INTRODUCTION

UNE INTRODUCTION À

LA CRYPTOLOGIE

L'art des codes secrets

Philippe Guillot

edp sciences

Collection « Une Introduction à »
dirigée par Michèle Leduc et Michel Le Bellac

La cryptologie

L'art des codes secrets

Philippe Guillot

17, avenue du Hoggar
Parc d'activités de Courtabœuf, BP 112
91944 Les Ulis Cedex A, France

Dans la même collection

Les atomes froids
Erwan Jahier, préface de M. Leduc

Le laser
Fabien Bretenaker et Nicolas Treps, préface de C. H. Townes

Le monde quantique
Michel Le Bellac, préface d'A. Aspect

Les planètes
Thérèse Encrenaz, préface de J. Lequeux

Naissance, évolution et mort des étoiles
James Lequeux

La fusion thermonucléaire contrôlée
Jean-Louis Bobin

Le nucléaire expliqué par des physiciens
Bernard Bonin, préface d'É. Klein

Mathématiques des marchés financiers
Mathieu Le Bellac et Arnaud Viricel, préface de J.-Ph. Bouchaud

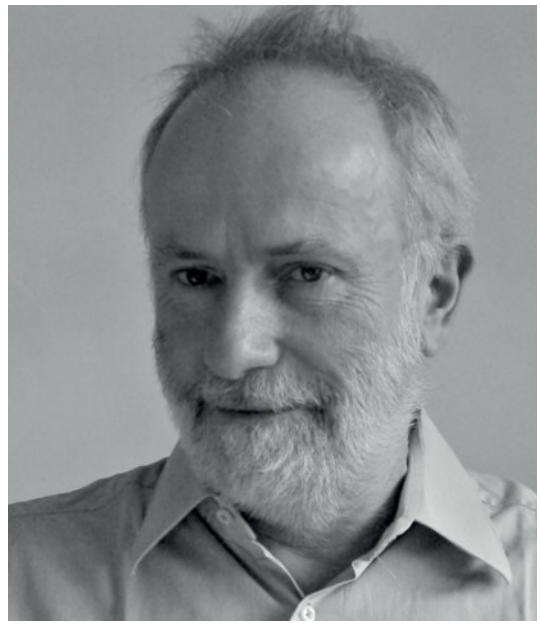
Physique et biologie
Jean-François Allemand et Pierre Desbiolles

Retrouvez tous nos ouvrages et nos collections sur
http://www.edition-sciences.com

Illustration de couverture : Clément Doranlo

Imprimé en France.

ISBN 978-2-7598-0811-3



Né en 1956, Philippe Guillot a été ingénieur de recherche en cryptologie à Thomson-CFS à partir de 1990. Il est devenu chef du laboratoire de cryptologie de Thales jusqu'en 2001, puis responsable du pôle sécurité de Canal-Plus Technologies de 2001 à 2003. Depuis 2003, il est maitre de conférences à l'Université Paris 8 en charge des cours de cryptologie, d'histoire de la cryptologie et d'algorithmique algébrique dans le master « mathématiques fondamentales et protection de l'information ».

This page intentionally left blank

Table des matières

Préface

La numérisation massive des données et le développement des réseaux de communication ont rendu possibles certains traitements automatisés auparavant inimaginables. En une fraction de seconde, le médecin peut désormais accéder à l'ensemble du passé médical et des résultats d'analyses de son patient ; le policier peut retrouver le nom d'un suspect à partir de son ADN ; un client peut consulter la liste des opérations effectuées sur son compte en banque et donner un ordre de virement depuis son téléphone mobile. Mais un individu mal intentionné peut aussi usurper l'identité d'un client et effectuer un virement en son nom ; il peut tenter d'obtenir des informations sur l'état de santé d'une personnalité connue, établir et rendre publiques des listes de patients atteints de maladie grave ou manipuler des dizaines de milliers de dossiers médicaux pour dissimuler les effets secondaires d'un traitement.

Si les technologies impliquées sont nouvelles, cette situation ne l'est évidemment pas : l'apparition de nouvelles techniques et l'ouverture d'un champ de possibilités inédit vont généralement de pair avec de nouveaux risques. En même temps que les avions sont apparus les accidents aériens et les pirates de l'air… Fort heureusement, le législateur, les scientifiques et les ingénieurs ont établi de nombreux garde-fous : les comportements répréhensibles sont punis par la loi, certaines opérations sont rendues techniquement impossibles. Mais ces solutions ne sont pas toutes parfaites et tous les risques ne peuvent pas être évités. Il ne faut pas pour autant tomber dans un rejet en bloc de ces technologies par peur du danger, réaction tout aussi absurde qu'une utilisation systématique sans évaluation critique des conséquences éventuelles. Comme dans tout autre domaine, le citoyen a besoin d'être conscient des garanties offertes par un système, et des risques encourus. Peut-être encore plus que dans tout autre domaine, un système informatique n'est socialement acceptable que s'il recueille la confiance des citoyens, et la confiance ne peut être établie que par la connaissance. Cette connaissance ne doit en aucun cas être réservée à quelques informaticiens ou férus de mathématiques au prétexte qu'ils seraient les seuls capables d'appréhender la complexité du domaine. Il ne s'agit pas que chacun maîtrise tous les détails

du fonctionnement de sa carte bancaire, mais qu'il comprenne ses fonctionnalités, les garanties qu'elle offre et celles qu'elle n'offre pas. Un patient qui doit subir une opération chirurgicale n'a nul besoin de savoir manier un bistouri, mais il est souhaitable qu'il sache à quoi sert une anesthésie. De la même façon, il est important que tout citoyen apprenne que les techniques permettant de protéger nos données et communications n'ont pas toutes les mêmes fonctionnalités, qu'elles n'offrent pas toutes la même sécurité et qu'elles ont bien sûr des limites.

C'est à cette œuvre salutaire que s'est attelé Philippe Guillot. Il a su brosser un panorama détaillé des techniques cryptologiques, de leurs applications et de leurs limites, qui ne soit pas un cours de troisième cycle universitaire, mais un ouvrage accessible à un large public. Pour autant, cet ouvrage ne se cantonne pas dans la présentation des procédés les plus simples, comme le RSA. Il évoque les techniques utilisées en pratique qui sont pourtant négligées par bien des auteurs, au prétexte qu'elles seraient moins élégantes, plus complexes ou trop récentes. Philippe Guillot parvient ainsi à donner une vue d'ensemble de la cryptologie qui est à la fois réaliste puisqu'elle englobe les méthodes employées dans la plupart des applications, et accessible. Par ses qualités pédagogiques hors du commun, il réussit même à familiariser le lecteur novice avec la sécurité physique des cartes à puce ou avec des concepts mathématiques aussi avancés que l'appariement de Weil. La lecture de cet ouvrage permettra ainsi à chacun de comprendre pourquoi aucun des procédés cryptographiques utilisés en pratique n'est parfaitement sûr, pourquoi la taille d'une clef cryptographique dépend fortement du système employé, ou comment les paramètres d'un système doivent évoluer au fil du temps pour prendre en compte l'augmentation de la puissance des ordinateurs. Elle apportera un éclairage indispensable à qui veut appréhender avec un esprit critique la mise en place de nouvelles téléprocédures, le déploiement de vastes systèmes d'information de santé ou de machines à voter.

Anne Canteaut,
directrice de recherche,
Inria Paris-Rocquencourt

Avant-propos

Alice aime son travail de paysagiste dans l'entreprise Thagem où elle doit aménager l'environnement de travail des mille cinq cents employés du site de Palombes-sur-Seine. L'essentiel de son activité est en plein air. C'est le printemps, les bouleaux lâchent leur pollen, et tout irait pour le mieux sans ce maudit rhume des foins qu'elle traîne depuis son adolescence. Ce soir en quittant le travail, il faudra qu'elle passe voir son médecin pour se faire prescrire un traitement anti-allergique.

En descendant les escaliers de son appartement parisien, elle allume son téléphone mobile :

– Allô, docteur Maison ? Puis-je passer vous voir cette après-midi vers 17 h 30 ?

Le rendez-vous est rapidement pris. La journée commence bien. Elle croise sans le remarquer le facteur venu déposer le courrier dans le hall de son immeuble et s'engouffre dans le métro, passe machinalement son sac à main le long du tourniquet et pense déjà aux aventures du commissaire Evenberg, héros du roman qu'elle a commencé avant-hier et qui lui fera passer plus vite son trajet.

Après avoir présenté son badge aux tourniquets d'accès de Thagem, son esprit commute déjà sur ses tâches de la journée. Elle démarre la fourgonnette de service pour aller prendre livraison des nouveaux rosiers destinés à agrémenter les abords du lac artificiel, fierté du directeur, et qui a obtenu un prix du meilleur environnement d'entreprise de la région.

À midi, elle vérifie le solde de la carte Moneix qui lui permet de payer le repas sans avoir à se préoccuper de faire l'appoint aux caisses. 1€ 23. Elle doit la recharger.

La journée passe vite. Elle repasse le tourniquet vers la sortie. C'est l'heure de son rendez-vous chez le médecin. Il fait beau. Elle décide de prendre un vélo en libre service avec son passe Circulo.

Elle avait oublié le changement d'adresse du docteur Maison ! Sans se démonter, elle télécharge l'application de navigation sur son téléphone qui lui indiquera la nouvelle adresse et l'itinéraire pour arriver à l'heure.

– Puis-je avoir votre carte Vitalix ?

Alice se laisse ausculter, et se réjouit d'avance à l'idée de soulager son nez bouché, ses démangeaisons et l'irritation insupportable de ses yeux.

– Vous n'avez qu'une sévère allergie au pollen, je n'ai rien remarqué d'autre, vous prendrez du Rhumactine en cas de production nasale abondante.

Alice sourit intérieurement en pensant au vocabulaire médical.

– Cela fera vingt-trois euros.

– Acceptez-vous la carte bancaire ?

– Oui, je préfère même ! Avoir moins d'espèces dans mon cabinet me rassure. Je me suis déjà fait braquer.

De retour dans son appartement, elle branche son ordinateur en se souvenant soudain qu'aujourd'hui est la date limite pour valider la déclaration de revenus du foyer.

« Une mise à jour est disponible pour votre ordinateur, télécharger ? »

– Encore !

Elle accepte la mise à jour, l'ordinateur redémarre. Enfin elle valide la déclaration des revenus.

Elle en profite pour commander sur Mississipi.fr la suite des aventures du commissaire Evenberg qui viennent de paraître.

C'est fini pour les préoccupations de la journée. Il est temps de se détendre avec Bob en allumant le téléviseur. Il y a au programme un bon film du cinéma italien des années soixante-dix sur la chaîne thématique à laquelle ils sont abonnés.

Cette tranche de vie fait intervenir pas moins de quinze situations au cours desquelles ont été menées une ou plusieurs opérations cryptologiques. Ceci illustre à quel point ce domaine a, en quelques années, envahi notre quotidien, sans que nous en ayons toujours pleinement conscience. Le lecteur est invité à identifier ces situations avant de consulter la solution page 173.

La cryptologie, née du besoin de transmettre des messages au seul destinataire autorisé, et dont le sens reste caché au messager et à quiconque pourrait l'intercepter, rassemble aujourd'hui un ensemble de méthodes destinées à protéger toute information contre une observation ou une intrusion malveillante.

En raison de la sensibilité des informations échangées, les milieux militaires et gouvernementaux sont naturellement intéressés à l'utilisation de la cryptologie. Avec l'essor des réseaux de télécommunication et la banalisation des données enregistrées, ces problèmes de sécurité concernent un ensemble de plus en plus large de la population.

Le développement de l'internet n'a été rendu possible qu'avec la confiance apportée par les moyens de protection des informations qu'il véhicule. Alors que jusqu'en 1998, l'utilisation des moyens cryptologiques était un monopole d'État, ces moyens ayant le statut d'arme de guerre, au même titre que les munitions et les explosifs, aujourd'hui, « l'usage des moyens de cryptologie est libre », comme il est stipulé dans l'article 30 de la loi pour la confiance dans l'économie numérique du 21 juin 2004.

Une connaissance des procédés mis en œuvre devient nécessaire pour en comprendre et en maîtriser l'usage. Un objectif de cette introduction à la cryptologie est de contribuer à la diffusion de ce savoir au plus grand nombre.

Quel service la cryptologie rend-elle ?

La cryptologie rend principalement deux services : la confidentialité et l'authentification. La problématique de la confidentialité est celle de la discrétion et du secret. L'information ne doit être accessible qu'à celui ou celle à qui l'information est destinée.

- Le programme de TV à péage ne doit être visible que par les abonnés.
- L'ordre des généraux, même s'il est intercepté, ne doit pas être connu de l'ennemi.
- Les parents de Jonathan doivent rester dans l'ignorance du lieu et de l'heure de son rendez-vous avec Olive.

Dans un système de confidentialité, l'adversaire est une oreille indiscrète.

La problématique de l'authentification est de s'assurer que l'information provient bien de l'émetteur annoncé, et qu'elle n'a été ni altérée ni intentionnellement modifiée au cours de son transfert ou de son stockage.

La banque vient de recevoir de Madame Betty Court un ordre de virement de dix mille ducats au bénéfice de son homme de confiance :

- Est-ce vraiment Betty Court qui a émis cet ordre de virement ?
- Le bénéficiaire désigné par elle est-il bien son homme de confiance ?
- Est-ce bien ce montant qu'elle a décidé de virer ?

L'adversaire d'un système d'authentification est un faussaire.

Les deux faces de la cryptologie

La cryptologie est la réunion de deux disciplines qui s'alimentent l'une l'autre : la cryptographie et la cryptanalyse. Le cryptographe conçoit des codes et des procédés résistants qui rendent le service de confidentialité ou d'authentification. Le cryptanalyste les attaque, brise leur résistance, cherche une faille, pour retrouver le sens caché du message, ou pour faire passer un faux pour un vrai. Ce sont ces attaques qui fournissent au cryptographe les critères de conception qui rendront ses procédés plus sûrs encore. Et ils seront à nouveau passés au crible du cryptanalyste.

Les utilisateurs d'un système cryptographique disposent d'un paramètre secret, d'une clé, détenue d'eux seuls, et sur lequel repose toute la sécurité. Si cette clé venait à être connue, tout le système s'effondrerait. Le cryptanalyste, lui, ne dispose pas de cette clé, et cherche quand même à pénétrer les messages.

L'activité cryptologique est encore présentée comme une course sans fin entre les codeurs et les briseurs de code. Une approche récente revendique une démarche scientifique et cherche à éviter cette boucle infinie en proposant dès la conception des preuves de sécurité.

Le premier chapitre présente les procédés de chiffrement traditionnels, balayant les moyens mis en œuvre depuis l'Antiquité grecque jusqu'à la mécanisation du calcul dans le courant du vingtième siècle. Leur présentation, suivant un point de vue historique, est l'occasion de voir comment les principaux concepts, encore en vigueur aujourd'hui, ont été introduits.

Le second chapitre est consacré aux procédés symétriques actuels. Ils sont appelés ainsi parce que la clé, c'est-à-dire le secret qui va permettre d'une part de chiffrer et d'autre part de déchiffrer, est partagée de manière symétrique entre l'émetteur et le destinataire du message.

Une avancée majeure est survenue dans le milieu des années 1970, avec l'invention de la cryptologie à clé publique, objet du troisième chapitre. Dans cette nouvelle cryptologie, les clés de l'émetteur et du destinataire ne sont plus identiques. Ces systèmes sont asymétriques. Et même, plus surprenant, la clé de l'émetteur peut sans inconvénient être dévoilée. Elle est publique. Le destinataire pourra déchiffrer à l'aide d'une clé différente qui, bien sûr, devra rester secrète. Ces mécanismes font appel à des mathématiques de plus en plus élaborées et ont permis de concevoir une multitude de nouveaux services, comme la signature, l'authentification, le vote, la monnaie électronique, etc.

Le quatrième chapitre est consacré à la cryptanalyse qui est le chiffre d'attaque, celui de l'adversaire qui cherche à pénétrer les messages sans disposer de la clé secrète qui lui permettrait de mettre à nu toutes les informations. Les principales attaques contre les systèmes symétriques sont présentées, ainsi que les algorithmes mathématiques qui permettent de contrer les systèmes à clé publique. La fin de ce chapitre présente un nouveau type d'attaque, non plus contre le procédé de camouflage, mais contre le dispositif matériel qui le réalise. Ces attaques reposent sur des mesures physiques, comme la consommation électrique ou le temps de calcul.

Le cinquième chapitre passe en revue la cryptographie de notre quotidien, en décrivant comment elle intervient dans nos objets familiers : carte de paiement, téléphone mobile, télévision à péage, ainsi que les protocoles qui assurent la sécurité de l'internet et qui ont permis de développer la confiance dans le commerce électronique.

L'émergence d'une science cryptologique autonome, dont l'objectif est de donner des assurances sur le niveau de sécurité atteint, est présentée au sixième chapitre. L'évaluation de la résistance des systèmes symétriques est fondée sur la théorie de l'information, qui est née de travaux effectués pendant la seconde

guerre mondiale pour établir des liaisons hautement sécurisées. Les preuves de sécurité des systèmes asymétriques sont plus récentes et dépendent des capacités de calcul de l'adversaire. On ne parle plus de sécurité inconditionnelle mais de sécurité calculatoire. Ce chapitre présente l'édifice cryptographique, qui consiste en une construction de méthodes de protection à clés secrètes ou à clés publiques, s'appuyant sur des fonctions élémentaires aux propriétés admises, dans une démarche de type axiomatique.

Le septième et dernier chapitre montre comment les sciences physiques font aujourd'hui leur entrée dans la cryptologie. Une contribution concerne l'attaque. Si un calculateur quantique voyait le jour, il rendrait inopérant la plupart des systèmes asymétriques actuels. L'autre contribution concerne la défense. La physique quantique apporte une solution originale au problème de l'échange de clé, en proposant un mécanisme, aujourd'hui fonctionnel, dont la sécurité repose, non plus sur certains problèmes mathématiques que l'on suppose difficiles à résoudre, mais sur les lois de la physique.

Trouverez-vous la clé ?

This page intentionally left blank

1

Les procédés traditionnels

Ce chapitre traite d'une période qui s'étend de l'Antiquité grecque jusqu'au début du vingtième siècle, quand le développement des calculateurs mécaniques, électromécaniques, puis électroniques a marqué le début d'une nouvelle ère. Cette cryptologie traditionnelle est un traitement de la langue écrite, avant d'être un calcul. Ce parcours historique montre comment les principaux concepts, toujours en vigueur aujourd'hui, ont été introduits.

1 Les substitutions simples

La première idée qui vient à l'esprit pour brouiller un texte écrit dans une langue à alphabet consiste à remplacer chaque lettre par une autre selon une règle convenue. Ce procédé s'appelle une *substitution simple*. Le chiffre de César en est un exemple. Il est réalisé en décalant l'alphabet. Il est mentionné par les historiens Suetone (vers 69, vers 130) et Aulu Gelle (vers 130, vers 180).

> *On possède enfin de César des lettres à Cicéron, et sa correspondance avec ses amis sur ses affaires domestiques. Il écrivait, pour les choses tout à fait secrètes, à travers des marques, c'est-à-dire un ordre arrangé de lettres de sorte qu'aucun mot ne pût être reconnu. Si on veut chercher et s'acharner jusqu'au bout, on change la quatrième lettre, c'est-à-dire un D à la place d'un A et pareillement pour toutes les autres.*
>
> Suetone, *La vie des douze Césars*

Le procédé de César tel que décrit ci-dessus consiste à appliquer un décalage de trois rangs dans l'alphabet. Voici la correspondance des vingt-trois lettres de l'alphabet du latin classique.

```
A B C D E F G H I K L M N O P Q R S T V X Y Z
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
D E F G H I K L M N O P Q R S T V X Y Z A B C
```

Pour retrouver le sens du message en clair, il suffit d'opérer le même décalage dans l'autre sens. Ce procédé subsiste encore aujourd'hui sous le nom de ROT13 qui opère un décalage de treize positions dans l'alphabet moderne. Il est utilisé pour brouiller un texte dans le réseau usenet qui sert encore à l'échange d'informations au sein d'une communauté. Ce décalage permet d'utiliser la même opération pour brouiller et pour clarifier le texte. Il n'y a aucun secret dans ce système qui ressemble plutôt à un *argot d'internet*.

La citation de Suetone montre que César utilisait ce procédé pour ses correspondances privées, et non pas pour des secrets militaires. Lors de ses campagnes, il utilisait un autre procédé qu'il cite lui-même dans *La guerre des Gaules*.

> *Il persuade alors un cavalier gaulois, en lui promettant de grandes récompenses, de porter une lettre à Cicéron. Il envoie celle-ci écrite en* ***lettres grecques****, afin que, si elle est interceptée, nos desseins ne soient pas pénétrés par les ennemis.*
>
> César, *La guerre des Gaules, V, XLVIII, 3–4*

Voici un message qu'aurait pu envoyer Jules César à son intendant, lorsque, retenu en Gaule dans ses quartiers d'hiver avec son armée, il en profite pour mettre à contribution les populations soumises par un tribut de guerre tout à fait habituel à l'époque (solution page 174) :

```
MMX KDOOMX TZM SVRAMPH LRXYHX IZHVDQY PDKQDX SHFZQMDX MPSHVDZM
SRSZOR VRPDQR, TZDX MQYVD GHFHP GMHX DFFMSMHX. P. YZOOMR DHX
DOMHQZP XROZHVH SRYHVMX HPHVHTZH D S. ZDOHVMR ZMOODP HMZX
FHQYZP PMOMEZX QZPPZP, MG HXY SVHYMZP TZRG FRQZHQHVDY.
```

Ces deux procédés de César ont en commun qu'ils opèrent le remplacement d'une lettre de l'alphabet par un signe différent. De nombreux autres graphismes sont utilisables pour camoufler du sens du message. Les Templiers utilisaient un alphabet spécial reposant sur la *croix de huit béatitudes* qui étaient l'emblème de leur ordre (Fig. 1.1). Les écoliers de toutes les époques reconnaîtront *le parc à cochon* (Fig. 1.2), utilisé aussi par les francs-maçons.

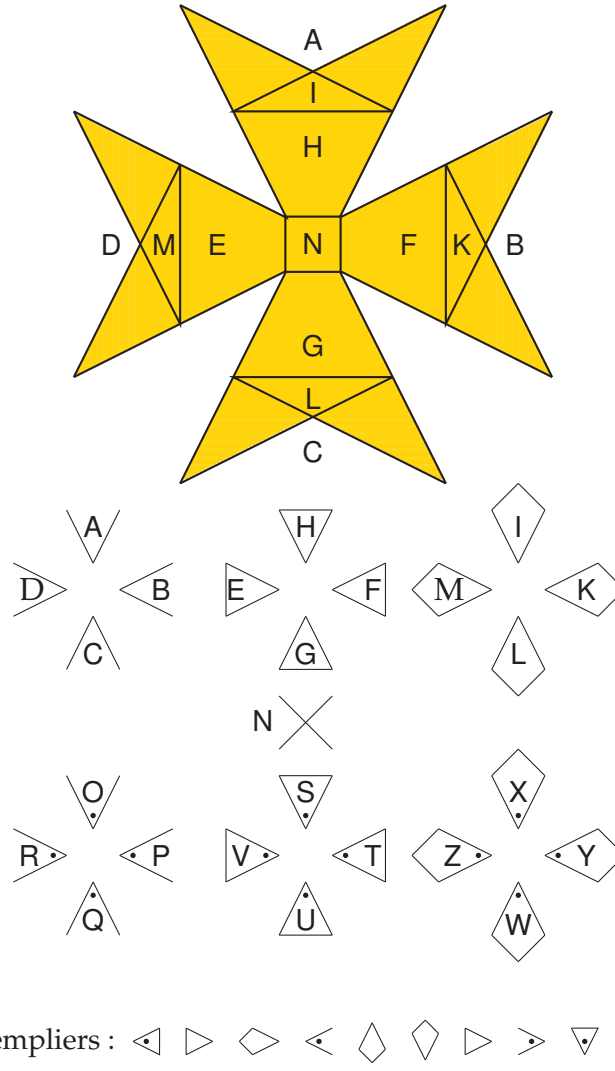


FIGURE 1.1. La croix des huit béatitudes, emblème de l'ordre des Templiers, est le support de l'alphabet dont se servaient les Templiers pour transmettre leurs lettres de crédit. Chaque lettre est représentée par un graphisme qui correspond à sa position sur la croix des huit béatitudes.

Dans la nouvelle *Les hommes dansants*, d'Arthur Conan Doyle, parue en 1903, Sherlock Holmes réussit à décrypter de mystérieux messages dessinés au crayon sur du papier, ou à la craie sur des murs, et où figurent les silhouettes de personnages qui ont l'air de danser (Fig. 1.3).

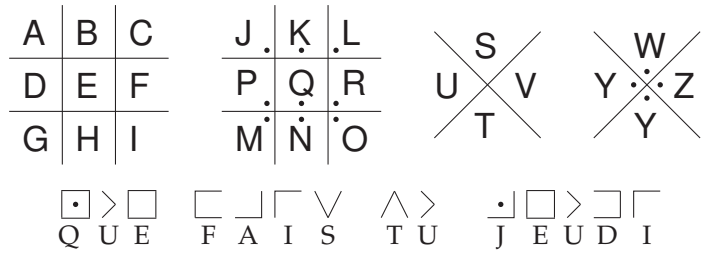


FIGURE 1.2. Le parc à cochon, procédé très ancien cité par Vigenère dans son *Traité des chiffres et des secrètes manières d'écrire*, Paris, 1586.

FIGURE 1.3. Les hommes dansants. Chaque figurine représente une lettre. Le talent de Sherlok Holmes et l'analyse des fréquences sont aisément venus à bout de ces mystérieux messages.

Si on se limite au décalage de César sur l'alphabet moderne, il n'existe que que vingt-cinq façons d'opérer et donc autant de décalages à tester pour retrouver le sens caché. Cela est réalisable manuellement, sans même l'aide d'outil de calcul. Il est plus sûr d'imaginer une substitution plus générale, qui remplace une lettre par une autre sans relation particulière. Il est seulement nécessaire que les lettres du texte en clair et celles du cryptogramme se correspondent une à une. Ce qu'on obtient ainsi est un *alphabet désordonné* comme par exemple celui-ci :

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

Le mode d'emploi de cet alphabet désordonné est des plus simples. Le A est remplacé par le M, le B par le R, le C par le Z, etc.

Le nombre d'alphabets désordonnés possibles est considérable. Il y a 26 choix possibles pour la première lettre, 25 pour la seconde, 24 pour la troisième, etc. Le nombre total d'alphabets désordonnés est le produit de tous les entiers de 26 jusqu'à 1, appelé la *factorielle* de 26 et noté 26! :

$$26 \times 25 \times 24 \times \cdots \times 2 \times 1 = 403\,291\,461\,126\,605\,635\,584\,000\,000.$$

Il n'est plus question d'essayer systématiquement toutes les possibilités, même en utilisant une machine très performante. Un super calculateur capable d'effectuer un milliard d'essais par seconde mettrait plus d'un milliard d'années pour explorer tous les alphabets possibles. Le cryptanalyste doit faire preuve d'habileté pour retrouver le sens caché d'un cryptogramme.

Les substitutions simples sont sensibles à l'analyse des fréquences, qui consiste à compter les occurrences des caractères et à comparer le résultat avec la distribution des lettres dans la langue du texte en clair. Le paragraphe 3 page 85 décrit les méthodes de résolution de ce type de chiffre. Pour le rendre plus résistant, les cryptographes ont imaginé de coder les lettres les plus fréquentes, comme le *e* ou le *a* de plusieurs façons différentes en alternant le choix du codage. En contrepartie, les lettres qui peuvent être remplacées par une autre sans inconvénient pour la compréhension sont supprimées. En français, on peut par exemple remplacer les *i* par des *j*, les *v* par des *u*. Ce type de substitution à représentations multiples s'appelle un *chiffre homophonique*. Il a été très utilisé pour les échanges diplomatiques à partir de la Renaissance.

2 Transpositions

Dans un procédé de transposition, les lettres du texte ne sont pas altérées. Seul l'ordre des lettres est changé de façon à aboutir à un mélange sans cohérence.

> *En un mot, les méthodes de transposition sont une salade des lettres du texte clair.*
>
> Étienne Bazeries (1846-1931), cryptanalyste militaire français.

Le chiffrement *Rail fence*, utilisé pendant la guerre de Sécession, consiste en une transposition obtenue en écrivant un texte dans un tableau par colonnes, éventuellement en descendant et en montant successivement. Le cryptogramme est constitué en écrivant le texte en suivant les lignes.

2.1 La grille tournante

La grille tournante, ou grille de Fleissner, du nom du colonel autrichien Édouard Fleissner von Wostrovitz (1825-1888), qui l'a présentée en 1881 dans son ouvrage *Handbuch der Kryptrographie*, est un chiffrement par transposition. Ce procédé cryptographique est décrit dans les articles du cryptographe polytechnicien français Gaëtan Viaris de Lesegno (1847-1901), ainsi que dans le roman de Jules Verne *Mathias Sandorf* en 1885. Le cryptogramme est disposé dans un carré, et en plaçant sur celui-ci une grille ajourée comprenant des trous convenablement placés, les premières lettres du message en clair apparaissent. La suite du cryptogramme est lue de manière similaire en tournant successivement la grille d'un quart de tour (Fig. 1.4).

D

E

F

G

H