# LES RÉVOLUTIONS CRYPTOLOGIQUES DE 1937 À NOS JOURS

En 1937, la cryptologie était réservée aux militaires et diplomates. Elle s'effectuait à la main ou impliquait des machines telle l'Enigma allemande, que l'on croyait indécryptable. La Seconde Guerre mondiale amena une révolution dans ce domaine et le décryptement prit une part importante à la victoire. Trente ans plus tard, une autre révolution a placé les mathématiques au cœur de la cryptologie. En 2017, cartes bancaires et messages sur Internet intègrent cette dernière dans la vie de chacun.

PAR **HERVÉ LEHNING**, PROFESSEUR DE MATHÉMATIQUES, CRYPTOLOGUE, ÉCRIVAIN ET JOURNALISTE SCIENTIFIQUE

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | 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 |
| b | 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 |
| c | 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 |
| d | 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 |
| e | 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 |
| f | 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 |
| g | 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 |
| h | 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 |
| i | 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 |
| j | 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 |
| k | 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 |
| l | 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 |
| m | 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 |
| n | 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 |
| o | 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 |
| p | 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 |
| q | 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 |
| r | 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 |
| s | 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 |
| t | 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 |
| u | 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 |
| v | 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 |
| w | 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 |
| x | 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 |
| y | 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 |
| z | 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 |

| | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Clef** | A | B | C | A | B | C | A | B | C | A | B | C | A | B | C | A | B | C | A | B | C | A | B |
| ***Message clair*** | *p* | *a* | *l* | *a* | *i* | *s* | *d* | *e* | *l* | *a* | *d* | *e* | *c* | *o* | *u* | *v* | *e* | *r* | *t* | *e* | | | |
| **Message chiffré** | P | B | N | A | J | U | D | F | N | A | E | G | C | P | W | V | F | T | T | F | | | |

**Figure 1.** Carré de Vigenère. La clef de chiffrement est « abc ». Elle indique dans quelles colonnes successives chercher les lettres du message chiffré. Quant aux lignes, elles sont désignées par les lettres du message clair. Pour déchiffrer le message en connaissant la clef, il suffit de retrouver la lettre chiffrée dans les colonnes « A », « B » ou « C » : elle se situe sur la ligne correspondant à la lettre du message d'origine. © Universcience / G. Reuiller.

Quand le Palais de la découverte ouvrit ses portes en 1937, la cryptologie, c'est-à-dire la science du secret, l'art de coder ou plutôt chiffrer ses messages et décrypter ceux des autres, avait déjà une longue histoire. Une première révolution théorique avait eu lieu à la fin du XIX^e^ siècle avec le cryptologue néerlandais Auguste Kerckhoffs (1835-1903), qui énonça le principe de base de la cryptographie moderne : un système de chiffrement ne doit pas reposer sur le secret de son fonctionnement (qui peut donc être connu de tous), mais sur celui d'une clef changée périodiquement.

Dès la Renaissance, le linguiste et diplomate français Blaise de Vigenère (1523-1596) avait conçu un système répondant au principe de Kerckhoffs, qui fut peu utilisé à l'époque. Sans doute était-il jugé trop complexe. Il consiste en un décalage des lettres variant selon une clef. Par exemple, la clef « abc » correspond à un décalage de 0 pour la première lettre, 1 pour la deuxième, 2 pour la troisième, 0 pour la quatrième, 1 pour la cinquième, etc. (fig. 1). Pour le déchiffrement, connaissant la clef, il suffit d'effectuer les mêmes décalages lettre à lettre, mais dans l'autre sens. Bien entendu, les clefs sont en général plus

**Enigma, une machine à chiffrer utilisée par l'armée allemande pendant la Seconde Guerre mondiale.**
© J. Paul, Crypto-Museum.

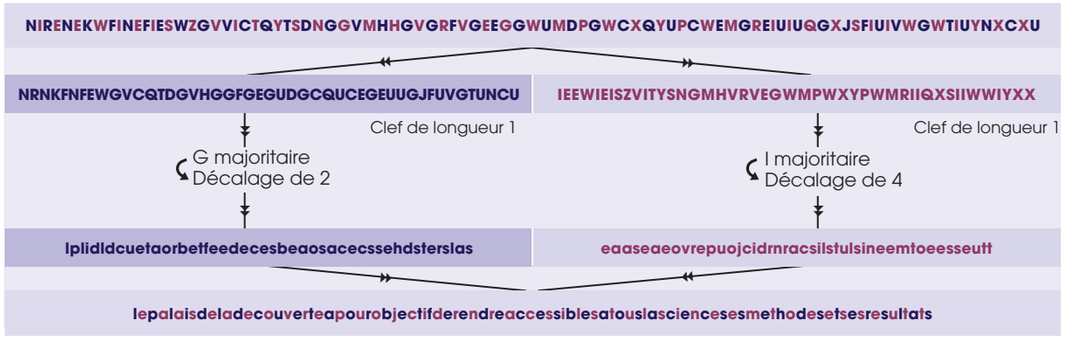


**Figure 2.** Ce message a été chiffré selon la méthode Vigenère, à l'aide d'une clef inconnue dont nous savons seulement qu'elle est constituée de deux lettres. Nous scindons alors le message en deux en prenant une lettre sur deux. Ces deux nouveaux messages peuvent être décodés en supposant que la lettre la plus fréquente remplace probablement un « e ». © Universcience / G. Reuiller.

complexes, néanmoins le principe reste identique. Il s'agit de chiffrement par substitution polyalphabétique, appelé ainsi car une même lettre peut être remplacée par différentes autres tout au long du message. Pendant la Seconde Guerre mondiale, plusieurs réseaux d'espionnage allemands l'employèrent. Les clefs utilisées se trouvaient dans un roman, comme l'écrivain gallois Ken Follett le décrit dans *Le Code Rebecca*. Si la clef choisie est aussi longue que la page d'un livre, ce chiffre est difficile à décrypter.

## LE MASQUE JETABLE

La solidité d'un chiffre de Vigenère réside dans la longueur et l'imprévisibilité de sa clef. Si cette dernière est de longueur 1, comme dans le cas du chiffre utilisé par Jules César (100-44 av. J.-C.), le chiffrement consiste à décaler toujours du même nombre de lettres. Le décryptement d'un message sans connaissance de la clef peut s'effectuer simplement en repérant la lettre la plus fréquente. Si le message initial est en français, elle remplace probablement la lettre « e », qui est la plus courante dans cette langue. Par exemple, dans « rcncku fg nc fgeqwxgtvg », la lettre la plus fréquente est « g », ce qui correspond à un décalage de 2 (e → f → g). En clair, le message signifie donc « palais de la découverte ». Cette astuce permet de décrypter également les messages chiffrés avec des clefs de longueur 2 (fig. 2). Par exemple, si nous savons que le message « niren ekwfi nefie swzgv victq ytsdn ggvmh hgvgr fvgee ggwum dpgwc xqyup cwemg reiui uqgxj sfiui vwgwt iuynx cxu » a été chiffré avec une clef de longueur 2, nous le scindons en deux messages, groupant pour chacun une lettre sur deux du message initial. Chaque « demi-message » ayant été chiffré par une clef de longueur 1, la méthode précédente leur est appliquée. Puis nous effectuons les décalages dans l'autre sens et assemblons les deux morceaux pour obtenir un texte ayant un sens : *Le Palais de la découverte a pour objectif de rendre accessibles à tous la science, ses méthodes et ses résultats*. La méthode fonctionne pour toute longueur à condition que le rapport entre la longueur du message et celle de la clef reste important, au moins 40 environ. Bien entendu, il est rare de connaître à l'avance la longueur des clefs, mais une technique d'analyse peut consister à essayer toutes les longueurs possibles.

**Figure 3.** Carnet de nombres aléatoires destiné au chiffrement. Le message original est transformé en une suite de nombres par le procédé voulu, qui est ajoutée ensuite chiffre à chiffre aux nombres du carnet. Le déchiffrement s'effectue par soustraction. © Ministère de la Défense.

Pour éviter le décryptement, un stratagème consiste donc à utiliser la méthode de Vigenère avec des clefs aussi longues que le message, aléatoires afin d'être imprévisibles et à les jeter après un seul usage. En créant la théorie de l'information, Claude Shannon (1916-2001) a montré, en 1949, que si la clef est aléatoire, ce chiffre, appelé *masque jetable*, est inviolable. Malgré son excellence, il ne peut être employé cependant pour des communications de masse, comme le demande une armée en campagne, en raison du problème de transfert des clefs. En revanche, il fut très utilisé par les espions soviétiques, et d'autres sans doute, pendant la guerre froide, d'où l'existence d'étranges petits carnets de nombres aléatoires (fig. 3) et de *radios de nombres* ne diffusant que des nombres.

## LES MACHINES À ROTORS

Les exemples précédents montrent que pour se servir des codes polyalphabétiques, mieux vaut pouvoir confier le chiffrement à des machines. Au cours des années 1930, l'armée française s'équipa ainsi, auprès de la firme Hagelin, d'une machine mécanique légère, la C-36 (fig. 4), destinée aux communications des petites unités tactiques, et d'une machine électromé-

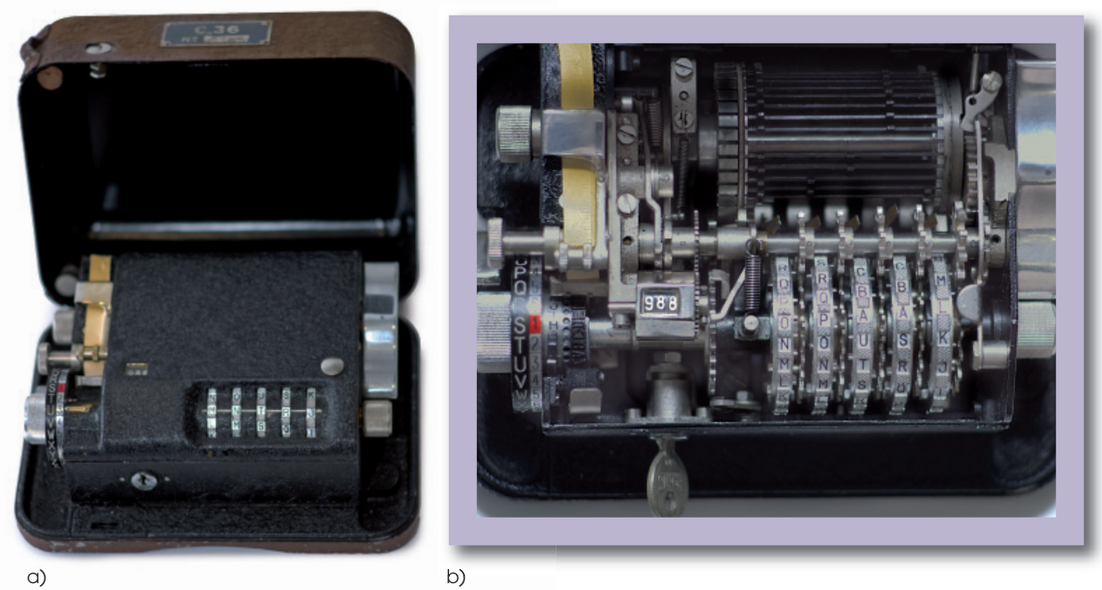


**Figure 4.** a) C-36 fermée. Les cinq lettres visibles sur le capot (ici MNTRJ) constituent une clef modifiable à chaque message. La machine est actionnée par le levier de droite. Les lettres à chiffrer sont choisies sur la roue de gauche et le chiffrement sort sur la bande de papier à gauche. b) C-36 ouverte. Les ergots des rotors sont visibles, chacun étant poussé vers la droite ou la gauche, ce qui constitue la clef principale avec la position de l'élément rouge sur la roue de gauche, ici devant le S. © J.-L. Desvignes.

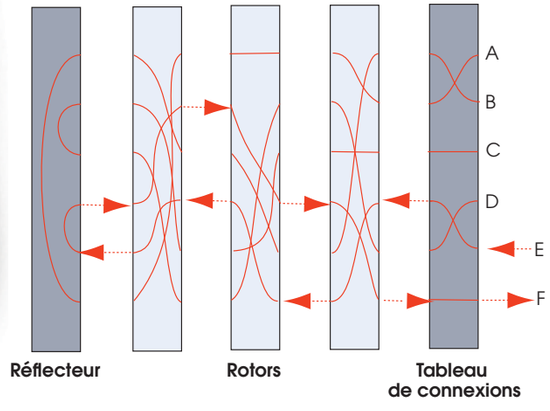


**Figure 5.** a) Une Enigma à trois rotors (au fond) comprenant un clavier de vingt-six touches, des lampes (au-dessus) et un tableau de connexions (face avant). b) Schéma simplifié de son fonctionnement : si la lettre « E » est tapée, elle est échangée tout d'abord avec « D » par le tableau de connexions. Puis, *via* les deux passages dans les trois rotors, c'est finalement « F » qui s'allume… a) © J. Paul, Crypto-Museum ; b) © H. Lehning.

canique lourde, la B-211, destinée aux communications au niveau des grosses unités. La C-36 a été perfectionnée, devenant la M-209 de l'armée américaine. Cette machine était assez solide pour son niveau d'utilisation. Cependant, dès 1943, les Allemands étaient capables de décrypter ses messages en quelques heures.

Le mécanisme de la C-36 repose sur un ensemble d'engrenages entraînés par une série de cinq rotors ayant respectivement 17, 19, 21, 23 et 25 ergots, qui doivent être configurés manuellement chaque jour selon un tableau tenu secret. Avec la position de la roue de gauche (celle comportant une marque rouge), cela constitue la clef du jour. Une seconde clef, choisie par l'opérateur à chaque message, est déterminée par la position initiale des rotors, visible quand le capot est fermé. Elle est envoyée en clair, mais de façon camouflée, dans le style de l'alphabet radio où « bravo » signifie « B ». Après le chiffrement d'une lettre du message, chaque roue avance d'un cran et une nouvelle configuration d'ergots est mise en place pour chiffrer la lettre suivante. Le message est chiffré ainsi lettre par lettre et le résultat imprimé sur une bande de papier. Il est déchiffrable à l'aide d'une autre C-36 réglée de la même manière.

## DANS LES ROUAGES D'ENIGMA

Dès 1926, l'armée allemande s'équipa d'Enigma, une machine électromécanique à trois rotors interchangeables conçue à l'origine pour les relations commerciales. Bien entendu, ses rotors ont été modifiés afin de remplir son rôle militaire. Extérieurement, Enigma ressemble à une machine à écrire avec un clavier de vingt-six touches représentant les lettres de l'alphabet (fig. 5a). Chaque fois que l'une de ces touches est actionnée, la lettre chiffrée



**Le décryptement de la machine à chiffrer allemande Enigma, résultat combiné de l'espionnage et du génie mathématique, a sauvé plusieurs centaines de milliers de vies et écourté la Seconde Guerre mondiale probablement de deux ans.**

correspondante s'éclaire sur un tableau lumineux. Pour réaliser cette opération, Enigma utilise essentiellement deux composants : le brouilleur, constitué de trois rotors associés à un réflecteur, et le tableau de connexions (fig. 5b).

Le schéma électrique présente deux particularités. D'une part, une lettre est toujours chiffrée par une lettre différente. D'autre part, grâce au réflecteur, si dans une certaine configuration de la machine, « E » est chiffrée en « F », « F » est chiffrée en « E ». Ces deux propriétés constituent des faiblesses qui aideront le décryptement. Mais la seconde est pratique d'un point de vue opérationnel puisque, pour déchiffrer un message chiffré par une Enigma, il suffit d'utiliser une autre Enigma configurée de façon identique.

En pratique, l'armée allemande disposait d'une clef par jour. Cette dernière était définie par le choix et la position initiale des rotors, ainsi que par la position des six fiches du tableau de connexions. Le calcul montre 10 586 916 764 424 000 clefs possibles pour la version la plus simple, ce qui explique pourquoi on croyait Enigma indécryptable. En réalité, elle l'aurait été probablement sans les erreurs de procédure allemandes… et l'espionnage français.

Le premier décryptement d'Enigma fut un succès conjoint de l'espionnage français et du génie de trois mathématiciens polonais : Marian Rejewski (1905-1980), Jerzy Różycki (1909-1942) et Henryk Zygalski (1908-1978). L'espionnage a fourni les tables de chiffrement de l'armée allemande de 1931 à 1938, recensant quotidiennement les clefs utilisées. Grâce à ce renseignement, les mathématiques ont permis de reconstituer les câblages de la version militaire d'Enigma et de fabriquer des répliques de cette machine dès 1933. Les messages furent déchiffrés alors régulièrement. Les mathématiciens polonais cherchèrent, et réussirent, à se passer des tables de chiffrement, en créant notamment une machine, la Bombe. Elle permettait de trouver la clef du jour en quelques minutes. Après la défaite de la Pologne puis celle de la France, les résultats polonais furent

## Aléatoire *versus* pseudo-aléatoire

**En français, aléatoire signifie imprévisible, lié au hasard. Cette définition montre qu'il n'est pas facile de fabriquer de l'aléatoire, même si les phénomènes quantiques le permettent. Une suite de nombres pseudo-aléatoires est une suite établie selon des règles précises, mais ayant l'aspect d'une suite aléatoire.** En voici une, typique, qui fut utilisée autrefois. Partant d'un nombre, nommé traditionnellement *germe*, multipliez-le par 16 807, puis prenez le reste du résultat dans la division par 2 147 483 647 et recommencez. Cela donne une suite de nombres compris entre 0 et 2 147 483 646 qui semble générée par le hasard. Par exemple, si vous prenez 21 comme germe, vous obtenez la suite : 21, 352 947, 1 637 012 935, 1 863 396 828, 1 356 463 995, etc. Cependant, elle est déterministe. Son côté « aléatoire » dépend d'un secret. Des chiffres contrevenant au principe de Kerckhoffs sont ainsi obtenus.

livrés aux Britanniques. Le mathématicien Alan Turing (1912-1954) et son équipe de Bletchley Park reprirent avec succès le décryptement en l'améliorant et l'adaptant aux complexifications successives d'Enigma. La guerre fut écourtée probablement de deux ans grâce à tous ces efforts.

### L'ÈRE ÉLECTRONIQUE

L'équipe de dix mille personnes réunie à Bletchley Park ne s'occupait pas que d'Enigma mais de toutes les machines à chiffrer allemandes, dont celle réservée aux messages entre le haut commandement et les armées, la machine de Lorenz. Elle était fondée sur le masque jetable, en binaire (chaque lettre étant codée préalablement sur cinq bits, « A » étant remplacé par exemple par « 00001 »), mais avec une clef pseudo-aléatoire (encadré *Aléatoire* versus *pseudo-aléatoire*). Une erreur de manipulation allemande permit de reconstituer l'algorithme de création des clefs et, en 1943, les Britanniques construisirent Colossus, le premier calculateur électronique de l'histoire, pour décrypter cette machine. Lors de la crise de Suez de 1956, les Britanniques firent savoir aux Français qu'il ne fallait plus utiliser la B-211, toujours en service. Cela déclencha la recherche d'une machine à chiffrer plus sûre, et les machines à rotors furent reléguées au niveau tactique. On revint au masque jetable, comme dans la machine de Lorenz mais avec des clefs réellement aléatoires, qui doivent être additionnées bit à bit au message pour obtenir le message chiffré (fig. 6).

Ainsi naquit la machine TAREC (transmission automatique régénératrice et chiffrante), utilisée par l'OTAN (Organisation du traité de l'Atlantique nord) dès le milieu des années 1950. La méthode ayant l'avantage de permettre des communications sécurisées sans d'autre échange secret que celui de la clef aléatoire (qui se transmettait sous forme de bandes perforées), elle était idéale pour la correspondance entre adversaires. Elle fut donc choisie pour le téléphone rouge entre Washington et Moscou, quand la crise des missiles de 1963 montra l'utilité d'une telle voie de communication. La France développa ensuite une machine électronique de chiffrement fondée elle aussi sur le masque jetable, mais avec une clef pseudo-aléatoire, la machine Myosotis.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Message clair | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| + Clef (aléatoire) | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| = Message chiffré | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| + Clef (aléatoire) | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| = Message clair | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |

**Figure 6.** Chiffrement d'un message par masque jetable aléatoire. Le message est transcrit d'abord en bits, qui sont ajoutés un à un à ceux de la clef fabriquée aléatoirement, selon les règles d'addition classiques du binaire (0 + 0 = 0, 0 + 1 = 1 + 0 = 1 et 1 + 1 = 0). Comment déchiffrer un tel message ? Il suffit d'ajouter simplement la clef au message chiffré, le message en clair est alors retrouvé ! © Universcience / G. Reuiller.

### LA RÉVOLUTION DES CLEFS ASYMÉTRIQUES

Dans tous les chiffres vus jusqu'à présent, la connaissance de la clef de chiffrement suffit pour déchiffrer : ils sont dits symétriques. C'est là que se situe leur principal point faible : si cette clef est interceptée par un tiers, le chiffrement n'a plus rien de secret pour lui. Aussi étrange que cela puisse paraître, il existe des chiffres pour lesquels savoir chiffrer n'implique pas de savoir déchiffrer. Ces chiffres sont dits asymétriques. La clef de chiffrement est dite publique, celle de déchiffrement privée ou secrète. Le premier chiffre asymétrique est dû à trois mathématiciens, Ronald Rivest, Adi Shamir et Leonard Adleman, qui le proposèrent en 1977. Cette méthode, nommée RSA, est fondée sur la difficulté d'un problème mathématique : la factorisation en nombres premiers. Un nombre premier est un nombre qui n'est divisible que par 1 et lui-même – tels 2, 3, 5, 7, 11, etc. Factoriser un nombre, c'est l'écrire comme produit de nombres premiers. Par exemple, $15 = 3 \times 5$ et $156\,323 = 223 \times 701$. Ce problème simple pour de petits nombres est complexe pour de plus grands, même si de nos jours nous savons factoriser ceux à plus de deux cents chiffres. Ainsi, la clef publique du code RSA est un nombre, produit de deux grands nombres premiers qui constituent, quant à eux, la clef secrète. Chacun peut chiffrer, mais seul le détenteur de la clef secrète peut déchiffrer. Ce système est assez lourd en calcul car il correspond à des élévations de grands nombres à une puissance élevée, alors que les systèmes symétriques correspondent à des additions. C'est pourquoi il est limité à l'authentification et l'échange de clefs symétriques. Il est utilisé dans les cartes bancaires, les messages sur Internet ou le téléphone sécurisé Teorem de Thales, réservé aux hautes autorités de l'État.

### LES DANGERS ACTUELS

Bien entendu, ces chiffrements difficilement décryptables, mis à la disposition de tous, déplaisent aux services de renseignements. Pour satisfaire le désir de l'État de surveiller escrocs et terroristes, une solution consiste à faire appel à un tiers de confiance gardant les clefs de chacun et d'instaurer une législation prévoyant d'y faire appel dans le cadre de certaines enquêtes. En 2013, Edward Snowden a révélé que la NSA (National Security Agency, Agence nationale de la sécurité) a préféré adopter une autre démarche et demandé aux fournisseurs de logiciels américains de créer des portes dérobées permettant de contourner leurs algorithmes de chiffrement. Mais si une telle porte existe pour pénétrer dans une citadelle, tout le monde peut la découvrir et l'utiliser. La NSA a créé ainsi une faiblesse dans tous les systèmes de chiffrement qu'elle contrôle : pourquoi les hackers se priveraient-ils alors de l'exploiter ? **H. L.**


## Hervé Lehning

**Après des études classiques (École normale supérieure, agrégation de mathématiques, maîtrise d'histoire des religions),** Hervé Lehning a enseigné les mathématiques, l'informatique et la cryptologie en école d'ingénieurs et en classe de mathématiques spéciales. Il est commandant de réserve, membre de l'Association des réservistes du chiffre et de la sécurité de l'information et de la Société mathématique de France.


## Pour en savoir plus


Guillot P., *L'art des codes secrets*, EDP Sciences, 2013.

Kahn D., *La guerre des codes secrets*, InterEditions, 1980.

Lehning H., *L'univers des codes secrets, de l'antiquité à Internet*, Ixelles éditions, 2012.

Site internet de l'ARCSI (Association des réservistes du chiffre et de la sécurité de l'information) : > www.arcsi.fr

Exposé « Vous avez un message secret » proposé par l'unité Mathématiques du Palais de la découverte.