Historique de la cryptanalyse

Caroline Pintoux et Hélène Arnaud

30 octobre 2009

Historiquement, on fait remonter l'invention des codes secrets à Jules César, mais il semble naturel de penser que dès que l'Homme a su écrire et donc transmettre des messages, il a cherché à préserver la confidentialité et l'intégrité de certains d'entre eux aux moyens de *codes* plus ou moins rudimentaires.

1 Les codes secrets dans l'antiquité

- Le tout premier document crypté que l'on connaisse est une tablette d'argile trouvée en Irak et datant du **XVIième siècle av. J.-C.**. Il s'agit d'une recette de poterie gravée sur la tablette par le potier qui a modifié l'orthographe des mots et en a supprimé toutes les consonnes.
- Entre le **Xe et VIIe siècle av. J.-C.** une technique de chiffrement par *transposition* serait attestée en Grèce (notamment par Plutarque et Enée le tacticien) : elle repose sur le changement de position des lettres dans le message, en utilisant un bâton de diamètre déterminé appelée `scytale`. On enroule en hélice une bande de cuir autour de la scytale avant d'y inscrire un message. Une fois déroulé, le message est envoyé au destinataire qui possède un bâton identique, nécessaire au déchiffrement.
- Aux alentours de **600 av. J.-C.**, le roi de Babylone Nabuchodonosor cachait les informations en les inscrivant sur le crâne rasé de ses messagers : une fois que leur chevelure avait repoussé, il envoyait son message, et le destinataire n'avait plus qu'à raser la tête du messager pour y lire l'information.
- À partir du **Vième siècle av. J.-C.**, l'une des premières techniques de chiffrement est utilisée dans les textes religieux par les Hébreux. Il s'agit d'une *substitution* alphabétique inversée ; on remplace chacune des lettres du texte clair par une autre lettre de l'alphabet en procédant comme suit : A devient Z, B devient Y, etc.
- Au **premier siècle av. J.-C.**, le code de César est utilisé dans l'armée romaine : il s'agit d'un code de substitution alphabétique, moins élaboré d'ailleurs que le code précédent : on choisit un nombre n et on décale toutes les lettres de l'alphabet de n vers l'avant : si par exemple $n = 4$, alors A devient D, B devient E etc...
  Ce code pourtant très rudimentaire est réutilisé pendant la **guerre de Sécession** aux Etats-Unis , ainsi qu' **en 1915** par l'armée russe . Une simple analyse de fréquence (certaines lettres, comme le "E" en anglais, apparaissent bien plus souvent que d'autres) permet généralement de trouver l'alphabet de substitution utilisé.

2 Avant le XXième siècle

- Gabriele de Lavinde , secrétaire du pape, écrit **en 1379** un recueil de codes et de clefs, appelé *Nomenclateur* qui sert pendant plusieurs siècles aux diplomates européens pour préserver et transmettre certaines informations.
- Les connaissances de la civilisation arabe dans le domaine de la cryptologie sont exposées dans *Subh al-a sha*, une encyclopédie en 14 volumes écrite par l'Égyptien Al-Qalqashandi en **1412**.
- **En 1467**, le savant italien Leone Battista Alberti explique le premier le principe d'un chiffrement par substitution *polyalphabétique* : au cours du chiffrement, on change plusieurs fois d'alphabet de chiffrement, rendant inutile toute analyse de fréquence. Il utilise pour ce faire un disque à chiffrer.
- Le premier livre imprimé traitant de cryptologie est publié **en 1518** par le moine bénédictin Jean Trithème .
- Un italien publie **en 1553** un recueil de clefs littérales utilisées pour les chiffrements polyalphabétiques, qui sont appelées des *mots de passe* par leur auteur Giovan Battista Bellaso .
- Le francais Blaise de Vigenère met au point **en 1586** une technique élaborée de substitution polyalphabétique inspirée de celle de Trithème qui ne sera déchiffrée qu'**en 1854**. Si on en connaît la clef, cet algorithme est très facile d'utilisation, pour chiffrer comme pour déchiffrer un message, et on peut produire une infinité de clefs qui résisteront à toute analyse statistique. Cette méthode de chiffrement a longtemps prévalu en cryptographie et a résisté à la cryptanalyse pendant presque 4 siècles.
- **Au XVIIième siècle**, le *Grand chiffre du roi Louis XIV* est utilisé à la cour du roi Soleil pour les communications de la plus haute importance. Les historiens disposent de quelques documents codés avec ce "chiffre", et connaître le contenu de ces documents est d'un intérêt historique certain. Hélas, faute d'information même statistique sur la nature des textes, et de connaissance ne serait-ce que de quelques mots de leur contenu, la solution de ce mystère n'a surgi que **vers 1893** quand Étienne Bazeries délivra finalement les historiens après trois siècles de perplexité.
- Le principe du disque à chiffrer est encore utilisé **en 1817** dans l'armée anglaise .
- Un pionnier du télégraphe, Charles Wheatstone , apporte sa contribution à la cryptologie **en 1854** en inventant le chiffrement de Playfair, du nom de celui qui l'a fait connaître. Cette technique est basée sur une méthode de substitution diagrammatique consistant à remplacer un couple de lettres adjacentes par un autre couple choisi dans une grille qui constitue la clé.
- **En 1883**, le cryptologue hollandais Kerckhoffs comprend que pour garantir la sécurité d'une information, il faut une *clef*, dont l'élaboration et la protection deviendra à la base de tout système de cryptage.

3 XXième siècle

- **En 1919**, le brevet d'une machine à chiffrer électromagnétique est déposé Hollande par un ingénieur, Hugo Alexander . Son idée sera reprise en Allemagne sous le nom de *machine Enigma* . Destinée aux civils, cette invention est un fiasco commercial,

mais les militaires allemands s'en serviront pendant la Seconde Guerre Mondiale : de nombreuses histoires cocasses sont associées à cette machine, à ses points forts et ses failles.

- Bien que les moyens de chiffrements électromécaniques, tels que la machine Enigma, aient prouvé leur efficacité en termes de sécurité, ils n'en restent pas moins encombrants et lents car nécessitant une double saisie des messages. Ces deux inconvénients majeurs rendant ce procédé quasiment inexploitable en milieu hostile, ils poussèrent les Américains à chercher un moyen de chiffrement assurant une communication efficace sur le terrain lors de la guerre qui les opposa aux Japonais : l'ingénieur américain Philip Johnston pensa à utiliser la langue *Navajo* comme procédé cryptographique. La méconnaissance quasi totale de cette langue ainsi que sa construction grammaticale très particulière, la rendant impénétrable aux étrangers, décidèrent de son utilisation. Voilà comment les Parleurs-de-code (Windtalkers) navajos prirent part à la campagne du Pacifique. Leur bravoure au combat fut reconnue de manière officielle par le gouvernement américain lorsqu'il leur dédia, en 1982, la journée du 14 août.

4 Et aujourd'hui...

Depuis les années 80, la mécanique quantique, qui décrit le monde à l'échelle des particules, a également fait son entrée dans la panoplie de la cryptologie. Dans cet univers probabiliste, d'étranges événements se produisent : à l'échelle macroscopique, mesurer la vitesse d'un objet (une voiture par exemple) ne modifie pas son état, mais à l'échelle d'une particule, ce n'est plus le cas. Cette propriété fondamentale est l'une des bases de la *cryptologie quantique*.