVQVX, LXJJVM GX ACGGBXV
N'CV M RCT ACU XJ, ACLLX JVCBRBXLX NMTR GX VCEMULX, BG
ACLLMTNXVM. MGCVR DBTVXTJ JCUR GXR RMWXR NU VCB,
LMBR BGR TX QUVXTJ QMR GBVX G'XAVBJUVX XJ IMBVX
ACTTMBJVX MU VCB G'XZQGBAMJBCT. GX VCB FMGJPMRMV IUJ
NCTA JVXR XIIVMEX, GM ACUGXUV NX RCT DBRMWX APMTWXM
XJ RXR WVMTNR IUVXTJ FCUGDXVRXR. GM VXBTX, XT VMBRCT
NXR QMVCGX NU VCB XJ NX RXR WVMTNR, DBTJ NMTR GM
RMGGX NU IXRJB. GM VXBTX QVBJ GM QMVCGX XJ NBJ : KUX GX
VCB DBDX XJXVTXGGXLXTJ ! KUX JXR QXTRXXR TX
J'XIIVMEXTJ QMR XJ KUX JCT DBRMWX TX APMTWX QMR NX
ACUGXUV. BG E M NMTR JCT VCEMULX UT PCLLX KUB QCRRXNX
XT GUB G'XRQVBJ NXR NBXUZ RMBTJR. QXTNMTJ GXR SCUVR NX
JCT QXVX, UTX GULBXVX, UT NBRAXVTXLXTJ XJ UTX RMWXR
ACLLX GM RMWXR NXR NBXUZ, IUVXTJ JVCUDXR XT GUB, XJ
GX VCB TMFUAPCNCTCRCV JCT QXVX G'XJMFGBJ ACLLX APXI
NXR NXDBTR, NXR LMWBABXTR, NXR APMGNXXTR XJ NXR
MRJVCGCWUXR. QMVAX KU'UT XRQVBJ RUQXVBXUV, UTX
BTJXGGBWXTAX, UT NBRAXVTXLXTJ, G'XZQGBAMJBCT NXR
RCTWXR, G'BTJXVQVXJMBCT NXR XT'BWLXR, GM RCGUJBCT NXR
QVCFGXLXR, IUVXTJ JVCUDXR XT GUB, XT NMTBXG, M KUB GX
VCB MDMBJ NCTTX GX TCL NX FXGJRPMMRMV, KUX NMTBXG
RCBJ NCTA MQQXGX XJ BG IXVM ACTTMBJVX G'XZQBAMJBCT.
GX QVXLBXV LCJ RXAVXJ XRJ CJPXGGC.

Étape 2 : Chiffre décalé de César

MHILY LZA ZBHL XBPZXBL MUYABUHL HWWPBZ JSHBKPZ JHLJBZ
KPJABT HYJHUBT LZA ULBAYVU

Étape 3 : Chiffre monoalphabétique avec homophones

IXDVMUFXLFEEDFXSOQXYQVXSQTUIXWF*FMXYQVFJ*FXEFQUQXJFPTUFX
MX*ISSFLQTUQXMXRPQEUMXUMTUIXYFSSFI*MXKFJF*FMXLQXTIEUVFX
EQTEFXSOQXLQ*XVFWMTQTUQXTITXKIJ*FMUQXTQJMVX*QEYQVFQTHMX
LFVQUVIXM*XEI*XLQ*XWITLIXEQTHGXJQTUQXSITEFLQVQUX*GXKIE
UVGXEQWQTHGXDGFXTITXDIEUQXGXKFKQVXSIXQXAVPUFXWGXYQVXEQ
JPFVXKFVUPUQXQXSGTIESQTHGX*FXWFQFXSIWYGJTFXDQSFIXEFXGJP
UFXSITXRPQEUGXIVGHFITXYFSSFI*CXC*XSCWWFTIXSOQXCXYQTCXYI
ESFCX*FXCKVQFXVFUQTPUFQXKI*UCXTIEUVCXYIYYCXTQ*XWCUUFTI
XLQFXVQWFXDCSQWWIXC*FXC*XDI**QXKI*IXEQWYVQXCSRPFUECTLIX
LC*X*CUIXWCTSFTIXUPUUQX*QXEUQ**QXJFCXLQX*C*UVIXYI*IXKQL
QCX*CXTIUUQXQX*XTIEUVIXUCTUIXACEEIXSOQXTITXEPVJQCXDPIVX
LQ*XWCVFTXEPI*IXSFTRPQXKI*UQXVCSSQEIXQXUCTUIXSCEEIX*IX*
PWQXQVZXLFXEIIUUXLZX*ZX*PTZXYIFXSOQXTUVZUFQXQVZKZXWXTQX*Z
*UIXYZEEIRPZTLIXTZYYZVKQXPTZXWITUZJTZXAVPTZXYQVX*ZXLFEU
ZTHZXQXYZVKQWFXZ*UZXUZTUIXRPZTUIXKQLPUZXTITXZKQZXZ*SPTZ
XTIFXSFXZ**QJVNWWIXQXUIEUIXUIVTIXFTXYFNTUIXSOQXLQX*NXTI
KNXUQVVNXPTXUPVAIXTNSRPQXQXYQVSIEEQXLQ*X*QJTIXF*XYVFWIX
SNTUIXUVQXKI*UQXF*XDQXJFVBVXSITXUPUUQX*BSRPQXBX*BXRFBVU
BX*QKBVX*BXYIYBXFTEPEIXQX*BXYVIVBQVQXFTXJFPXSIWB*UVP
FXYFBSRPQFTDFTXSOQX*XWBVXDPXEIYVBXTIFXVFSOFPEIXX*BXYBVI
*BXFTXSILFSQXQXQRPBUIV

Étape 4 : Chiffre de Vigenère

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJB
 GWRLFNF GHU DWUUMB SVLP SN CMUEKQCTESWR
 EEKOYSSIWCTUAXYOTAPXP LWPNTCGOJBGFQ
 HTDWXIZAYGFFNSXCSEYNCTSSPNTUJNYTGG
 WZGRWUUNEJU UQEAPYMEKQHUIDUXFPGUYTS
 MTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFB
 DJQCUSWVBPNLGOYLSKMTEFVJJTWWMFMWPN
 MEMTMHRSPXFSSKFSTNUOCZGMDOE OYEEKC
 PJRGPMURSKHFRSEIUEVGOYCW XIZAYGOSAA
 NYDOEOYJLWUNHAMEBFELXYVLWNOJNSIOFR
 WUCCE SWKVIDGMUCGOCR UWGNMAAFFVNSIUD
 EKQHCEUCPFCMPVSUDGAVEMNYMAMVLFMAOY
 FNTQCUAFVFJNXKLNEIWCWODCCULWRIFTWG
 MUSWOVMATNYBUHTCOCWFYTNMGYTQMKBBNL
 GFBTWOJFTWGNTEJKN EEDCLDHWTVB UVGFBI
 JGY YIDGMVRDGMPLSWGJLAGOE EKJOFEKNYN
 OLRIVRWVUHEIWUURWGMUTJCDBNKGMBIDGM
 E EYGUOTDGGQE UJYOTVGGBRUJYS

Étape 5 :

109	182	6	11	88	214	74	77	153	177	109	195	76	37	188	
166	188	73	109	158	15	208	42	5	217	78	209	147	9	81	
80	169	109	22	96	169	3	29	214	215	9	198	77	112	8	30
117	124	86	96	73	177	50	161								

Étape 6 :

OCOYFOLBVNPIASAKOPVYGESKOV MUFGUWMLNOOEDRNCFOR SOCVMTUUTY
 ERPFOLBVNPIASAKOPVIVKYEOCNKOCCARICVVLTSOCOYTRFDVCVOOUEG
 KPVOOYVKTHZSCVMBTWTRHPNKLRCUEGMSLNLVZSCANSCKOPORMZCKIZU
 SLCCVFDLVORTHZSCLEGUXMIFOLBIMVIVKIUAYVUUFVWVCCBOVOVPFRH
 CACSFGEOLCKMOCGEUMOHUEBRLXRHEMHPBMPLTVOEDRNCFORSGISTHOG
 ILCVAIOAMVZIRRLNIIWUSGEWSRHCAUGIMFORSKVZMGCLBCGDRNKCVC P
 YUXLOKFYFOLBVCKDOKUUHAVOCOCLCIUSYCRGUFHBEVKROICSV PFTUQ
 UMKIGPECEMGCGPGGMOQUSYEFVGFHRA LAUQOLEVKROEOKMUQIRXCCBCV
 MAODCLANOYNKBMVSMVCNVROEDRNCGESKYSYSLUUXNKGEGMZGRSONLCV
 AGEBGLBIMORDPROCKINANKVCNFOLBCEUMNKPTVKTCGEFHOKPDULXSUE
 OPCLANOYNKVKB UOYODORSNXLCKMGLVCVGRMNOPOYOFOCVKOCVKVWOF C
 LANYEFVUAVNRPNCWMIPO RDGLOSHIMOCNMLCCVGRMNOPOYHXAIFOOUEP
 GCHK

Étape 7 :

MCCMMCTRUOUUUUREPUCCTCTPCCCCUUPCMMF
RTCCRUPECCMUUPCMPEPPUPURUPPMEUPUCE
UUCUCCCMEMTUPETPCMRCMCCUCCMPECRTMR
UPMPMRCPMMCRUMCUUEURPPCMOUUEUCCMUM
TUCUCUTMUUUPMUUCTCUPMMCCRPPPPMMMME
EUMRCCCPUUEUPMUMMCCPECUCUPCTCUEPMP
CUUEEUUUTPMMUCCTCCPPPCTPUCUCCCUREU
TUCMEPCCCEMUUUPRMMTMUCMMMCCCCCCEPU
ECUMRERUUUUMURCCPMUURUUPMUPRPPUUUU
MRCCPCPEURMMMPUTC RUUEOUUUMCMUURUPU
RUCMUCRUMMCUPUUMUCREUUUPCCURRCPRMC
TRCUUURCTPPMUUCCUUUUMUUEPCRMEMPMPUU
CCUMMUUMCUCMCCCRCTCCMEEUPTMUUMMMCC
PPTMCPTEOUUUMUUCRMCCCMCPRCRCEPMMCMC
PUUCMCCOMTPRCMCPCPMCPCERRECCRRECRU
PUEEPMUMTCUCEUUTPCEUMRCUUURRUCRUUC
RPPTTCPCPCUCUMUMPECEERPMMRMURUMEPM
RMMCPRUCRCPEERP UUUUREPCCMMEPPPRCCU
MPCCCMMEEUUPPERUECPUEMUCCUUCPUEPUC
MCMCUUCMMMUCUPCCMMUUUCUOPUCUPMPUECC
EUPMCEPRCTRMCCUUTECECCRMUCURUCMUCR
CMPCCUORUCTUCCMCUCMUMMTRUMCMMCPUUM
UPCCMPCUUEPCTECTUUTCEEMTUCTEPPRUUM
UUECMUMRUEPCUMPPOURUCCUPUCUCUEPCMM
ECCUCECP PCCCCOCRCRCRTUCPPTPUOCUORU
CCCEUCPPMRRC EUUURURCCMTPPURPPCTRRRT
RUUPMTMUUETRPROEMPTPTEPRERPTRUUMT
RUMTPPPRUUPEOUTPTROMUUERMMEPUTTOTO
OMTPRMPPTMREURRUPMTRPPREMUPRTRMMEO
UMMUPUUOUMEMOMECEPEUUUUCRUTTTTRTUPTT
PEREMUUREEPETRMPTRUUUOTRUUOOTTTOTT
ETETOUPOMTUUOUTOEETPTEMUUTURCUOPTR
POTEEMCOUUEPRMPTTTUPPRETTROEMUETPO
PMTERTEUUUPUPUUEMMOTOUMORRCMUUUEU

OTTEM TTCTMETEREUMUEETUMETPUTPUETTM
PEERTCPTOUUTRERETUTRETRTRUTCMTCUUT
POMTTPTPTOUMEOTTRPEPUTTTTRTTOUMUUTP
EECTMPPMUECTRPUCTEUUETPTOTPMTMCPUE
PPUPRMTPCRURPREMERTUEEROROTOMMRCUU
EUTPTPEPPEUUTPOTPPMEPEMTRREEUTUUTOTP
REEROPORRMUUTMPRTTMEEETERUTMTOOCPE
PPMPMTPRRMEPREUMMPRTREEPUTTPECTURU
RCOPEEEEEOOUEMOMPTUECERMMMPPEPMEUR
TEUMRTTPUTCEROETMUUROTOTTRMUETETTR
PROUTUUPREUTTRTPMTUPEEMETEPTOETUUT
EPTMUUEEPPTPMUPTTEPRMUTTPMUMMECRETE
PTRTURPMTOOUEEO TOURUURTUEUTPOMTPPU
REOTCMCPRPROOEERUUEERUMUUUCPPCPUET
ERURPORPTPCTPERERMUTTREUPRTMECUREP
POUTMOTCTMPTPOEUUTOTPTOREUETURMETR
EPEEPRUCPEMMPTMUUTTEOERMURUURUTPTT
ECETORTMTMETTUEMUUCTOPEMUUEPUMCMUC
MTPOUCECNTREMCPCMCTPMMPPCMUUUUCMCC
CPTMMUCREUUCTAREUCURECPMRCECUCEUCC
PMCTTPCREURMUTUPMPPPMMCUTMCMCCEUUCT
UPUUUUURCUMEPOTUUUCTEPCCPMCCTPCPUM
ERUCUMEMMRMUPCMUCUCRUUUUCPCUPCECM
CUUPOPCUUUUCUTTCPCM CUUCCEPUUPCMPUC
MMMPUUUEPMPPECR CMPRECR RUMCU ECPUPUC
EMPMUCRTUTUCRCCUPUUCUMMPUUUUECUUCC
ECPPPRRMCMMECCRM MRCC ECTURMCECCCPMM
MRPECUUUCPPMMECCMMRRCMUCMRCPUCMUC
CCPCTRCUUEUCCMTEMCRCP ECCUUCUUCPETP
CCPPTUMPCMPCMCEUCCCPCUCTCCCMTUMPTU
MEUCPPMUMPMREMCUMMMERUCUCCMPUUEUC
PCEPPRUUCCUCTPUETERCMMMURUUPURPUEE
MUMUMRCUUCRMRCPTMECEMMUCUCUUPPETTT
MPCPMUUEMPPCUTPMCMUUPUCCPMPRCMCRPU
PMEUURCOCP CUEPMRCPTMMMMCCECUMCUU
CEC PPUCPNRMEPCUURJCUCPR TUERMCCRPMU

URUUPMEUPCECPTRUTUMCECEFCUTCUCPEPC
CUUETFPFCDUUMCMMROUCCFPUCFFEPMECRFCM
CUMPUCUUUEMMCUTMCUMCUEUCMUCCTPUREU
PPCOPMPMUUMMMUUETPUUUUUFPPPMUECERU
RPURTPMFPFPMEMCTUPCMECPPCCEMURMPTUU
RCUEPCUECPUTCURUCPRUMTCCCCMPUCMEPE
MPRUPPECCPCUUCCCEUMRUUEUUEUCPCPMFU
CUMPUCUMPPREUUUPEUPEUUCTPOTUPETUOE
COTTEMOTEUTEUMUPMUTPOUPETERPUTPRUU
UPOTTEPTRRMTCETOROPMTRETRCOETPROEE
PTEPMMEUPEPEPUPUUREEPERTPEECEPORTU
EMETTEPTERMMTTETTTPORUMFTTERPPUURM
TTOMTMUMMUJTUOEPEUUOTCPEPTMRERURPE
TPPTTPPCORPTTTMUTRUPTTERREURPRTRETT
RCPRCUUMUPRUUUMTPRTRETTUUUOCUMUUUU
MOTTFEMETTERKPCCTCETUURMEPEEORCPETMP
PRUTTRUUETMOTMUUMTERUTOTCRPMURMUMR
MPMOOMOUOTPOREMEMUPTORTRRPOOUTPPPE
PMTPEOCTRMEETORTPEMMPEEETRURURPPU
PURTROUMTMRCUOTETRCRPEECPTEEUEMTT
PURUPEUCEUUMPEMUUTTEREUMERTTETTTME
UTMRTORMECUCUEUEPRUMTUUERMUTREUPE
EMEERCUUUTRMRTRMUUMMEPPTPRTEMTEMPE
UETPOOOUUMOTOUTCOPEPRUURTTTMMURTUTE
TPCOTEMTUOETRMTEETEMMTUMOEEOOUMOPTP
RUTMRMTRTPTUUEPUUPURROEUERUUOUPRTM
ETPEPPOTRMCMRUTTPUUEURTTEETETUUEUE
ETURRMEEMRZURCTPEMUUREPRUEORURUOPT
UMPEMTTFTUEMUPMCRTOOOUTPPMUUPUPERE
RUUOUEETUPETETPTTTEMRUURTTTUTTMUPR
PRRURUUTMTURTCUEEOMRRTEETTMUTPPRPEP
TREEOOTTETRETRUTPRUTMUUUTMUUCTUUPU
ERUEEMMUEETTPETMUMETTETTPMREMRTPT
TOURTPPOETTOMTPTETETUPTUCUMUCUOETUC
PECUCMUPMUCUTTUCTUUMUCURPUCPMCUMU
CCEPCMMUCPTPUMUPUCMECMPUMPMPMUEMPPE

PUTEUMEPEPUPUURMTPEMRPMMPTPOPRCRUE
PCMPFMRCCCPUCUPTUMUUPCPemptuumCCCU
PCCUTUUURCEMPEUCMRPPEPCMMUMPECMT
RERPUMPCCPTUCMCOPCURUECMTECMMCCRPP
EPUUCUTMUUUCCTMCMECPCUUUPUCUUUTCUC
CPTUUCMMPPREMCUURUUMUEUUPPUCRPMRU
PCMUEECUUCUURCERRCUCPMPUUMTUURCMP
EMUUUUCTUMTTTCUMPUMCMRTUUUCPPMEPUC
TOUPCMMCECUMCPECUPMTEPRUURURMPUPER
CRUCCCMPCUCMRMPMPPEEPTPEMCURCPCPUR
UTEUUEUUUPTCUCCEMMTUTREREMPRRMUCC
RCUMUEPUPUEUEPMUTRUCCMUUCMMUUPMECM
MEMUUUCMRPCMCUUCCETPCPRRMURRCTECMC
MUUUUUUECUUCUUTEPMUURCCCUURCUCECPP
UCMURCUUCRUCMCRCUUCUMEMUUCPPPPRCR
URUCMCPPCRMPUEPUMPOMUMMCUUUPCCCECT
MRPUPMPOCCTPCMUUMCMCCTUCECUUMCCMCU
ERTTRCMMUMTCPERUUMMTRUEUMCMCCMCUUP
MUCCTPUMCUTPUMCUUUUCPPUCETUPERTRUU
UUMMCUMEEMCTCCPURRUURCPUPCCUPMPMM
URUCCCEPRPUMMUTCMCMCCCUCPPCMEPCRE
MUURCTPEMCMCCPRUCCUUUCCUUPCUUPUTRU
EEUUUEUCRPMRUUUOCPOCRPCMECRCPCECUU
ECPUMPPEPCPRMPEUCPTUEMTUTTEOPRUEP
EPMTPUPTTRREEPUEMMOPMUPRUUUMEMPPPU
TOUROPROPPMETPRMTUURPTPUUTOUUMTEPC
OEMCUUTPUUPTOTUUTTUUURTPTRTTMOCTRU
TROTTROPTUMPPMURTEUMTPEUMCMPREPMRE
EEEUTTTEUUTMTPURUEUUMTUPPUTTREMTPT
RRUTURTRUUTOTEROTMUUU?MUPTPUURTERU
MMTMTTUPRPPPEMEPCMUMTRREMUCEUPPTTT
TTPRUUURTEEPUPUTMMTUPMRUOPEUEETMMP
EMTPECRETMEOUTMEEPREUMEMRTOTEMTOTP
TECEPTUTREEEMPPTPEECPPTMUUTMUMPRME
REUUPTOEOPUETRTTEPMOUMPEUTMTTMUUU
TTPTERMTRRUURUUEURTEEMUTTEPOUUEMEE

PCRURMETMETOREUUOTRTPRTTEUMMTPMMRP
EUURERTEOTUTRROTOTETTEOTUEUUETUETP
MUOORTOUMCOTUECEUUREUUMTTERUOTTNTE
TTEOTUTEPTTRCTUUPPERUTOUUEORMUEMPRE
MUUPOFMOUOOTECEUOETUCMTTPPTTUURTTNMO
PTPUCMTUUOMUMTTTORTUPETETROMTRET TU
EUUTPPTMEUMURUUUUURETUTRURRTTPTPTPO
ETEMUCTCOUEMTTMTUEUPTUPUPPTROTUEER
OEROUEMCPTERCPTMUUMTOMCEMUTPTTTOU
TOEMTTPPCREPOTEPPEERPOPPOTEUUUURPUU
CPRPRMTREUUERMUCTOPTTUUTPMCTRMETEM
MUOPTUUETPPMMRMTUPRMUPRMOUPRTEUUUR
MMCORTUMTOETMUPMUTTPUTTERMUUPCETMT
UPTPPETRUTTPOTMECURCPUOPMTPMCMPPEC
MMUORRMPCMMORCCUTCCOMCUUPRCPPPUUU
EUPRUPMCECTMCCUURPPMUUEUUUUCETUURC
PUUREUCECEUCCUECUUURCPMCCCUPRMUCMU
CPRUPPUOMP UUUCMUUCPMUCRCPMMTCMUOM
CMCCMUUPCCTURUEUUUCUMTUCCMMUCTCERU
RUMRPRUCUCEMUCCUUUBTUMCPCURPURCUUM
UPPCEMPPPUUMPPCCPRCECCRMCPPRCCRP
MUUURCMEP CPUCCCCUPRRUUPMCEMCUTMUCC
MEPMMPPMUUCCEMPREUUTCPCUCMCCUCMRTP
MPCUCPPMRCPCEPMPFPMRUUCCUUPRCERTU
UPCUMUPUMP CRCCEPCUCCPMTRPCPCUUCRPP
RURCCMEUURUUMURPEMRUCCMMUCRMCTMRPR
CUCMCUUCUMMUUEMCTMCCMUCTCMUCMPMUT
RURREOCUCRCUPUCMPCEUCCEUUEPUMPTCCE
URCUUCPURCTPEUUMMUUCCMMMTUCRCRMRPO
UCUCUPCMPCUCTPMHUPUCUMUMCUTPPMEUUU
PUPCUUUUCMPUEMCUPCCRPPRUUMCCUCUPCP
CPCCUUUCURCCPURCUTURECRUUCMTCCCMUC
CPPPCMUCCUUUUUMMPUCRCUECCTPCPMEECM
UUCCCUUMCPCCCUUCUPCUPUTCMMCUIMMUM
PUMMPTRMMPPPMRUUUCUURETUCPECRPURUR
CCCTPPMT PUPMPPMRMUEPUPUUUUUEPUCNPR

P P C C R O U U E C T U P C U P C C U U C P C P C M U E C M U T U U
 P C U U T P P P C M M U P C C R U C E R T U C T E C M C U U E C R P
 U M C U T C U E C C U P C U C C P U R P M M T U T P P O C U R C P C
 P P M C M C C C P U P P M R U T E R M O T U M U U E M R C U U T P U
 P P T T T M U O T T E R P R E T T R M T E M T E U U T T R P T T C U
 T M T U P M R E U P M U E U U U U U P T E T C P U C E E C T E R M M
 T M O T M P M E T R P E R O P E M E M M P R P T R U P T U O E U M P
 P U R M U U E M M M P U C P U M U T M P E U U O P P U O M P T O T R
 R M T P C P P P R E P E E R M R E M U T P O U E M P P E E R R M T R
 T O M E P T E M U E P R T U R O O T O M U P P E R O T T P T T M P P
 T P C U U U M T T U R E O P M T R E T T M E E U U O P M E R M P E T
 E E R M U T T M M P E P O E T M E T E R U U O O R M E M M T R U U R
 U O P R U P R P P U U U E E E T T T T P E U R E R R P U E T R U U E
 O O U E T E U U M U T U R U T R U U T O P O T U P M U R U U E R U
 U U P U O O T T T P M E U E R T M O U M T P P P E O M T T U U U O E
 U U E T U U E T U R P U M T M M E R R U U E T O T P T T T R P T M P
 E E M T M E U U P O E T T P P P R U T E E C O U M E U U T T R T T T
 R T T R T T M E P P T R T P O U T R T T O P E C R T P U T T C E M P
 T O M R E T T T R E U C O T O T R P R U R P T U T E U U E P M E O T
 M M U U U R R E T M O U M M P C P E T P T P R M T U P U E T E T E E
 M C C T E R U R O E E P R R R R T P T U U M T P E E M C U O U U R E
 C T U P P R T P P M T M U M C T T T P R R E O U T P E R U T M P U R
 R U T U M O T T E E T M T R M R T O M T R R R R T O P T T E R U O O M
 U T P R M M P R P U E T M E U T T M P P R T P T P T T U U M R T E T
 T R R O T U R U T R U U C M R C M T O C R U T P O T T P T M T E O R
 R M R U E U R R T T O U R U P T U E C T E O T M T P R T P U M M R E
 E E P O R P U R P R U M E M O T T R O P R U E T T U E T R O M T O U
 E O P U T M T U R P T P R R T M O R E T C T M T M U E T T M R T T E
 O R P C P P M M U M T T O U M T E U U R T R T R M E M U U T M T U T
 R E T P M T P P M M

Étape 8 :

Umkehr- walze		Walze 3		Walze 2		Walze 1		Stecker- brett		Tastatur
Y A		B A		E A		A A				A
R B		D B		K B		J B				B
U C		F C		M C		D C				C
H D		H D		F D		K D				D
Q E		J E		L E		S E				E
S F		L F		G F		I F				F
L G		C G		D G		R G				G
D H		P H		Q H		U H				H
P I		R I		V I		X I				I
X J		T J		Z J		B J				J
N K	←	X K	←	N K	←	L K	←		←	K
G L		V L		T L		H L		?		L
O M		Z M		O M		W M				M
K N	→	N N	→	W N	→	T N	→		→	N
M O		Y O		Y O		M O				O
I P		E P		H P		C P				P
E Q		I Q		X Q		Q Q				Q
B R		W R		U R		G R				R
F S		G S		S S		Z S				S
Z T		A T		P T		N T				T
C U		K U		A U		P U				U
W V		M V		I V		Y V				V
V W		U W		B W		F W				W
J X		S X		R X		V X				X
A Y		Q Y		C Y		O Y				Y
T Z		O Z		J Z		E Z				Z

KJQPWCAISR XWQMASEUPFOCZOQZVGZGWW
KYEZVTEMT PZHVN OTKZHRCCFQLVRPCCWL
WPUYONFHO GDDMOJXGGBHWWUXNJEZAXFU
MEYSECSMA ZFXNNASSZGWRBDDMAPGMRWT
GXXZAXLBX CPHZBOUYVRRVFDKHXMQOGYL
YYCUWQBTAD RLBOKYXQPWUUA FMIZTCEA
XBCREDHZJ DOP SQTNLIHIQHNMJZUHS MVA
HHQJLIJRR XQZNFKHUIINZPMPAFLHYONM
RMDADFOX TYOPEWEJGEC AHPYFVMCIXAQD
YIAGZXLD TFJWJQZMGBSNERMI PCKPOVLT
HZOTUXQLR SRZNQLD HXHLGHYDNZKVB FDM
XRZBROMD PRUXHMF SHJ

Schlüssel

0716150413020110

Schriftzeichen

```
begin 644 DEBUGGER.BIN
(-&>`_EU-_/ $`
,
end
```

Étape 9 :

```

begin 600 text.d
MM5P7)_8F_,H[JOF1C//L/W+)%QSK*Q37CJ-N 'W[_;CQSTW'UY0S2,\LQVG0
M@1&HY^1MHYI\>2P'F:6Y*E%X4A&$2'=L28$$..9["-ZIGA_VP(GIPK[CW3^L
M55+60D^&=FS61(L96YG> '59*1Q^)/C?$1/C&9PN35-HP;.>V8_/P(.:+R(
M61]'NG^UF:,#57MMQSKN[N7M>1NE;2(!RUA495Q16!;Q<*( "[C*"A"@%A+=S
M8AR45+G$-#8A?29V_.6%7*6D$J_G4JX'JM^1? K@._#(B/N7-<YNU;/,JF8C
M6LD[90MVJ2'I*.G@>9U%!E(33!S^K# N7JH_Y5RYE&=J@S!>^<C3Y=PD%-RP
M9&+^"JLPOK%T)-5KI>IUA"W;7;&D(D-2/U'$3\C7 ?]B* 3*C/Y!%U >&V6
M%W85NJ:JPO(>#C1)CFEL&^H3YKR2.59XJVD??\MX+ [S?3X_F^/*1$NGH$B&
MI$!L2-C'E/@OD*&5;6+P+G1S D49AO=#9\C!4D$/F;C(H#MX:\%G[K[OR+2RG
M@SCSVG!A5%FEV!=$YD"V.2T06@>C-&)3H<:Y9BOR=V#S_>\:S8GZ.*A"$!T
MZOE=/4QWLLB<[:K8T TZ@C9_,( #D:/G4)P2>,S?%9: Q]MV0;?F9;F1VP'@
M=!XCI_M>2?F=' ;20):%Y61[.! -W8%7M3BJUX/&!--E@A7C\(>5SZXESA$!LZ
MF\_U//JGV"KKHE259927962%P-9J!*J@ DPJF]M2/>DXHA?JT"^2C7;_-9B;
MBM'CFTYUR#DOA7.J4ZW8=+3(9O>#4A+^!=4IV_6A!(PNGZ:T$O)659KNGS=>
MN"?LQ3$6F*I43Q(3_U:64V/L9$<E%">*#A9P>@(66#XDS!)-'*\JZE.,=G29
MOJLH!9.Y#+=?]"C?2/?H5O!A]<KW^H%J "&+>EXK;II6)N6JY$%UB'BN3'F
MMS[XKP#JY(:3@V);U2,5PG 6$!46;.B/K'E7$4'MKN1]* YX^R"Q?Q+;,"./
MPL(<[>]UF90L7[<]9^E0*:NMBI(Q+B'>-IHF+,J0&"G0F.5L8@")<Y$<ZRU=
M']&L9!WD1Y<V[D:/:4J(+X(NIKKDF0@#:5O_3G%7]AG5H.? ,%;D)=7'HKE
M.(_E=(*(W5HO3RA5WP8<!ZM.K2T.:&#P\LV;!7W$ K3)/A7D&P8SVO3-?$U1
M2J10K3T>2)OVRA'Y;C<DZVV+'$VXI_ $JZ^)^39,'.7MK,0*QOP906QRQ0F(*
M&8J90!Z">N;S%MD%$A.SD?'^\'K)*R_@XE6V# >&P.$L#$,%N"C[H:A_EPH$V
M\H)(;C0#3^C] T9Z0=,9UQ(3N^3D],9PVM<AJ.T:('(.=1FB;NBV_YS!\7ON
M?-T%5B;2J^TORBWA^Z$B'$K8LC;'A+>@87(6!8Q%FRS=^;Y*0$FC">;I!NI*
@##0SNY_0_-EK1>;84QMT0/(KQQ2LL+R##K:I=NK7.OT

end

```

Étape 10 :

Message court :

```

10052 30973 22295 13534 12990 66921 15454 81904 58209 26472 18119
11542 99190 01294 87266 20201 55809 80932 92390 96710 64341 91354
27685 27572 48495 78859 80627 33369 29356 36094 85523

```

Message long :

begin 600 text.d

M.4#)>S I:R!!4)NA+\%T%V/(AW!7HHDP\$;T[\E!RWA?,J8:X#D[!:XF,A>K
MXT9\$Q)37\IOMG6KL-\$6?A!#FZ2Y)N+4%*.^2K!SP?Z2'8O7LZ]QP \T=QG-*
MAMJA;Q@3H[8^U/L<ILL%TA0J9M*F@8F?H:76%<33JOESAP=@3:(\:8NBGFM0
M,MP3B^CP%/D8DICZ\$VO(7IS(DTJRZ&#Y- 7I\ -#VI0">J@+O!CT.+6B9K\$J%
4:EAB9%1#;(P+I>1!#<+2+;(7.W<

end

Annexes

Annexe A

Premier paragraphe de *A void*, la traduction en anglais par Gilbert Adair de *La Disparition*, de Georges Perec

Today, by radio, and also on giant hoardings, a rabbi, an admiral notorious for his links to masonry, a trio of cardinals, a trio, too, of insignificant politicians (bought and paid for by a rich and corrupt Anglo-Canadian banking corporation), inform us all of how our country now risks dying of starvation. A rumour, that's my initial thought as I switch off my radio, a rumour or possibly a hoax. Propaganda, I mur-mur anxiously — as though, just by saying so, I might allay my doubts — typical politicians' propaganda. But public opinion gradually absorbs it as a fact. Individuals start strutting around with stout clubs. "Food, glorious food !" is a common cry (occasionally sung to Bart's music), with ordinary hard-working folk harassing officials, both local and national, and cursing capitalists and captains of industry. Cops shrink from going out on night shift. In Mâcon, a mob storms a municipal building. In Rocamadour, ruffians rob a hangar full of foodstuffs, pillaging tons of tuna fish, milk and cocoa, as also a vast quantity of corn — all of it, alas, totally unfit for human consumption. Without fuss or ado, and naturally without any sort of trial, an indignant crowd hangs 26 solicitors on a hastily built scaffold in front of Nancy's law courts (this Nancy is a town, not a woman) and ransacks a local journal, a disgusting right-wing rag that is siding against it. Up and down this land of ours looting has brought docks, shops and farms to a virtual standstill.

Première publication en France de *La Disparition*, Éditions Denoël, 1969, en Grande-Bretagne ; Harvill, 1994.

© Éditions Denoël, 1969

© Pour la traduction anglaise, Harvill, 1994. Reproduction autorisée par Harvill Press.

Annexe B

Quelques conseils élémentaires pour l'analyse de fréquence

1. Commencez par compter la fréquence des lettres dans le texte chiffré. Huit lettres seulement devraient avoir une fréquence inférieure à 1 %, et elles sont mises probablement pour : **f, h, j, k, w, x, y** et **z**. Une seule des lettres a une fréquence supérieure à 10 %, ou même à 15 %, et représente probablement **e**. Si le texte chiffré n'obéit pas à cette répartition des fréquences, envisagez la possibilité que le texte ne soit pas écrit en français. Vous pouvez identifier la langue en analysant la distribution des fréquences dans le texte chiffré. En anglais, par exemple, cinq lettres ont une fréquence inférieure à 1 % (**j, k, q, x** et **z**) et une seule, le **e**, a une fréquence supérieure à 10 %. En italien, trois lettres ont une fréquence supérieure à 10 % et neuf lettres ont des fréquences inférieures à 1 %. En allemand, la lettre **e** a une fréquence extrêmement élevée de 19 %, ainsi n'importe quel texte présentant un signe avec une telle fréquence a des chances d'être en allemand. Lorsque vous avez identifié la langue, vous utilisez la table des fréquences appropriée pour effectuer votre analyse de fréquence. On peut ainsi décrypter même les textes chiffrés dans une langue inconnue, du moment que l'on possède la table de fréquence appropriée.
2. Si la corrélation au français s'impose, mais que le texte clair n'apparaît pas immédiatement, ce qui est souvent le cas, concentrez alors vos recherches sur les paires de lettres répétées. En français, les doublets les plus courants sont, dans l'ordre, **ss, ll, mm, rr, tt, nn, pp, ee, cc, ff**. Si le texte chiffré contient des caractères répétés, vous pouvez supposer qu'ils représentent l'un de ces doublets.
3. Si le texte chiffré respecte les espaces entre les mots, alors essayez d'identifier les mots courts, d'une, deux ou trois lettres. Les mots d'une lettre sont soit **a**, soit une lettre suivie d'une apostrophe comme **l'** ou **n'**. Les mots de deux lettres qui reviennent le plus souvent sont : **de, il, le, et, je, la, ne, un, en, ce, se, sa, du**. Les mots de trois lettres les plus fréquents sont : **que, les, son, mon, pas, lui, une, des, qui, est**.

4. Si vous le pouvez, utilisez une table de fréquence sur mesure pour le message que vous tentez de déchiffrer. Par exemple, les messages militaires tendent à omettre pronoms et articles, et l'absence de **je**, **le**, **un** ou **a**, réduira la fréquence de certaines des lettres les plus répandues. Si vous savez que vous attaquez un message militaire, le mieux serait que vous lui appliquiez une table de fréquence générée par d'autres messages militaires.
5. Une des capacités les plus utiles à un cryptanalyste est la faculté d'identifier des mots, voire des phrases, simplement en devinant leur sens. Al-Khalil, un des premiers cryptanalystes arabes, montra ce talent en décryptant un texte chiffré grec. Il supposa que le texte chiffré commençait par la formule « Au nom de Dieu ». Ayant corrélié ces lettres à une section précise du texte chiffré, il put les utiliser comme levier pour avoir prise sur le texte chiffré. On appelle ceci des mots probables (en anglais, des cribs).
6. Dans certains cas, la lettre la plus répandue dans le texte chiffré peut être le E, la deuxième le A et ainsi de suite. Autrement dit, la fréquence des lettres dans le texte chiffré correspond exactement à celle de la table de fréquence. Le E du texte chiffré semble bien représenter e, et la même chose sera vraie pour les autres lettres, pourtant le texte apparaît être du charabia. Dans ce cas, vous devez être en face, non d'un chiffre de substitution, mais d'un chiffre de transposition. Toutes les lettres se représentent elles-mêmes, mais elles ne sont pas à leur place.

Annexe C

Le code dit de « la Bible »

En 1997, la publication du livre de Michael Drosnin, *The Bible Code*, eut des répercussions mondiales. Drosnin prétend que la Bible contient des messages cachés que l'on peut découvrir en y recherchant des suites de lettres équidistantes (EDLS). Une EDLS est relevée dans n'importe quel texte, en choisissant une lettre de départ et en sautant ensuite un certain nombre de lettres à chaque fois. Ainsi par exemple dans ce paragraphe, nous pouvons partir de la lettre *M* de *Michael* et sauter, disons, de cinq lettres en cinq lettres. Nous obtenons la séquence *meshle...*

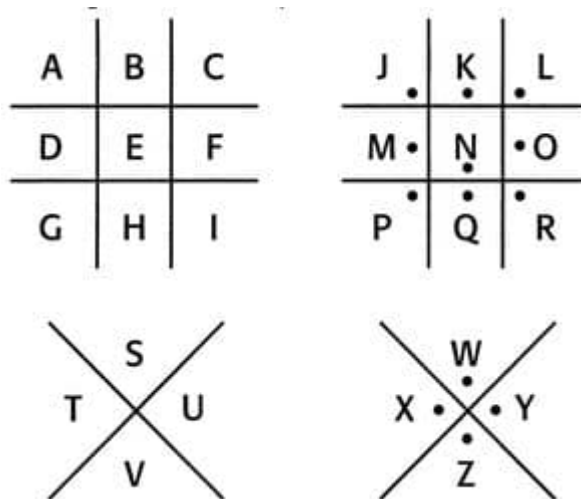
Cette séquence-ci ne donne pas un mot ayant un sens, mais Drosnin réussit à trouver dans la Bible un nombre surprenant de séquences de cette sorte qui, non seulement, comportaient des mots intelligibles, mais même parfois des phrases entières. Il prétendait ainsi avoir trouvé des allusions aux assassinats de John et Robert Kennedy, et d'Anouar al-Sadate. Dans une séquence, le nom de *Newton* était mentionné non loin du mot *pesanteur*, et dans une autre encore *Edison* apparaissait à côté de l'ampoule électrique ! Le livre de Drosnin est basé sur un article publié par Doron Witzum, Eliyahu Rips et Yoav Rosenberg, mais il est beaucoup plus ambitieux dans ses démonstrations et s'est attiré quantité de critiques. D'abord, le texte étudié est énorme : dans un texte suffisamment long, il n'est pas étonnant qu'en variant le point de départ et la longueur des espacements, on puisse faire apparaître des phrases porteuses de sens.

Brendan McKay essaya, à l'Université nationale australienne, de démontrer combien l'argumentation de Drosnin était faible en cherchant des séquences engendrées de la même manière dans *Moby Dick*. Il découvrit treize indices ayant trait aux assassinats de gens célèbres, dont Trotsky, Gandhi et Robert Kennedy. Par ailleurs, les textes hébreux sont d'autant plus riches en éventuelles séquences interprétables qu'ils ne comportent que très peu de voyelles. Cela permet de faire dire à la suite de lettres un peu ce qu'on veut, en insérant des voyelles où on le juge bon, ce qui rend plus facile d'en tirer des prédictions.

Annexe D

Le chiffre Pigpen (l'Enclos des cochons)

Le chiffre de substitution monoalphabétique a perduré pendant des siècles sous des formes variées. Le chiffre Pigpen, qui fut utilisé par les francs-maçons au XVII^e siècle, est aujourd'hui familier aux écoliers. Le chiffre ne substitue pas une lettre à une autre, mais substitue à chaque lettre un symbole conformément au dessin ci-dessous :



Pour crypter une lettre, on cherche sa position sur l'une des quatre grilles et l'on reproduit la portion du dessin de la grille qui la contient. D'où :

a =

b =

⋮

z =

Si vous connaissez la clef, ce chiffre est enfantin à déchiffrer. Sinon, on peut le briser facilement par :

LEJLEVO JO CFOKOLO

Annexe E

Le chiffre Playfair

Le chiffre Playfair a été popularisé par Lyon Playfair, premier baron Playfair of St Andrews, mais il avait été inventé par sir Charles Wheatstone, un des pionniers du télégraphe électrique. Les deux hommes vivaient de part et d'autre du pont Hammersmith, à Londres, et se rencontraient souvent pour échanger des idées sur la cryptographie.

Ce chiffre remplace chaque paire de lettres du texte clair par une autre paire. Pour crypter et décrypter un message, émetteur et récepteur doivent convenir d'abord d'un mot-clef. Nous pouvons prendre le prénom de Wheatstone, Charles, comme mot-clef. Ensuite, avant le chiffrement, on écrit les lettres de l'alphabet en formant un carré de 5 lettres sur 5 lettres, en commençant par le mot-clef et en poursuivant par l'alphabet dans l'ordre, I et J fusionnant en un seul élément.

C	H	A	R	L
E	S	B	D	F
G	I/J	K	M	N
O	P	Q	T	U
V	W	X	Y	Z

Ensuite le message est scindé en paires de lettres, ou digrammes. Chaque digramme doit être composé de deux lettres différentes, nous serons donc amenés à insérer un x supplémentaire entre les deux m de hammersmith.

Texte clair : au pont de hammersmith ce soir

Texte clair en digrammes : au-po-nt-de-ha-mx-me-rs-mi-th-ce-so-
ir

Le chiffrement peut commencer. Tous les digrammes vont tomber dans une de ces trois catégories : les deux lettres sont sur la même ligne, ou dans la même colonne, ou rien. Si les deux lettres sont sur la même ligne, elles seront remplacées par les deux lettres figurant à leur droite immédiate ; ainsi *mi* devient NK. Si l'une des lettres est en bout de ligne, elle est remplacée par la lettre en tête de la même ligne, (*ni* s'écrirait GK). Si les deux lettres sont dans la même colonne, elles sont remplacées par la lettre immédiatement au-dessous d'elle ; ainsi *ce* devient EG. Si l'une des lettres est en bas de colonne, elle est remplacée par la lettre en haut de la colonne ; ainsi *ve* devient CG.

Si les lettres du digramme ne sont ni sur la même ligne, ni dans la même colonne, on applique une règle différente. Pour chiffrer la première lettre, suivez la ligne sur laquelle elle figure jusqu'à ce qu'elle croise la colonne où figure la deuxième lettre ; la lettre qui se trouve à l'intersection remplacera la première lettre. Pour chiffrer la deuxième lettre, suivez sa ligne jusqu'à ce qu'elle croise la colonne de la première lettre : la lettre située à l'intersection remplacera la deuxième lettre. Ainsi *me* devient GD.

Texte clair en digrammes : au - po - nt - de - ha - mx - me - rs - mi - th - ce - so - ir
Texte chiffré : LQ-QP-MU-FS-AR-KY-GD-HD-NK-PR-EG-EP-MH

Le destinataire, qui connaît le mot-clef, peut aisément déchiffrer le message en inversant le processus : par exemple, les lettres chiffrées appartenant à la même ligne seront déchiffrées en les remplaçant par les lettres à leur gauche immédiate.

Playfair n'était pas seulement un savant, c'était aussi un personnage public important, et il était déterminé à promouvoir l'idée de Wheatstone auprès des hommes politiques. En 1854, il en parla au cours d'un dîner où se trouvaient le prince-consort Albert et le futur Premier ministre, lord Palmerston, et plus tard il présenta Wheatstone au sous-secrétaire aux Affaires étrangères. Celui-ci regretta que ce système soit trop compliqué pour être utilisé sur un champ de bataille, sur quoi Wheatstone répondit qu'il se faisait fort d'apprendre la méthode aux garçons de l'école primaire voisine en un quart d'heure. « C'est possible, répondit l'homme des Affaires étrangères, mais vous ne l'apprendrez jamais aux attachés. »

Playfair insista et finalement le British War Office adopta secrètement cette technique, et s'en servit sans doute pendant la guerre des Boers. Il

sembla d'abord efficace, mais en réalité, le chiffre Playfair n'était guère défendu. On pouvait l'attaquer en regardant quels digrammes apparaissaient le plus souvent dans le texte chiffré, et en supposant qu'ils représentaient les digrammes les plus courants (en anglais : th, he, an, in, er, re, es ; en français : es, en, ou, de, nt, te, on).

Annexe F

Le chiffre ADFGVX

Le chiffre ADFGVX utilise à la fois la transposition et la substitution. Le chiffrement commence par l'établissement d'une grille de 6 x 6 cases, les 36 cases étant ensuite remplies par la disposition au hasard des 26 lettres et des 10 chiffres. Chaque ligne ou colonne de la grille est identifiée par une des six lettres A, D, F, G, V, X. La disposition des éléments sur la grille est partie intégrante de la clef et doit donc être communiquée au destinataire pour qu'il puisse déchiffrer les messages.

	A	D	F	G	V	X
A	8	p	3	d	l	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Dans un premier temps, on va prendre chaque lettre du message, regarder sa position sur la grille, et lui substituer les lettres en tête de sa ligne et de sa colonne. Ainsi 8 sera remplacé par AA et p par AD. Voici un message crypté selon ce système.

Message	attaque à 10 h 5
Texte clair	a t t a q u e a 1 0 h 5
Texte chiffré (1 ^{ère} étape)	DV DD DD DV XX GD XD DV AV XG DX FV

Jusque-là, nous appliquons un simple chiffre de substitution, et l'analyse de fréquence en viendrait à bout. La seconde étape du chiffre ADFGVX est une transposition qui va rendre la cryptanalyse bien plus difficile. La transposition dépend d'un mot-clef, qui ici sera MARC, et qui doit être connu des deux correspondants. On applique le système de transposition suivant. D'abord, les lettres du mot-clef sont écrites sur la première ligne d'une nouvelle grille. Ensuite, on porte le texte chiffré de la première étape sur une série de lignes, comme ci-dessous. Les

colonnes de la grille sont ensuite replacées de telle sorte que les lettres du mot-clef soient dans l'ordre alphabétique. Le texte chiffré final est obtenu en descendant chaque colonne l'une après l'autre et en écrivant les lettres selon ce nouvel ordre.

M	A	R	C
D	V	D	D
D	D	D	V
X	X	G	D
X	D	D	V
A	V	X	G
D	X	F	V

Déplaçons les colonnes
 pour mettre les lettres
 du mot-clef
 dans l'ordre
 alphabétique


A	C	M	R
V	D	D	D
D	V	D	D
X	D	X	G
D	V	X	D
V	G	A	X
X	V	D	F

Texte chiffré final : V D X D V X D V D V G V D D X X A D D D G D X F

Le texte chiffré final pourra être transmis en morse, et le destinataire inversera le procédé de chiffrement pour retrouver le texte original. Le texte chiffré n'est fait qu'avec six lettres ADFGVX, qui qualifient les lignes et les colonnes de la première grille. On demande souvent pourquoi ces lettres ont été choisies plutôt que, disons, A, B, C, D, E et F. La raison en est que A, D, F, G, V et X ne se ressemblent pas lorsqu'on les traduit dans le système points et traits du morse, ce qui minimise les risques d'erreurs dans les transmissions.

Annexe G

Pourquoi il ne faut pas utiliser deux fois un chiffre à clef jetable

Pour les raisons exposées dans le chapitre 3, les textes chiffrés cryptés selon un chiffre à clef à usage unique ne sont pas attaquables. Cette sécurité repose sur l'obligation de l'utiliser une fois et une seule. Si nous interceptions deux textes chiffrés, cryptés selon la même feuille du bloc à usage unique, voici comment nous procéderions pour les décrypter.

Nous aurons des chances de ne pas nous tromper si nous supposons que le premier texte chiffré contient le mot **que**, et nous commencerons la cryptanalyse en postulant que le message n'est qu'une suite de **que**. Ensuite, nous établissons le chiffre jetable qui permettait de transposer la suite de **que** dans le premier texte chiffré. Ceci est une première approche, mais comment savoir quelles parties du chiffre ainsi élaboré sont exactes ?

Nous pouvons appliquer au deuxième texte chiffré, le chiffre jetable que nous avons établi, et voir s'il en ressort un texte clair qui ait un sens. Si nous avons de la chance, nous pourrions discerner quelques fragments de mots dans le deuxième texte clair qui nous indiqueront que les parties correspondantes de notre chiffre jetable sont justes. Ceci nous montrera quels endroits du premier message comportaient réellement **que**.

En partant des fragments identifiés dans le second texte clair, nous pouvons reconstituer un peu plus le chiffre jetable et en déduire de nouveaux fragments identifiés dans le premier texte clair. Nous continuons la progression de la même manière. Nous finirons, en faisant cette navette d'un texte à l'autre, par déchiffrer entièrement les deux.

Ce procédé est très proche du déchiffrement d'un message chiffré avec le chiffre de Vigenère et dont la clef consiste en une série de mots, comme dans l'exemple, au chapitre 3, où la clef était : CANADA-BRESILEGYPTECUBA.

Annexe H

Solution des mots croisés du *Daily Telegraph*

Horizontalement

1.Troupe

4.Short Cut

9.Privet

10.Aromatic

12.Trend

13.Great deal

15.Owe

16.Feign

17.Newark

22.Impale

24.Guise

27.Tree

28.Centre bit

31.Token

32.Lame dogs

33.Racing

Verticalement

1.Tipstaff

2.Olive oil

3.Pseudonym

5.Horde

6.Remit

7.Cutter

8.Tackle

11.Agenda

14.Ada

18.Wreath

19.Right nail

20.Tinkling

21.Sennight

23.Pie

25.Scales

26.Enamel

34.Silencer

29.Rodin

35.Alight

30.Bogie

Annexe I

Exercices pour le lecteur intéressé

Certains des plus illustres déchiffrements de l'histoire ont été réussis par des amateurs. Ainsi, Georg Grotefend, qui fit les premières découvertes sur l'écriture cunéiforme, était un instituteur. Pour ceux de mes lecteurs qui brûlent de suivre sa voie, qu'ils sachent que plusieurs écritures restent mystérieuses. L'écriture minoenne, dite Linéaire A, a découragé toutes les tentatives de déchiffrement, en particulier parce qu'on dispose de très peu de matière sur laquelle travailler. L'étrusque ne souffre pas du même problème, avec plus de 10 000 inscriptions disponibles, mais il a lui aussi tenu en échec les spécialistes les plus compétents.

La langue ancienne européenne la plus surprenante apparaît sur une unique pièce, le disque de Phaistos, qui a été trouvé en Crète en 1908. C'est une table toute ronde, datant d'environ 1700 avant J.-C., et qui porte un texte clair écrit en forme de deux spirales, une sur chaque face. Les signes ne sont pas faits à la main, mais à l'aide de divers tampons, ce qui en fait le plus ancien exemple connu de dactylographie. Curieusement, on n'a trouvé aucun autre document similaire, aussi ne dispose-t-on que de bien peu d'information : 242 caractères divisés en 61 groupes. Pourtant, la *dactylographie* même du document semble impliquer une large diffusion, et les archéologues ne désespèrent pas de finir par mettre au jour un lot de disques identiques, et de faire la lumière sur cette écriture impénétrable.

En dehors de l'Europe, un des grands défis est le déchiffrement de l'Indus, une écriture remontant à l'âge du bronze que l'on a trouvée sur des milliers de sceaux du troisième millénaire avant J.-C. Chaque sceau porte le dessin d'un animal accompagné d'une courte inscription, mais le sens de ces inscriptions a jusqu'ici échappé à tous les spécialistes. Dans un seul cas, l'écriture a été relevée sur une planche de bois portant des lettres de 37 centimètres de haut. C'est peut-être le plus vieux panneau d'affichage au monde. Cela prouverait que l'alphabétisation n'était pas réservée à une élite, et pose une question : sur quoi portait cette annonce ? La réponse la plus probable est sans doute qu'il s'agissait là

d'une célébration d'un roi, et si l'on pouvait découvrir l'identité du roi en question, l'affiche offrirait le moyen d'attaquer le reste de l'écriture.

Annexe J

Les mathématiques du système RSA

Ce qui suit est une description simplifiée de la procédure de chiffrement et de déchiffrement RSA.

- (1) Alice choisit deux nombres premiers p et q . Ces nombres devraient être géants, mais pour la simplicité de la démonstration, nous supposons qu'Alice a posé $p = 17$ et $q = 11$. Elle doit garder ces nombres secrets.
- (2) Alice forme le produit de l'un par l'autre et obtient ici $N = 187$. Elle doit choisir un autre nombre et, dans le cas présent, elle choisit $e = 7$. Elle doit faire en sorte que la somme $e + (p-1) \times (q-1)$ soit un nombre premier relatif, mais ceci est affaire de technique.
- (3) Alice peut maintenant diffuser e et N par un moyen approprié, type annuaire de téléphone. Ces deux nombres étant nécessaires pour le chiffrement, ils doivent être disponibles pour toute personne ayant à crypter un message pour Alice. L'ensemble de ces deux nombres s'appelle la clef publique. (Tout en étant un élément de la clef publique d'Alice, e peut aussi figurer dans la clef publique de n'importe qui d'autre. Toutefois, chacun doit attribuer une valeur différente à N , qui dépend du choix de p et q .)
- (4) Pour crypter un message, celui-ci doit d'abord être converti en un nombre N . Par exemple, un mot est traduit en bits selon le code ASCII, et ces bits sont considérés comme l'écriture binaire du

nombre décimal M . Celui-ci est alors crypté pour obtenir le texte chiffré, C , selon la formule :

$$C = M^e \pmod{N}$$

- (5) Imaginons que Bernard veuille envoyer à Alice un baiser, simplement la lettre X. En ASCII, celle-ci est représentée par 1 011000, qui est équivalent à 88 en système décimal. Donc $M = 88$
- (6) Pour crypter ce message, Bernard commence par chercher la clef publique d'Alice, et trouve $N=187$ et $e = 7$. Cela lui procure la formule de chiffrement requise pour crypter les messages pour Alice. Avec $M = 88$, la formule donne :

$$C = 88^7 \pmod{187}$$

- (7) Obtenir cela d'une machine à calculer n'est pas évident, surtout avec les nombres géants qui devraient être utilisés, car la machine ne peut pas afficher de trop grands nombres. Cependant, il existe une technique simple pour calculer des exponentielles en arithmétique modulo n . Nous savons que, puisque $7=4+2+1$,

$$88^7 \pmod{187} = [88^4 \pmod{187} \times 88^2 \pmod{187} \times 88^1 \pmod{187}] \pmod{187}$$

$$88^1 = 88 = 88 \pmod{187}$$

$$88^2 = 7\,744 = 77 \pmod{187}$$

$$88^4 = 59\,969\,536 = 132 \pmod{187}$$

$$88^7 = 88^1 \times 88^2 \times 88^4 = 88 \times 77 \times 132 = 894\,432 = 11 \pmod{187}$$

Bernard envoie alors à Alice le texte chiffré $C = 11$.

(8) Nous savons que les exponentielles en arithmétique modulo sont des fonctions à sens unique, aussi est-il très difficile de repartir de $C = 11$ pour retrouver le message original, M . Ève ne peut donc pas déchiffrer le message.

(9) Alice, au contraire, peut le déchiffrer, car elle dispose d'informations particulières : elle connaît les valeurs de p et de q . Elle calcule un nombre d , la clef de déchiffrement, encore appelée clef privée. Le nombre d est calculé selon la formule suivante :

$$e \times d = 1 \pmod{(p-1) \times (q-1)}$$

$$7 \times d = 1 \pmod{16 \times 10}$$

$$7 \times d = 1 \pmod{160}$$

$$d = 23$$

(Déduire la valeur de d n'est pas immédiat, mais l'algorithme d'Euclide permet à Alice de trouver d facilement et infailliblement).

(10) Pour décrypter le message, Alice applique les formules suivantes :

$$M = C^d \pmod{187}$$

$$M = 11^{23} \pmod{187}$$

$$M = [11^1 \pmod{187} \times 11^2 \pmod{187} \times 11^4 \pmod{187} \times 11^{16} \pmod{187}] \pmod{187}$$

$$M = 11 \times 121 \times 55 \times 154 \pmod{187}$$

$$M = 88 = X \text{ en ASCII}$$

Rivest, Shamir et Adleman avaient créé une fonction à sens unique particulière qui ne pouvait être inversée que par quelqu'un ayant une information spéciale, à savoir les valeurs de p et de q . Chaque fonction peut être personnalisée en choisissant p et q qui, multipliés l'un par l'autre, donnent N . La fonction permet à n'importe qui d'adresser des messages cryptés à une personne désignée en utilisant le N choisi par cette personne, mais seul le destinataire peut décrypter le message

puisque'il est le seul à connaître p et q , et donc le seul à connaître la clef de déchiffrement d .

Glossaire

Algorithme de chiffrement : processus d'opérations à effectuer pour le chiffrement, qui doit être lié à une clef qui le précise.

Alphabet chiffré : redistribution des lettres de l'alphabet usuel, qui permet ensuite de déterminer comment chaque lettre du message sera chiffrée. L'alphabet chiffré peut aussi se composer de nombres ou de n'importe quels autres caractères, mais, dans tous les cas, il impose de changer les lettres du message d'origine.

ASCII (American Standard Code for Information Interchange) : code standard américain pour l'échange d'information, qui traduit en nombres les caractères de l'alphabet et autres.

Carnet de code : liste d'équivalents qui remplaceront les mots ou les phrases du message d'origine.

Chiffre : n'importe quel système appliqué pour dissimuler le sens d'un message en remplaçant chaque lettre du message d'origine par une autre.

Chiffre décalé de César : à l'origine, chiffre par lequel chaque lettre d'un message est remplacée par la lettre figurant trois places plus loin dans l'alphabet. Plus généralement, chiffre qui remplace chaque lettre du message par une lettre x places plus loin dans l'alphabet, x étant un nombre de 1 à 25.

Chiffre de substitution : cryptosystème dans lequel chaque lettre du message est remplacée par un autre caractère, mais garde sa place dans le message.

Chiffre de transposition : cryptosystème dans lequel chaque lettre du message reste inchangée, mais mise à une autre place dans le message.

Chiffre de Vigenère : chiffre polyalphabétique qui fut inventé vers 1500. Le carré de Vigenère comporte 26 alphabets différents, chacun étant un alphabet décalé selon le chiffre de César, et un mot-clef établit quel alphabet chiffré sera utilisé pour crypter chaque lettre du message.

Chiffrer : transformer le message d'origine en message chiffré.

Clef : paramètre qui transforme l'application de l'algorithme général de chiffrement en le spécifiant. Généralement, l'ennemi peut connaître l'algorithme utilisé, mais il ne doit en aucun cas connaître la clef.

Clef asymétrique (cryptographie à) : forme de cryptographie dans laquelle la clef utilisée pour le chiffrement n'est pas la même que celle utilisée pour le déchiffrement. S'applique aux cryptosystèmes à clef publique, tel le RSA.

Clef privée : clef utilisée par le receveur pour décrypter les messages dans un cryptosystème à clef publique. La clef privée doit être tenue secrète.

Clef publique : clef utilisée par l'envoyeur pour crypter les messages dans un cryptosystème à clef publique. La clef publique est disponible pour tout le monde.

Clef publique (cryptographie à) : cryptosystème qui résout le problème de la distribution de clefs. La cryptographie à clef publique demande un chiffre asymétrique, afin que chacun puisse créer une clef publique de chiffrement et une clef privée de déchiffrement.

Clef symétrique (cryptographie à) : forme de cryptographie où la clef nécessaire pour crypter le message est la même que celle nécessaire pour le décrypter. Le terme recouvre toutes les formes traditionnelles de chiffrement, c'est-à-dire celles en usage avant les années 70.

Clefs (distribution des) : processus destiné à assurer à la fois à l'envoyeur et au receveur l'accès à la clef nécessaire pour crypter et décrypter un message, en évitant qu'elle ne tombe dans des

maines ennemies. La distribution des clefs était le problème majeur pour la logistique et la sécurité avant l'invention de la cryptographie à clef publique.

Code : système pour dissimuler le sens d'un message en remplaçant chaque mot ou phrase du message par un caractère ou un ensemble de caractères différents.

Coder : transformer le message d'origine en message codé.

Cryptanalyse : technique qui permet de déduire le texte en clair du texte chiffré, sans connaître la clef.

Crypter : chiffrer ou coder.

Cryptographie : technique du chiffrement d'un message, ou ensemble des méthodes utilisées pour cacher le sens d'un message. Le terme est souvent appliqué dans un sens plus général pour signifier la science des messages secrets, et est employé alors comme un synonyme de cryptologie.

Cryptographie quantique : forme infrangible de cryptographie fondée sur la théorie quantique, en particulier le principe d'incertitude qui établit l'impossibilité de mesurer simultanément tous les paramètres d'un objet. La cryptographie quantique garantit un échange sécurisé de suites aléatoires de bits, qui seront ensuite utilisées comme base pour un chiffre jetable.

Cryptologie : science de l'écriture secrète sous toutes ses formes, englobant à la fois la cryptographie et la cryptanalyse.

Déchiffrer : transformer un message chiffré en un message clair conforme à l'original. Ce terme s'applique en principe au destinataire qui connaît la clef nécessaire pour obtenir le texte en clair, mais on l'utilise aussi dans le cas d'un intercepteur ennemi qui opère le déchiffrement par la cryptanalyse.

Décoder : transformer un message codé en un message clair conforme à l'original.

Décrypter : déchiffrer ou décoder.

DES (Data Encryption Standard) : standard de chiffrement des données développé par IBM et adopté en 1976.

Distribution de clefs de Diffie-Hellman-Merkle : procédé dans lequel envoyeur et récepteur peuvent convenir d'une clef secrète par une conversation publique. La clef choisie, l'envoyeur peut utiliser un chiffre comme le DES pour crypter un message.

Longueur de clef : le chiffrement informatisé impose des clefs qui ont la forme de nombres. Parler de la longueur d'une clef, c'est faire référence au nombre de chiffres, ou bits, de cette clef, et cela permet de préciser aussi le plus grand nombre qui peut être utilisé comme clef, ce qui fixe également le nombre de clefs possibles. Plus la clef peut être longue (ou plus grand est le nombre de clefs possibles), plus longue sera la durée nécessaire à la cryptanalyse pour essayer toutes ces clefs.

Modèle de chiffrement à usage unique (parfois appelé masque jetable ou à clef une-fois) : seule méthode de chiffrement infrangible connue. Elle repose sur une clef aléatoire de même longueur que le message. Chaque clef doit être utilisée une fois et une seule.

NSA (National Security Agency) : département du ministère américain de la Défense, responsable de la sécurisation des communications américaines et de l'attaque des communications des autres pays.

Ordinateur quantique : ordinateur extrêmement puissant qui applique la théorie quantique, en particulier la théorie disant que chaque objet peut être dans différents états en même temps (superposition), ou qu'un objet peut être dans plusieurs univers à la fois. Si les scientifiques pouvaient produire l'ordinateur quantique sur une assez grande échelle, il détruirait toutes les sécurités assurées par les chiffres actuels, en dehors du chiffre jetable.

Pretty Good Privacy (PGP) : algorithme de chiffrement informatisé développé par Phil Zimmermann et basé sur le RSA.

RSA : premier système qui répondait aux nécessités de la cryptographie à clef publique, inventé par Ron Rivest, Adi Shamir et Leonard Adleman en 1977.

Séquestre de clef : schéma suivant lequel des copies de clefs privées sont déposées chez un tiers — l'agent du séquestre — qui les remettra aux représentants de la loi, sous certaines conditions, par exemple si l'ordre en est donné par un tribunal.

Signature digitale : méthode pour prouver l'authenticité d'un document électronique, souvent générée par l'auteur du document crypté avec sa clef privée.

Stéganographie : technique pour cacher l'existence d'un message, par opposition à la cryptographie qui en dissimule le sens.

Substitution homophonique (chiffre de) : chiffre qui offre plusieurs substitutions possibles pour chaque lettre du texte en clair. S'il y a, disons, six substitutions possibles pour la lettre *a*, ces six caractères ne représenteront que la lettre *a*. C'est une variante du chiffre de substitution monoalphabétique.

Substitution monoalphabétique (chiffre de) : chiffre de substitution où l'alphabet chiffré reste le même au cours de tout le chiffrement.

Substitution polyalphabétique (chiffre de) : chiffre de substitution où l'alphabet chiffré change au cours du chiffrement, comme dans le chiffre de Vigenère. Ce changement s'exécute selon une clef.

Texte chiffré : message obtenu après chiffrement.

Texte en clair : message original avant chiffrement.

Remerciements

Lorsque j'écrivais ce livre, j'ai eu le privilège de rencontrer certains des plus grands concepteurs et briseurs de codes vivants, depuis ceux qui ont travaillé à Bletchley Park jusqu'à ceux qui créent des chiffres qui participeront à l'âge de l'information. Je voudrais remercier Whitfield Diffie et Martin Hellman, qui ont pris le temps de me décrire leurs travaux lorsque je les ai rencontrés sous le soleil californien. De même, Clifford Cocks, Malcolm Williamson et Richard Walton m'ont beaucoup aidé lors de ma visite à un Cheltenham nuageux. En particulier, je suis reconnaissant à l'Information Security Group du Royal Holloway College qui m'a autorisé à assister aux cours du Master of Science sur la sécurité de l'information. Le professeur Fred Piper, Simon Blackburn, Jonathan Tuliani et Fauzan Mirza m'ont tous fait profiter d'utiles leçons sur les chiffres et les codes.

En Virginie, j'ai eu la chance d'être accompagné dans un circuit sur les traces du chiffre de Beale par Peter Viemeister, un spécialiste de ce mystère. De plus le Bedford County Museum et Stephen Cowart de la Beale Cypher and Treasure Association m'ont aidé dans mes recherches sur le sujet. Je suis également reconnaissant à David Deutsch et Michele Mosca, de l'Oxford Centre for Quantum Computation, à Charles Bennett et son groupe de recherche au laboratoire Thomas J. Watson d'IBM, à Stephen Wiesner, Leonard Adleman, Ronald Rivest, Paul Rothmund, Jim Gillogly, Paul Leyland et Neil Barrett.

Derek Taunt, Alan Stripp et Donald Davies m'ont raconté comment Bletchley Park avait vaincu Enigma et j'ai obtenu l'assistance du Bletchley Park Trust, dont les membres donnent régulièrement des conférences qui éclairent un certain nombre de points. Le Dr Mohammed Mrayati et le Dr Ibrahim Kadi m'ont révélé les lointaines percées faites par la cryptanalyse arabe, et ont eu la gentillesse de me communiquer leur documentation. Le périodique *Cryptologia* a publié des articles sur la cryptanalyse ainsi que sur d'autres sujets cryptographiques, et je voudrais remercier Brian Winkel de m'avoir envoyé des exemplaires de ces magazines.

J'encourage mes lecteurs à visiter le National Cryptologic Museum près de Washington, et les Cabinet War Rooms à Londres, et j'espère qu'ils seront aussi passionnés que je l'ai été par ces visites. Merci aux conservateurs et aux bibliothécaires de ces musées de m'avoir aidé dans mes recherches. Quand j'étais pressé par le temps, James Howard, Bindu Mathur, Pretty Sagoo, Anna Singh et Nick Shearing m'ont tous aidé à trouver des articles importants et intéressants, des livres et des documents, et je leur suis reconnaissant de leurs efforts. Merci aussi à Antony Buonomo à www.vertigo.co.uk, qui m'a aidé à créer mon site web.

Je me suis aidé de nombreux livres et articles. La bibliographie contient certaines de mes sources, mais elle est incomplète et ne constitue pas une liste de références exhaustive. Elle ne propose que des ouvrages qui peuvent intéresser un lecteur non spécialiste. Je voudrais en signaler un en particulier : *The Codebreakers*, de David Kahn. Ce livre retrace à peu près tous les événements cryptographiques à travers l'histoire, ce qui en fait une source inestimable.

Diverses bibliothèques, institutions et personnes privées m'ont procuré des photographies. Toutes les sources sont signalées dans les crédits photographiques, mais des remerciements particuliers vont à Sally McClain, qui m'a envoyé des photos de parleurs de code navajos ; au professeur Eva Brann, qui a découvert la seule photo d'Alice Kober ; à Joan Chadwick, qui m'a envoyé une photo de John Chadwick, et à Brenda Ellis qui m'a prêté des photos de James Ellis. Merci aussi à Hugh Whitemore, qui m'a autorisé à citer un extrait de sa pièce *Breaking the code*, basée sur le livre d'Andrew Hodges, *Alan Turing - The Enigma*.

Sur un plan personnel, je voudrais remercier amis et famille qui m'ont soutenu pendant les deux années où j'écrivais ce livre. Neil Boynton, Dawn Dzedzy, Sonya Holbraad, Tim Johnson, Richard Singh et Andrew Thompson m'ont tous aidé à ne pas devenir fou lorsque je me battais avec des concepts cryptographiques sophistiqués. En particulier, Bernadette Alves m'a apporté à la fois soutien moral et critique constructive. Mes remerciements vont aussi à toutes les personnes et institutions qui ont forgé ma carrière, dont Wellington School, Imperial College et le groupe High Energy Physics de l'université de Cambridge ; Dana Purvis, à la BBC, qui a permis mon premier passage à la télévision ; et Roger Highfield, du *Daily Telegraph*, qui m'a encouragé à écrire mon premier article.

Pour finir, j'ai eu la chance insigne de travailler avec des personnalités éditoriales comptant parmi les meilleures. Patrick Walsh est un agent qui a l'amour de la science, le souci de ses auteurs et un enthousiasme sans bornes. Il m'a mis en rapport avec les éditeurs les plus capables et les plus agréables, tout particulièrement Fourth Estate, dont le personnel a supporté superbement mes sollicitations constantes. Enfin — mais c'est, bien sûr, le plus important —, mes éditeurs, Christopher Potter, Leo Hollis et Peternelle van Arsdale, m'ont aidé à tracer un chemin très droit à travers un sujet qui multiplie tours et détours depuis des siècles. Je leur en suis extrêmement reconnaissant.

Éléments de bibliographie

La liste ci-dessous rassemble des livres abordables par la plupart de mes lecteurs. J'ai évité de donner des références par trop techniques, mais certains des ouvrages ci-dessous contiennent une bibliographie détaillée. Si vous souhaitez par exemple en savoir plus sur le déchiffrement du Linéaire B (chapitre 5), je vous recommande *Le déchiffrement du Linéaire B*, de John Chadwick. Cependant si, là encore, vous ne trouvez pas assez de précisions, les références qu'il cite vous les apporteront.

Il y a énormément d'éléments concernant les codes et les chiffres sur Internet. J'ai donc, en plus des livres, établi une liste de sites-web qui méritent une visite.

Ouvrages généraux

Kahn, David, *The Codebreakers*, Scribner, New York, 1996.

Newton, David E., *Encyclopedia of Cryptology*, ABC-Clio, Santa Barbara, 1997.

Smith, Lawrence Dwight, *Cryptography*, Dover, New York, 1943.

Beutelspacher, Albrecht, *Cryptology*, Mathematical Association of America, Washington, 1994.

Chapitre 1

Gaines, Helen Fouché, *Cryptanalysis*, Dover, New York, 1956.

Al-Kadi, Ibrahim A., « The origins of cryptology : The arab contributions », *Cryptologia*, vol. 16, no. 2, April 1992, pp. 97-126.

Fraser, Lady Antonia, *Mary, Queen of Scots*, Random House, London, 1989.

Smith, Alan Gordon, *The Babington Plot*, Macmillan, London, 1936.

Steuart, A. Francis (ed.), *Trial of Mary, Queen of Scots*, William Hodge, London, 1951.

Chapitre 2

Standage, Tom, *The Victorian Internet*, Weidenfeld & Nicholson, London, 1998.

Franksen, Ole Immanuel, *Mr Babbage's Secret*, Prentice-Hall, London, 1985.

Franksen, Ole Immanuel, « Babbage and cryptography. Or, the mystery of Admiral Beaufort's cipher », *Mathematics and Computer Simulation*, vol. 35, 1993, pp. 327-67.

Rosenheim, Shawn, *The Cryptographie Imagination*, Johns Hopkins University Press, Baltimore, 1997.

Poe, Edgar Allan, *The Complete Tales and Poems of Edgar Allan Poe*, Penguin, London, 1982.

Viemeister, Peter, *The Beale Treasure : History of a Mystery*, Hamilton's, Belford, 1997.

Chapitre 3

Tuchman, Barbara W., *The Zimmermann Telegram*, Ballantine, New York, 1994.

Yardley, Herbert O., *The American Black Chamber*, Aegean Park Press, Laguna Hills, 1931.

Chapitre 4

Hinsley, F.H., *British Intelligence in the Second World War : Its Influence on Strategy and Operations*, HMSO, London, 1975.

Hodges, Andrew, *Alan Turing : The Enigma*, Vintage, London, 1992.

Kahn, David, *Seizing the Enigma*, Arrow, London, 1996.

Hinsley, F.H., et Stripp, Alan (eds), *the Codebreakers : The Inside Story of Bletchley Park*, Oxford University Press, Oxford, 1992.

Smith, Michael, *Station X*, Channel 4 Books, London, 1999.

Harris, Robert, *Enigma*, Arrow, London, 1996.

Chapitre 5

Paul, Doris A., *The Navajo Code Talkers*, Dorrance, Pittsburgh, 1973.

McClain, Sally, *The Navajo Weapon*, Books Beyond Borders, Boulder, 1994.

Pope, Maurice, *The Story of Decipherment*, Thames & Hudson, London, 1975.

Davies, W.V., *Reading the Past : Egyptian Hieroglyphs*, British Museum Press, London, 1997.

Chadwick, John, *The Decipherment of Linear B*, Cambridge University Press, Cambridge, 1987.

Chapitre 6

Data Encryption Standard, FIPS Pub. 46-1, National Bureau of Standards, Washington, 1987.

Diffie, Whitfield, et Hellman, Martin, « New directions in cryptography », *IEEE Transactions on Information Theory*, vol. IT-22, November 1976, pp. 644-54.

Gardner, Martin, « A new kind of cipher that would take millions of years to break », *Scientific American*, vol. 237, August 1977, pp. 120-24.

Hellman, M.E., « The mathematics of public-key cryptography », *Scientific American*, vol. 241, August 1979, pp. 130-39.

Schneier, Bruce, *Applied Cryptography*, John Wiley & Sons, New York, 1996.

Chapitre 7

Zimmermann, Philip R., *The Official PGP User's Guide*, MIT Press, Cambridge, 1996.

Garfinkel, Simson, PGP : *Pretty Good Privacy*, O'Reilly & Associates Sebastopol, 1995.

Bamford, James, *The Puzzle Palace*, Penguin, London, 1983.

Koops, Bert-Jaap, *The Crypto Controversy*, Kluwer, Boston, 1998.

Diffie, Whitfield, et Landau, Susan, *Privacy on the Line*, MIT Press, Cambridge, 1998.

Chapitre 8

Deutsch, David, *The Fabric of Reality*, Allen Lane, London, 1997.

Bennett, C.H., Brassard, C., et Ekert, A., « Quantum Cryptography », *Scientific American*, vol. 269, October 1992, pp. 26-33.

Deutsch, D., et Ekert, A., « Quantum computation », *Physics World*, vol. 11, no. 3, March 1998, pp. 33-56.

Quelques livres disponibles en français

David Kahn, *La guerre des codes secrets*, InterÉditions, Paris, 1980.

Douglas Stinson, *Cryptographie, Théorie et Pratique*, International Thomson Publishing, France, Paris, 1997.

Bruce Schneier, *Cryptographie appliquée*, International Thomson Publishing, France, Paris, 1997.

Jacques Stern, *La Science du secret*, Odile Jacob, Paris, 1998.

Sites Internet

The Mystery of the Beale Treasure

<http://www.roanokeva.com/ttd/stories/beale.html>

Bletchley Park

<http://www.cranfield.ac.uk/cc/bpark/>

The Alan Turing Homepage

<http://www.turing.org.uk/turing/>

Enigma emulators

http://www.attlabs.att.co.uk/andyc/enigma/enigma___j.html

<http://www.izzy.net/-ian/enigma/applet/index.html>

Phil Zimmermann and PGP

<http://www.nai.com/products/security/philphil.asp>

Electronic Frontier Foundation

<http://www.eff.org/>

Centre for Quantum Computation

<http://www.qubit.org/>

Information Security Group, Royal Holloway College

<http://isg.rhbnc.ac.uk/>

National Cryptologic Museum

<http://www.nsa.gov> :8080/museum/

American Cryptogram Association (ACA)

<http://www.und.nodak.edu/org/crypto/crypto/>

Cryptologia

<http://www.dean.usma.edu/math/resource/pubs/cryptolo/index.htm>

Cryptography Frequently Asked Questions

<http://www.cis.ohio-state.edu/hypertext/faq/usenet/cryptography-faq/top.html>

RSA Laboratories' Frequently Asked Questions About Today's Cryptography

<http://www.rsa.com/rsalabs/faq/html/questions.html>

Yahoo ! Security and Encryption Page

<http://www.yahoo.co.uk/Computers-and-Internet/Security-and-Encryption/>

Crypto Links

<http://www.ftech.net/monark/crypto/web.htm>

INDEX

Les numéros de pages renvoyant aux figures et tableaux apparaissent en italique.

A

Abhorchdienst (service d'écoutes allemand)

Abou Simbel, temple d' - (Égypte)

ABU BAKR, calife

Adab-al-Kuttab

ADAIR Gilbert

ADFGVX, code

ADLEMAN Leonard

Agnus Dei (Agnès), « bombe » de A. Turing

AHERN Bertie

akkadien, langue

ALBERT, prince

ALBERTI Léon Battista

ALEXANDER C.H.O'D.

Alexander Weekly Messenger

ALEXANDRE LE GRAND

algorithme

ALI, calife

Al-Kindi, Abu Yusef Ya'qub ibn Is-haq ibn as-Sabbah ibn omran ibn Ismail

American Escrowed Encryption Standard

American Journal of Archeology

ANNE BOLEYN, reine d'Angleterre

archéologie *passim*

ARISTAGORAS DE MILET

ARISUE lieutenant-général Seizo

ARPA (Advanced Research Projects Agency, USA)

ARPANet, réseau

« Art, L' - », poème de Th. Gautier

ASCII (American Standard Code for Information Interchange)

Association pour le chiffre et le trésor de Beale

atbash (chiffre hébreu)

AT&T Bell, Laboratoires

Aum Shinrikyo, secte

B

BABBAGE Benjamin

BABBAGE Charles

BABINGTON Anthony

BABOU Philibert

BACON Roger

BAKE Jr, caporal Henry

BAKHTIAR Chapour

BALFOUR Arthur

Baltimore Technologies, société

BANKES W.J.
BAUGH William
BAZERIES commandant Étienne
BEALE Thomas J. chiffre de
Beale Papers, The
BENALLY John
BENNETT Charles
BÉRÉNICE, reine d'Égypte
BERNSTORFF von
Bible, La
Bible Code, The, de M. Drosnin
BIRCH Frank
bits, voir nombres binaires
Biuro Szyfrow (Pologne)
BLEGEN Carl
Bletchley Park, centre de (Angleterre)
Boers, guerre des
« bombes » : de Rajewski de Turing
BOHR Niels
BOTHWELL James HEPBURN, comte de -
BRAILLE Louis
BRANN Eva
BRASSARD Gilles
Breaking the Code, de H. Whitemore
BREJNEV Leonid
British Tabulating Machinery, usine
BULONDE général Vivien de
Bureau du chiffre américain
Bureau du chiffre français
Bureau 40 (de l'Amirauté britannique)

C

cabinets noirs

calculateurs

Cali, cartel de

CAMDEN William

Capstone (cryptosystème)

Captain Midnight, feuilleton radiophonique

CARAMAN Philippe

CARDAN Jérôme

CATHERINE D'ARAGON, reine d'Angleterre

CECIL William

Center for Democracy and Technology

CÉSAR Jules chiffre de -

CHADWICK John

CHAMBERLAIN Neville

CHAMPOLLION Jean-François

CHAUCER Geoffrey

« chevaux de Troie »

chiffre alphabétique du livre de substitution de transposition

Chiffrierstelle, bureau (Allemagne)

Choctaws, peuple

CHURCHILL Sir Winston

CICÉRON

CIEZKI capitaine Maksymilian

cillies (*messages prévisibles*)

clef(s) aléatoire asymétrique chiffrement de la *-passim* ; distribution
des - jetable (clef-une-fois) longueur de la - privée
publiquerecouvrement des - séquestre des - - symétrique

CLÉMENT VII, pape

CLÉOMÈNE

CLÉOPÂTRE, reine d'Égypte

CLINTON Bill

clipper (cryptosystème)

COCKS Clifford

COCKS Gill

code

Codebreakers, The, de D. Kahn

codographe

Colossus, machine anglaise

Commission nationale de contrôle des interceptions de sécurité
(France)

COMSEC (Communications Security, USA)

CONAN DOYLE Sir Arthur

CONNER major général Howard

COOKE William Fochergill

copte, langue

Coran, Le

courrier duœur

cribs (mots probables)

Crimée, guerre de -

criminalité

CROWELL William

cryptanalyse : *passim*

Crypto AG, société

cryptographie : définition et liberté quantique

Cryptographie militaire, La, de A. Kerckhoffs Van Nieuwenhof

CUKIER Niel

D

DACIER M.

Daily Telegraph, The

DAMM Arvid

DARCY Lord

DARNLEY Henry STEWART, comte de

DARPA (Agence des projets de recherche avancée de la Défense Américaine)

DATO Leonardo

Débarquement du 6 juin 1944

Déchiffrement du Linéaire B, Le, de J. Chadwick

Déclaration d'indépendance américaine

Déclaration universelle des Droits de l'homme

DEMARATUS

démotique (écriture)

DENNING Dorothy

DENNISON commandant Alastair

Département américain de la Défense voir Pentagone

De Re Aedificatoria, de L.B. Alberti

DES (Data Encryption Standard), chiffre

DEUTSCH David

Différence Engine N° 1, machine

Différence Engine N° 2, machine

DIFFIE Whitfield : le système Diffie-Hellman-Merkle

DIODORE DE SICILE

Disparition, La, de G. Perec

disque à chiffrer

Documents in Mycenaean Greek, de J. Chadwick et M. Ventris

DÖNITZ amiral Karl
DROSNIN Michel
DUMAS Alexandre

E

EASTLAND James
Échelon, système d'écoutes
ECKARDT von -
ECKERT J. Presper
écoutes téléphoniques
EDISON Thomas
EDOUARD VI, roi d'Angleterre
Égypte des pharaons, L', de J.-F. Champollion
Electronic Frontier Foundation
ELISABETH I^{re}, reine d'Angleterre
ELISABETH TUDOR
ELLIS James
ELTSINE Boris
e-mail problèmes de sécurité signatures
ÉNÉE LE TACTICIEN
ENIAC, machine
Enigma, machine allemande navale
Enemy of the State, film
escrow-key
EVANS Sir Arthur
Évidence d'un dialecte grec dans les archives mycéniennes, de J. Chadwick et M. Ventries

F

factorisation

FBI (Federal Bureau of Investigation)

FEISTEL Horst

Ferranti, société

FISCHER Mary

FISCHER Mel

FLAMSTEED John

FLEMING Ian

FLOWERS Tommy

flux, analyse des -

fonctions mathématiques à sens unique l'arithmétique modulo

FOURIER Jean-Baptiste

FRANÇOIS I^{er}, roi de France

FRANÇOIS II, roi de France

FRANKLIN Benjamin

FREEH Louis J.

fréquences, analyse des

FRICKE amiral Kurt

FRIEDMAN colonel William

G

GANDHI Mahatma

GARDNER Martin

GARFINKEL Simon

GAUTIER Théophile
GC&CS (Government Code and Cypher School, Angleterre)
GCHQ (Government Communications Headquarters, Angleterre)
Geheime Kabinets-Kanzlei (Autriche)
Geheimschriften und die Dechiffirkunst, Die, de F.W. Kasiski
GENDRON Victor
GEORGEL Abbot
GIFFORD Gilbert
GILLOGLY James
GÖDEL Kurt
GOOD Jack
GORBATCHEV Mikhaïl
GÖRING Hermann
Grand Chiffre (de Louis XIV)
GREY Nigel de
GROTEFEND Georg
GROVER Lov
Guadalcanal, bataille de—(1942)
GUDERIAN général Heinz
Guerre des Gaules, La, deésar
Guerre mondiale, Première
Guerre mondiale, Seconde
GUILLAUME II, empereur d'Allemagne
GUILLAUME D'ORANGE
GUISE Marie de
GUITRY Sacha

H

HACKMAN Gene

Hadith

HALL amiral Sir William

HAMMER Carl

HAFSA

Handbuch der Kryptographie, de Wostrowitz

HARDY G.H.

HAROCHE Serge

HART Clayton et George

HEBERN Edward

HEISENBERG Werner

HELLMAN Martin

HENRIETTE, reine d'Angleterre

HENRY VIII, roi d'Angleterre

HERBERT, Jr, Hiram

HÉRODOTE

HERSCHELL, John

hiératique (écriture)

hiéroglyphes cryptés

HILTON Peter

HINSLEY Sir Harry

HISTAÏAEUS

Histoire du déchiffrement, de M. Pope

Histoires, d'Hérodote

HITLER Adolf

HODGES Andrew

HOMÈRE

Hommes dansants, Les, de A. Conan Doyle

HOOVER Herbert

HORNER capitaine E.W.

HUGO Victor

I

IBM, société

IDEA, chiffre

Illiade, d'Homère

indécidabilité

Indus (écriture)

Internet le commerce sur les virus

Iwo-Jima, bataille de -

J

JACQUES V, roi d'Écosse

JACQUES VI, roi d'Écosse

JANCIK Joseph

JOHNSON Lyndon B.

JOHNSTON Philipp

JONES lieutenant-colonel James E.

JONES Sir Henry

Journal of the Society of Arts

K

KAHN David

Kaiser *voir* GUILLAUME II

Kàma-sùtra

Karnak, temple de - (Égypte)

KASISKI Friedrich Wilhelm

KEILLOR Garrison

KENNEDY John F.

KENNEDY Robert

KERCKHOFFS VAN NIEUWENHOF Auguste prince de -

KINDI Abu Yusuf al-

KING amiral Ernest

KING Martin Luther

KIRBY Rollin

KIRCHER Athanasius

KIRK George H.

KOBER Alice

KOCH Alexander

KONHEIM Alan

Kriegsmarine

KRUH Louis

L

LANGER major Gwido

LENOIR Alexandre

LÉON Sir Herbert

LÉONIDAS

Lettre sur les œuvres d'art et sur la nullité de la magie, de R. Bacon

Linéaire A (écriture)

Linéaire B (écriture)
Lorenz, chiffre de -
Los Alamos, laboratoire national de - (USA)
Louis XIII, roi de France
Louis XIV, roi de France
Louis XV, roi de France
Louvois François LE TELLIER, marquis de
Lucifer (chiffre)
Luftwaffe

M

MAHOMET
MÀMUN Al -, calife
MANUELITO Johnny
Manuscrit sur le déchiffrement des messages cryptographiques, de al-Kindi.
MARCONI Guglielmo
MARNIX Philippe van
MARIE STUART, reine d'Écosse
Masque de Fer, énigme du -
Mathematician's Apology, The, de G.H. Hardy
Mathias Sandorff, de J. Verne
MATSEN Wayne
MAUBORGNE major Joseph
MAUCHLY John W.
McCABE William
McKAY Brendan

MENZIES Sir Stewart
Menwith Signals Intelligence Base (Yorkshire)
Mercury Rising, film
MERKLE Ralph
micropoint
Midway, bataille de - (1942)
Mille et Une Nuits, Les
MILNER-BARRY Stuart
MINOS, roi de Crète
Minotaure
MIT (Massachusetts Institute of Technology)
Moby Dick, de H. Melville
modulo, arithmétique
monnaie quantique
MONTGOMERY révérend
MORAY comte de -
MORCOM Christopher
MORRISS Robert
MORSE Samuel
Morse, code
mots croisés
mots probables
MUGGERIDGE Malcolm

N

NAPOLÉON I^{er}, empereur
National Bureau of Standards (USA)

Navajo, code

Navajo, peuple

Navajo Code-Talkers, The, de. Paul

Network Associates, société

New Kind of Cipher that Would Take Millions of Years to Break, A, de M. Gardner

NEWMAN Max

NEWTON Isaac

NIMITZ amiral Chester

NIXON Richard

nombres binaires

nomenclature

Note, de M. Ventris

NSA (National Security Agency, USA)

nuls, signes

O

Odyssée, d'Homère

Ædipus aegyptiacus, de A. Kircher

On Computable Numbers, de A. Turing

« Opération Sans-Pitié »

ordinateurs, chiffrement par — naissance des quantiques et transmission de la clef utilisation des nombres binaires

OTHMAN, calife

P

Pacifique, guerre du —

PAGE Denys

PAINVIN lieutenant Georges

PALMERSTON Lord Henry TEMPLE

PARSONS Marilyn

parleurs de code (navajos)

PATTERSON Nick

PAUL Doris

PAULET Sir Amyas

Pentagone

PEREC Georges

PGPfone

PGP (Pretty Good Privacy), système

Phaistos, disque de

PHARNABAZE DE PERSE

PHELIPPES Thomas

PHILIPPE II, roi d'Espagne

Philosophie du déchiffrement, La, de Ch. Babbage

phonogrammes

photons polarisation des

PIE, pape

Pierre de Rosette

Pigpen, chiffre

piqûres d'épingle

PLAYFAIR baron Lyon chiffre de

PLINE L'ANCIEN

POE Edgar Allan

POPE Maurice

PORTA Giovanni

Précis du système hiéroglyphique, de J.-F. Champollion

PRINTEMPS Yvonne

Problèmes pour une théorie ambitieuse de la cryptographie, de W. Diffie

PROBUS Valerius

PTOLÉMÉE, pharaon

Purple, machine japonaise

Q

quantique, théorie et cryptographie monnaie et ordinateurs rôle des photons dans la la superposition les univers parallèles

Quarterly Review

qubits

R

radio

RAF (Royal Air Force)

RAMSÈS, pharaon

REAGAN Ronald

REJEWSKI Marian

« REX » (agent français)

RICCIO David

RIDLEY capitaine

RIPS Eliyahu

RITTER Richard

RIVEST Ron fonction de

ROGERS Daniel
ROSENBERG Yoav
ROSSIGNOL Antoine et Bonaventure
Royal Navy
RSA, chiffre
RSA Data Security Inc., société
RUSSELL Bertrand

S

SADATE Arouar al-
SAGAN Carl
Salamine, bataille de
Scarabée d'or, Le, de E.A. Poe
SCHERBIUS Arthur
Scherbius et Ritter, société
SCHLIEMANN Heinrich
SCHMIDT Hans-Thilo
SCHMIDT Rudolph
SCHRODINGER Erwin
Scientific American, The
SCUDAMORE John
scytale
Sécession, guerre de
Seizing the Enigma, de. Kahn
Sénat américain
SHAMIR Adi
SHOR Peter

SIDNEY Sir Philipp
SIGABA (ou M-143-C), machine américaine
SITTIG Ernst
SIXTE, pape
SMITH Will
SMOLIN John
Society of Worldwide International Financial Telecommunication
SORO Giovanni
Spycatcher, de P. Wright
Sphynx du Sans-Fil, Le, machine
stéganographie
STIMSON Henry
substitution homophonique monoalphabétique polyalphabétique
SUÉTONE
SZAO, machine de Lorenz.

T

TAWELL John
Télégramme de Zimmermann, Le, de B. Tuchman
télégraphe
tempest-attack
Théorie ondulatoire de la lumière, La, de Th. Young
THWAITES John Hall Brock
tiers de confiance
TILTMAN John
Times, The, quotidien
trafic, analyse de —

Traicté des chiffres, de B. de Vigenère

Traité de l'Astrolabe, de G. Chaucer

transposition

TRAVIS commandant Edward

Trésor de Beale, Le, de P. Viemeister

TRITHÈME Jean

TROTSKYéon

TUCHMAN Barbara

TURING Alan machine universelle de machines de « bombes » de

TURING Ethel

TURING Julius

TUTTE Bill

TWINN Peter

Typex, machine anglaise

U

Ultra

Ultra Secret, The, de F.W. Winterbotham

UMAR, calife

V

VÀTSYÀYANA

VENTRIS Michael

Verisign, société

VERNE Jules

Vicomte de Bragelonne, Le, d'A. Dumas

Victoire (« bombe » de A. Turing)

VIEMEISTER Peter

Vies des douze Césars, de Suétone

VIÈTE François

VIGENÈRE Blaise de carré de chiffre de
virus

VOLTAIRE

Voyage au centre de la terre, de J. Verne

W

WACE A.J.B.

WALSINGHAM Sir Francis

WALTON Richard

WARD James B

Wassenaar, amendement (1998)

WELCHMAN Gordon

WHEATSTONE Sir Charles

WHITE Nicolas

WHITEHEAD Alfred N.

WHITEMORE Hugh

WIESNER Stephen

WILLIAMSON Malcolm

WILLIS Bruce

WILSON Woodrow

WINGFIELD Richard

WINTERBOTHAM capitaine F.W.

WITSUM Doron

WITTGENSTEIN Ludwig

World Crisis, The, de W. Churchill

WOSTROWITZ

WRIGHT Peter

X

XERXÈS, roi de Perse

Y

YAMAMOTO amiral Isoruko

YARDLEY Herbert O.

YOUNG Thomas Fentes de

YOUSEF Ramsey

Z

ZIMMERMANN Arthur télégramme de

ZIMMERMANN Phil

Crédits photographiques

Illustrations au trait de Miles Smith-Morris.

Hiéroglyphes reproduits avec l'autorisation des Presses du British Museum. Caractères du Linéaire B reproduits avec l'autorisation de Cambridge University Press.

[Fig. 1](#) Scottish National Portrait Gallery, Edimbourg ; [Fig. 6](#) Ibrahim A. Al-Kadi et Mohamed Mrayati, King Saud University, Riyad ; [Fig. 9](#) Public Record Office, Londres ; [Fig. 10](#) Scottish National Portrait Gallery, Edimbourg ; [Fig. 11](#) Cliché Bibliothèque Nationale de France, Paris ; [Fig. 12](#) Science and Society Picture Library, Londres ; [Fig. 20](#) et [25](#) *The Beale Treasure — History of a Mystery* par Peter Viemeister ; [Fig. 26](#) Collection David Kahn, New York ; [Fig. 27](#) Bundesarchiv, Coblenz ; [Fig. 28](#) National Archives, Washington ; [Fig. 29](#) General Research Division, The New York Public Library, Londres ; [Fig. 31](#) et [32](#) Collection Luis Kruh, New York ; [Fig. 38](#) Collection David Kahn, New York ; [Fig. 39](#) et [40](#) Science and Society Picture Library, Londres ; [Fig. 41](#) et [42](#) Collection David Kahn, New York ; [Fig. 43](#) Imperial War Museum, Londres ; [Fig. 44](#) et [45](#) Collection personnelle Barbara Eachus ; [Fig. 47](#) Agence Godfrey Argent, Londres ; [Fig. 50](#) Imperial War Museum, Londres ; [Fig. 51](#) Telegraph Group Limited, Londres ; [Fig. 52](#) et [53](#) National Archives, Washington ; [Fig. 54](#) et [55](#) British Museum Press, Londres ; [Fig. 56](#) Louvre, Paris © Photo RMN ; [Fig. 58](#) Department of Classics, University of Cincinnati ; [Fig. 59](#) Collection personnelle Eva Brann ; [Fig. 60](#) D.R. ; [Fig. 61](#) Collection personnelle Joan Chadwick ; [Fig. 62](#) Sun Microsystems ; [Fig. 63](#) Stanford, University of California ; [Fig. 65](#) RSA Data Incorporated ; [Fig. 66](#) Collection personnelle Brenda Ellis ; [Fig. 67](#) Collection personnelle Clifford Cocks ; [Fig. 68](#) et [69](#) Collection personnelle Malcolm Williamson ; [Fig. 70](#) Network Associates, Incorporated ; [Fig. 72](#) Penguin Books, Londres ; [Fig. 75](#) Laboratoire IBM Thomas J. Watson.