

Date: Dimanche 17 octobre 2004 à 01:35:06
Sujet: 7 Cryptographie

Tout sur la cryptographie

La cryptographie est l'art de crypter des messages.

[Le chiffre de César](#) ; [Le carré de Polybe](#)

[Blaise De Vigenère](#) Histoire de la Cryptographie
La cryptographie (du grec Kruptos : cacher , et de Graphein : écrire) a toujours existé , ce sont les Spartiates qui ont les premiers compris qu'il fallait plus que de la force pour gagner des batailles. C'est pourquoi ils essayèrent de trouver des moyens de s'envoyer des messages que l'ennemi ne pourrait pas intercepter. Mais ils comprirent très vite qu'il était très difficile d'inventer de nouveaux moyens de communication. Ils essayèrent alors de cacher l'existence même du message , c'est la steganographie (du grec Steganos : imperceptible et de Graphein : écrire). Ils inventèrent donc la Scytale (voir dessin ci dessous).

Environ 400 ans avant JC , Hérode un journaliste grec extrêmement fouineur raconte que Histié (qui vivait en Perse) a envoyé un esclave à Aristogoras (un tyran grec qui était aussi le gendre de Histié). Chez Aristogoras l'esclave déclara seulement : "Rase moi le crâne". Aristogoras fit alors venir un barbier et on rase la tête de l'esclave , sur le crâne rasé de l'esclave on peut alors voir une phrase tatouée : "Histié conseille à Aristogoras de se révolter contre les Perses." Mais ce système est beaucoup trop long car il faut raser , tatouer et attendre la repousse des cheveux. Imaginez sur un champ de bataille si l'on doit donner des ordres à d'autres régiments , il faudrait un esclave déjà prêt (tatoué) pour chaque ordre différent.

Vers 150 ans av JC , Polybe un historien Grec a l'idée d'un procédé de cryptage [le carré de Polybe](#).

Peu de personne semble avoir utilisé [le carré de Polybe](#) pourtant ses atouts sont nombreux et rendent très difficile la cryptanalyse.

Plus tard dans l'antiquité un cryptographe dont vous connaissez tous le nom , Jules César invente une méthode de cryptage simple et rapide : [Le code \(ou le chiffre\) de César](#). Il s'en servait pour écrire ses amis politiques sans dangers. La méthode utilisée est une méthode par substitution car chaque lettre est remplacée par une autre. César remplaçait chaque lettre par celle située

trois rang plus long dans l'alphabet. Bien sur on peut deplacer d'autant de rang que l'on veut. Pour plus de precisions que ce soit technique ou historiques , allez sur chaque page des differentes methodes de cryptographie. Un peu de Vocabulaire

Le texte texte après avoir été dècrypter ou avant d'avoir été crypté est un "Texte Clair".

Une fois crypté on dit qu'il est chiffré , codé ou brouillé.

Lorsque le texte a été chiffré on l'appelle alors cryptogramme.

Lorsque l'on retrouve le texte clair c'est que l'on a decodé , dechiffré , decrypté ou cassé le code.

Lorsque l'on cherche la methode pour dechiffrer un texte crypté c'est une cryptanalyse.

La personne qui fait une cryptanalyse est un cryptanalyste.

Une methode pour chiffré un texte est un code ou un chiffre (ex : [Le chiffre de Càsar](#)).

Le fait de chiffrer et de dechiffrer est la cryptographie ou cryptologie.

Publication de Tout sur l'informatique - Programmation C#, Sècuritè, Divx, P2P:
<http://www.zmaster.fr>

URL de cette publication

<http://www.zmaster.fr/modules.php?name=News&file=article&sid=37>