Date: Dimanche 17 octobre 2004 à 02:35:06
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 Vignenère Histoire de la Cryptographie
La cryptographie (du grec Kruptos : cacher , et de Graphein : écrire) a toujours existée , 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 essayérent 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 essayérent alors de cacher l'existence même du message , c'est la steganographie (du grec Steganos : impénétrable et de Graphein : écrire). Ils inventérent donc la Scytale (voir dessin ci dessous).

Environ 400 ans anvant JC , Hérote un journaliste grec extremement fouineur raconte que Histiée (qui vivait en Perse) a envoyé un esclave à Aristogoras (un tyran grec qui était aussi le gendre de Histiée). Chez Aristogoras l'esclave déclare seulement : "Rase moi le crâne". Aristogoras fait 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 tatoué : "Histiée conseille à Aristogoras de se revolter sontre les Perses." Mais ce systéme 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 a d'autres régiments , il faudrait un esclave deja pret (tatoué) pour chaque ordre different.
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 methode de cryptage simple et rapide : Le code (ou le chiffre) de César. Il s'en servait pour écrire à ses amis polititiens sans dangers. La methode utilisé est une methode par substitution cr chaque lettre est remplacé par une autre. César remplacait chaque lettre par celle situé

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

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

URL de cette publication
http://www.zmaster.fr/modules.php?name=News&file=article&sid=37