CRYPTOGRAPHIE

La cryptographie est l'ensemble des techniques qui permettent de chiffrer et de déchiffrer un message, dont le contenu ne doit être connu que de son expéditeur et de son destinataire.

Son déchiffrement par un tiers n'est pourtant pas impossible. Il nécessite la connaissance d'un certain nombre de données fondamentales.

Au cours des siècles, de nombreux systèmes cryptographiques ont été mis au point, de plus en plus perfectionnés, de plus en plus astucieux !

Comment procéder à une attaque d'un chiffre ?

Analyse statistique de la fréquence d'apparition des lettres :

Dans les textes longs, les lettres n'apparaissent pas avec la même fréquence. Ces fréquences varient suivant la langue utilisée. En français, les lettres les plus rencontrées sont dans l'ordre : E S A I N T R U L O D C P M V .... avec les fréquences :

E	S	A	I	N	T	R	U	L	O	D
14.69%	8.01%	7.54%	7.18%	6.89%	6.88%	6.49%	6.12%	5.63%	5.29%	3.66%

Voici la méthode d'attaque : dans le texte crypté, on cherche la lettre qui apparaît le plus, et si le texte est assez long cela devrait être le chiffrement du E, la lettre qui apparaît ensuite dans l'étude des fréquences devrait être le chiffrement du S, puis le chiffrement du A... On obtient des morceaux de texte clair sous la forme d'une texte à trous et il faut ensuite deviner les lettres manquantes.

Enigme de la semaine des maths 2020 :

VL XQH PDFKLQH HVW FHQVHH HWUH LQIDOOLEOH,

.....

HOOH QH SHXW SDV DXVVL HWUH LQWHOOLJHQWH

.....

Principe de ce chiffrement : .....

Ce chiffrement s'appelle le chiffre de César, il a été utilisé par Jules César pendant la guerre des Gaules (101-44 av JC) pour envoyer des messages chiffrés à Ciceron. Il fut très solide jusque dans les années 800.

Inconvénients de cette méthode de chiffrement :

- La fréquence d'apparition des lettres dans un texte nous renseigne très vite sur le décodage de certaines lettres
- Il n'y a que 26 clés possibles. (26 décalages possibles), il suffit de les tester toutes pour déchiffrer le message.

Afin que chaque lettre ne soit pas chiffrée par le même symbole, **Blaise de Vigenère** (1523-1596) diplomate et cryptographe français améliora le chiffre de César en utilisant des clés différentes suivant la position des lettres.

On choisit un mot : LOIRE
la lettre L est la 12e lettre de l'alphabet, ainsi la 1ère lettre du message sera décalée de 11 lettres vers la droite.
la lettre O est la 15e lettre de l'alphabet, ainsi la 2e lettre du message sera décalée de 14 lettres vers la droite , etc ...