© LL/ROGER-VIOLLET

**Du code de Jules César à la cryptographie quantique, les méthodes pour coder un message ont été développées autour d'un même axe. Une seule est parfaitement inviolable, celle du « chiffre de Vernam ». Mais sa lourdeur d'emploi la réserve à des usages très spécifiques.**

# Les secrets de César et du téléphone rouge

**Hervé Lehning**
**professeur de mathématiques spéciales au lycée Janson-de-Sailly.**
Herve.lehning@prepas.org

D'après Suétone, à l'époque de la guerre des Gaules, Jules César chiffrait ses messages sensibles en remplaçant chaque lettre par la troisième la suivant dans l'alphabet [1]. Ainsi, ATTAQUEZA QUATREHEURESPARLENORD devient : DWWDTXHCDTXDWUHKHXU HVSDUOHQRUG.

Le décryptage est facile si l'on connaît la clef de chiffrement : il suffit de décaler les lettres de façon inverse.

Au IX^e siècle, le savant arabe Abu Yusuf al Kindi constatait que, dans deux textes assez longs, les fréquences d'apparition de chaque lettre sont proches. En calculant ces fréquences et en les comparant aux fréquences usuelles, il retrouvait les substitutions alphabétiques utilisées. Par exemple, dans le cas du message précédent, les lettres les plus fréquentes sont D et H. En français, ce sont E et A. En essayant les diverses hypothèses et en calculant les autres fréquences, le message est vite déchiffré. La méthode d'al Kindi permet normalement de casser tout système cryptographique où chaque lettre est toujours codée de la même façon.

Pour remédier à cette faiblesse des codes à substitution alphabétique, un diplomate français de la Renaissance, Blaise de Vigenère imagina de faire varier le décalage du code de César en fonction d'un mot arbitrairement choisi. Ce mot, par exemple CESAR, est la « clef du chiffrement ». Comment s'en sert-on ? On l'écrit d'abord sous le message autant de fois que nécessaire puis on décale les lettres du message de 2 pour C, de 4 pour E et ainsi de suite [fig. 1]. Dans notre exemple, nous obtenons le message : CXLAHWIRAHWELRVJIMRVUTSRCG RGRU

L'analyse des fréquences ne fonctionne plus et on ne peut facilement décrypter de tels messages que si l'on dispose de la clef.

Mais cette méthode de cryptage n'est pas sans failles, elle non plus. Le mathématicien anglais Charles Babbage eut l'idée au XIX^e siècle de chercher des répétitions dans les messages. Dans notre exemple, on remarque la répétition du motif AHW. Il peut s'agir d'une coïncidence mais, plus probablement, un même texte a été codé avec la même partie de la clef. On voit par ailleurs que les deux répétitions sont séparées par cinq lettres. S'il ne s'agit pas d'une coïncidence, la longueur de la clef est un diviseur de 5.

Si l'on divise le message en six groupes suivant qu'il a été crypté par l'une ou l'autre des lettres de la clef, on obtient CWWJUG, XIEITR, LRLMSG, AARRRR et HHVVCU. Chacun de ces groupes correspond à un chiffrement par décalage, la méthode des fréquences d'al Kindi lui est donc applicable. Dans notre exemple, les groupes sont trop courts pour permettre le décryptage mais, de façon générale, la méthode de Babbage est d'autant plus fructueuse que le rapport entre la longueur totale des messages cryptés et celle de la clef est grand.

Seule solution pour empêcher tout décryptage : utiliser une clef aussi longue que le message lui-même et la jeter après usage. Le cryptographe américain Gilbert Vernam eut cette idée simple en 1917 — Claude Shannon

**Fig.1 Chiffre de Vigenère**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A | T | T | A | Q | U | E | Z |
| C | E | S | A | R | C | E | S |
| C | X | L | A | H | W | I | R |

**LE DÉCALAGE EST FAIT selon le numéro d'ordre d'apparition de chaque lettre dans l'alphabet : 0 pour A, 1 pour B, etc. Ici, la clef du chiffrement est CESAR.**

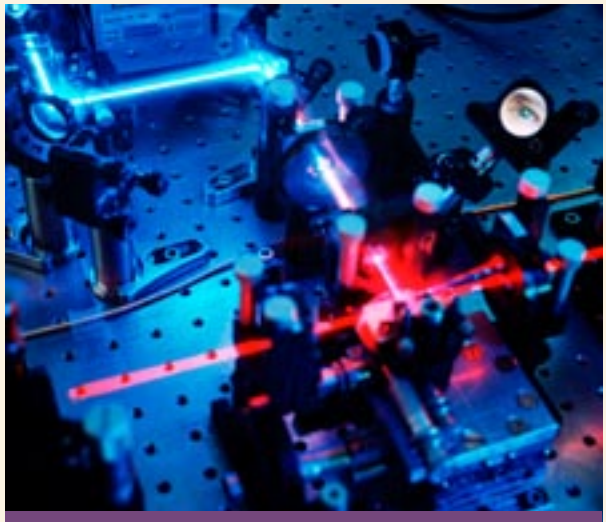
[1] Suétone, *Vies des douze Césars*, livre I, LVI-8.

[2] N. Constans, « Quatre premiers lauréats pour le Prix La Recherche », *La Recherche*, décembre 2004, p. 42.

montrera par la suite que le chiffre de Vernam est inviolable. Sans rentrer dans les détails, disons que, si la clef est aléatoire, le message obtenu en l'appliquant est également aléatoire.
Aujourd'hui, un message comme
ATTAQUEZAQUATREHEURESPARLENORD
est d'abord numérisé, c'est-à-dire mis sous la forme d'une suite de 0 et de 1. En code ASCII, le mot ATTAQUEZ devient :
01000001010101000101010001000001010100010101010101000101010011010.
La clef doit être une suite aléatoire de 0 ou 1, par exemple :
10101101011110010101000111100001110101011010111000000011110001110.
Pour coder, on l'ajoute les deux suites :
11101100001011010000010110100000100001001111101101000010110100.
Pour décoder, il suffit d'ajouter la clef au message codé car, en mode binaire, 1 + 1 = 0.
Les faiblesses du seul code dont l'invulnérabilité est prouvée : la taille de la clef et, surtout, la nécessité de la transmettre de façon totalement secrète. C'est pour cette raison que son usage est aujourd'hui réservé à quelques applications en informatique, à l'armée et aux milieux diplomatiques. C'est lui qui est notamment utilisé pour le « téléphone rouge » reliant Washington et Moscou.

## Des clefs vraiment aléatoires

Mais les choses pourraient rapidement changer, grâce à la maîtrise des photons dans le cadre de la cryptographie quantique. La première tentative d'utilisation de la mécanique quantique pour le transfert de clefs, en 1984, est due à deux chercheurs canadiens, Charles Bennet et Gilles Brassard. La cryptographie quantique — objet d'un des *Prix La Recherche* en 2004 [2] — permet tout à la fois de créer des clefs véritablement aléatoires et de les transférer de façon impossible à intercepter sans destruction.



© VOLKER STEGER/SPL/COSMOS

**VOICI À QUOI POURRAIT RESSEMBLER L'APPAREIL DE DEMAIN pour coder des messages. La cryptographie quantique a en effet quitté le domaine de la recherche fondamentale (ici un laboratoire de l'Institut de physique expérimentale à Vienne) pour atteindre celui du développement et de la commercialisation.**

Quel est le principe ? On polarise les photons — c'est-à-dire que l'on impose une direction à leur champ électrique — à 0, 45, 90 ou 135 degrés. Les interlocuteurs (émetteur et récepteur) disposent de deux liaisons : une fibre optique et une liaison radio. Par la fibre, l'émetteur envoie une suite de photons polarisés aléatoirement. Le récepteur les fait passer à travers un filtre polarisant orienté aléatoirement à 0° (rectiligne) ou 45° (diagonal) derrière lequel est situé un détecteur de photons. Si le filtre est rectiligne, un photon orienté à 0° le traverse puis est détecté. Un photon orienté à 90° est stoppé. En revanche, un photon orienté à 45° ou 135° traverse le filtre avec une probabilité de 0,5. Ainsi, on peut distinguer entre un photon à 0° ou 90° mais pas entre des photons à 45° ou 135°. De même, un filtre diagonal permet de distinguer les photons à 45° et ceux à 135°, mais pas entre ceux à 0° ou 90°. Le récepteur note 0 si le photon traverse et 1, sinon. Pour éliminer les cas incertains, il donne l'orientation de son filtre à la réception (diagonal ou rectiligne). S'il diffère de l'orientation à l'émission, le bit envoyé est incertain, donc supprimé. La clef transmise est la suite des bits conservés [fig. 2].
En cas d'interception de la communication, un espion doit émettre les photons correctement vers le récepteur. Pour cela, il doit procéder comme le récepteur puis réémettre. Comme il a une chance sur deux d'avoir utilisé le mauvais filtre, la moitié des photons réémis seront faux.
La cryptographie quantique a aujourd'hui quitté le domaine de la recherche fondamentale pour atteindre celui du développement et de la commercialisation. Cependant, vitesse et distance de transfert restent très limitées : une centaine de bits par seconde pour une distance maximale de 100 kilomètres. Pour aller au-delà on songe à utiliser des satellites ou des retransmetteurs. La clef de Vernam quantique sera alors peut-être la clef du succès de la cryptographie. ■■

### POUR EN SAVOIR PLUS

■ Gilles Brassard, *Cryptologie contemporaine*, Masson, 1992.

## Fig.2 De la polarisation à la clef

| Émission | 0° | 45° | 90° | 45° | 0° | 135° | 90° | 0° | 45° |
|---|---|---|---|---|---|---|---|---|---|
| Bit envoyé | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| Filtre réception | diag. | diag. | rect. | diag. | rect. | rect. | rect. | diag. | rect. |
| Traverse ? | non | oui | non | oui | oui | non | non | non | oui |
| Bit reçu | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| Clef | X | 0 | 1 | 0 | 0 | X | 1 | X | X |

**L'ÉMISSION DE PHOTONS POLARISÉS REÇUS ENSUITE À TRAVERS UN FILTRE ÉGALEMENT POLARISÉ permet de créer des clefs aléatoires et secrètes. Un détecteur de photons note 0 si le photon traverse et 1, sinon. Pour les cas incertains, si l'orientation du filtre à la réception diffère de l'orientation à l'émission, le bit est supprimé. La clef transmise est la suite des bits conservés.**