

A propos de cryptographie

(extraits de <http://interstices.info/crypto-chiffre-lettres>)

Écriture secrète, la cryptographie a longtemps été une affaire de diplomates et de militaires, soucieux de protéger leurs messages. Son essor moderne est dû aujourd'hui aux mathématiciens et aux informaticiens de talent.

La cryptographie (« écriture secrète ») est la science des codes secrets, littéralement des codes « destinés à mettre à l'écart » ceux qui ne connaissent pas telle ou telle information. On se sert tous les jours de la cryptographie : carte bancaire, chaînes de télévision à péage, déclaration de revenus sur Internet, signature électronique, etc. La sécurité peut être en effet considérée comme la distribution de la confiance. La cryptographie permet aux gens de s'assurer que cette confiance ne sera pas compromise lors des communications.

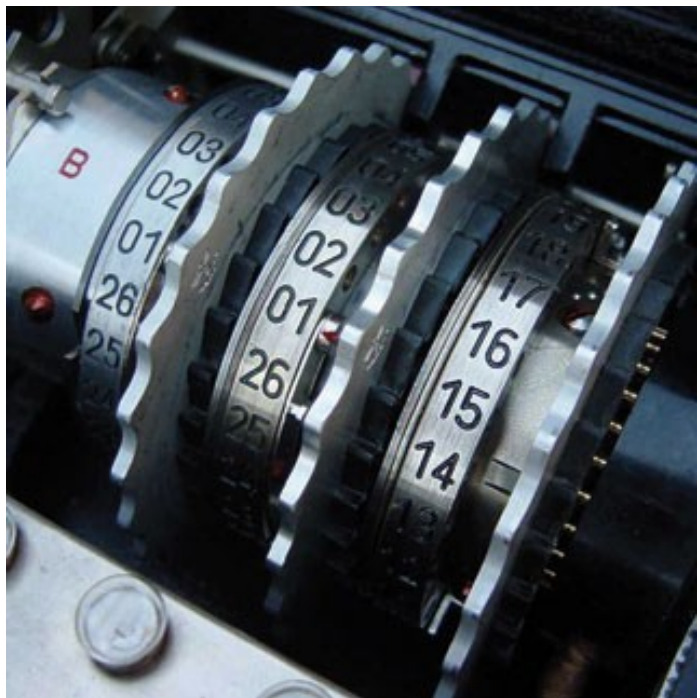
L'histoire des codes secrets a été souvent façonnée par les militaires et les diplomates, depuis Jules César jusqu'au Téléphone rouge qui reliait le Kremlin et la Maison Blanche, en passant par le cassage (avec l'aide des Polonais) des codes de la machine *Enigma* de la marine allemande par les plus brillants mathématiciens britanniques, dont Alan Turing. Ce cassage, de l'aveu du Premier ministre de l'époque Winston Churchill, a accéléré l'issue de la guerre de plusieurs mois, épargnant la vie de milliers de personnes.

Ce que croyait Jules César, qui était un peu prétentieux, comme le sont parfois les gens dans sa situation. Pour envoyer ses messages secrets à ses soldats sur le champ de bataille, il choisissait la même clef secrète pour toutes les lettres. Sur l'alphabet circulaire de 26 cases, il fallait toujours avancer de 3 cases. César ne trompant guère que les analphabètes et les esprits médiocres, sa technique a malgré tout été utilisée pendant des siècles. Il a pourtant commis deux erreurs : croire que les gens ne verraient jamais aucun motif particulier se répéter dans les messages chiffrés et croire qu'il pouvait se permettre de choisir son initiale, le C (3), comme secret qui cèlerait à tout



La carte bancaire fait partie des utilisations de codes secrets au quotidien. © I. Maugis

Les communications militaires font appel aux [codes secrets](#) + pour protéger les contenus des messages. Au quotidien, une carte bancaire ou de sécurité sociale Vitale utilise aussi ces codes de protection.



Détail de la machine *Enigma* © B. Lord, 2008
Voici un [détail de la machine Enigma](#) + utilisée par l'armée allemande pendant la seconde guerre mondiale, pour crypter ses messages. On distingue nettement les rotors qui servent à chiffrer et déchiffrer les messages secrets.

jamais l'accès à la pensée secrète de César. Ce secret volé a dû apparaître aux premiers casseurs du Chiffre de César comme le signe intangible qu'ils avaient réussi.

C'est dire l'importance extrême de la « qualité de fabrication » du pseudo-hasard que l'on produit en machine. Il faut que notre secret ne dépende pas de nous : le nom de votre chat ou votre date d'anniversaire sont de mauvais choix pour constituer un bon secret. Un embrouillamini inextricable de lettres minuscules, majuscules, de nombres et de signes de ponctuation fait au contraire un excellent mot de passe.


Le problème mathématique du Chiffre de César vient du fait que toutes les lettres vont subir le même décalage par 3 sur le cercle alphabétique. Chaque lettre ne pouvant se transformer qu'en une seule autre lettre, ce code secret est appelé mono-alphabétique. Par exemple, tous les E vont devenir des H une fois chiffrés. Or, on peut se dire que le E est une lettre qui revient très souvent en latin, et qu'il y a donc de fortes chances pour que la lettre qui revient le plus souvent dans le message chiffré soit un E en clair. On peut ainsi retrouver les correspondances lettres cryptée/en clair avec leurs fréquences d'apparition respectives. Il se produit « une fuite d'information » (notion que l'Américain Claude Elwood Shannon a formalisée le premier en 1948). Il y a un trou dans l'algorithme qui laisse fuir la clef secrète. On détecte un trou de sécurité en essayant de repérer des motifs, souvent subtils, qui se répètent. Si on est un pirate, on va tenter par contre de s'y engouffrer et de voler le secret.


Au XVI^e siècle, le diplomate Blaise de Vigenère a joué les plombiers sur l'algorithme du Chiffre de César. Son algorithme continue pourtant de fuir : il n'a fait que rajouter une rustine, mais une rustine de génie. Vigenère s'est avisé que le problème de l'algorithme de César venait du fait qu'il ne changeait jamais sa clef secrète, parce que le décalage sur le cercle était toujours le même. Alors il s'est dit qu'il fallait aussi « faire tourner la clef », mais sur son cercle à elle : Vigenère choisit un mot (pouvant être inventé) de plusieurs lettres comme clef secrète (César n'utilisait une clef que de longueur 1 lettre, et toujours égale à la lettre C : 3). Ainsi, la clef secrète pour une lettre en clair change à chaque fois, et périodiquement. Une fois qu'on a utilisé la dernière lettre de la clef secrète, on revient à la première pour chiffrer la prochaine lettre en clair, et ainsi de suite. Comme chaque lettre en clair peut potentiellement devenir plusieurs lettres différentes une fois chiffrée, on parle de « code poly-alphabétique ».

Ici, le problème est qu'il y a un motif qui se répète encore dans le message chiffré, parce que chaque lettre de la clef secrète revient périodiquement. Les répétitions dans le message chiffré apparaissent quand il est en phase avec la clef : quand une même suite de lettres du message en clair est chiffrée plusieurs fois avec la même suite de lettres de la clef secrète. En estimant la longueur des suites de lettres qui se répètent une fois chiffrées, on obtient la longueur de la clef. Le même décalage pour chiffrer revenant périodiquement, on peut se dire que le Chiffre de Vigenère n'est finalement qu'un Chiffre de César qui utiliserait périodiquement la même clef. On doit donc simplement pratiquer autant de cassages élémentaires du Chiffre de César qu'il y a de lettres dans la clef secrète. Indépendamment, le mathématicien britannique Charles Babbage eut cette idée en 1854, qu'il ne divulgua pas, jusqu'à ce que Friedrich Kasiski la retrouve par lui-même et la publie en 1863.

Plus généralement, le trou du Chiffre de Vigenère peut se boucher de deux manières :

- soit en utilisant une clef secrète de la même longueur que le texte à chiffrer ;
- soit en « pré-brouillant » les lettres qui restent à crypter à l'aide de lettres déjà cryptées. La première solution est appelée « Chiffre de Vernam » (1917). Mais il est très compliqué de gérer de longues clefs secrètes, aussi ce code secret a-t-il surtout servi pour le Téléphone rouge. Par contre, c'est le seul dont on peut prouver qu'il est étanche : il ne laisse pas fuir une seule goutte de la clef.

La seconde piste fait l'objet de toute l'attention des chercheurs et le nouveau standard mondial depuis 2001, l'[AES](#)  (inventé par les Belges Joan Daemen et Vincent Rijmen), fait encore partie de cette

famille de solutions. La taille des clefs utilisées de nos jours dans l'AES est de 256 bits (les lettres de l'ordinateur valant 0 ou 1). C'est de plus un algorithme qualifié de très sûr car on ne connaît pas d'attaques performantes pour le neutraliser. Le précédent standard, le [DES](#) , mettrait aujourd'hui une petite semaine à être cassé avec des moyens de calcul informatiques raisonnables : il devenait poreux car sa clef n'était longue que de 56 bits.

Références:

<http://interstices.info/crypto-chiffre-lettres>

<http://interstices.info/rsa> quelques liens entre maths et codage.

<http://interstices.info/protocole-cryptographique> une facette applicative pour introduire les concepts

<http://interstices.info/enigma> un point d'entrée historique sur le sujet

<http://interstices.info/expose-crypto> un très bel exposé facilement accessible sur le sujet

<http://interstices.info/secrets-partages> sur les liens crypto image que vous citez