CRYPTOGRAPHIE

À RETENIR

Définition

L'Homme a toujours ressenti le besoin de dissimuler des informations, bien avant même l'apparition des premiers ordinateurs et des machines à calculer. C'est dans ce but qu'est née la **cryptographie**. Ce mot désigne l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire, permettant de les rendre inintelligibles sans une action spécifique.

La cryptographie est aujourd'hui omniprésente : dans le secteur médical (pour protéger des données), dans les communications (via HTTPS par exemple), dans les transactions et les cryptomonnaies, etc.

EXEMPLE

L'un des exemples antiques les plus célèbres remonte à Jules César, qui chiffrait ses communications à l'aide d'une technique aujourd'hui appelée « code de César ».

Le code de César est un chiffrement par décalage : chaque lettre est remplacée par une lettre située à une certaine distance dans l'alphabet. César utilisait une distance de 3.

EXERCICE 1

1. Déchiffrer le message suivant : « OHV PDWKV F'HVW WRS » . . . . . .
2. Chiffrer un message, et le faire deviner à votre voisin. Vous pouvez utiliser un autre décalage ! . . . . . .

. . . . . .

EXEMPLE

Dans le film *Imitation game*, il est question d'une autre technique de chiffrement : le code Beale. Il repose sur le principe suivant :

1. On choisit un texte de référence. Il s'agit de la « clé » de notre chiffrement.
2. Pour chaque lettre du message à coder, il faut trouver un mot du texte « clé » qui commence par cette lettre. La position du mot dans le texte donne le nombre qui code la lettre.

EXERCICE 2

Voici un texte clé.

Aujourd'hui, le ciel est bleu, le vent est rapide, et le soleil est orangé.

1. L'utiliser pour déchiffrer le mot suivant : « 5 9 1 7 14 ». . . . . .
2. Utiliser ce texte (ou un autre de votre choix) pour chiffrer un mot que vous ferez deviner à votre voisin.

. . . . . .

EXEMPLE

Dans son *Traicté des chiffres ou secrètes manières d'escrire*, paru en 1585, Blaise de Vigenère expose une technique de chiffrement dont il faudra plusieurs siècles pour venir à bout. Elle repose ici encore sur une clé (secrète cette fois-ci), mais aussi sur un carré de lettres.

La machine Enigma, utilisée par les allemands pendant la Seconde Guerre mondiale pour chiffrer leurs communications, utilise une technique proche de celle-ci.

Pour plus d'informations, se référer au lien suivant : `https://bibmath.net/crypto/index.php?action=affiche&quoi=poly/vigenere`.

À RETENIR

Définition

Une autre manière de protéger un message est de le cacher par des techniques de **stéganographie**. Avec ce type de procédés, le message n'est pas modifié ; il est simplement caché (dans une image, dans une musique, dans une vidéo, dans un texte, etc).

EXERCICE 3

Voici un message envoyé par un espion allemand au cours de la Seconde Guerre mondiale (et sa traduction à côté).

Message original	Traduction
Apparently neutral's protest is thoroughly discounted and ignored. Ismam hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.	Apparemment la protestation des pays neutres est totalement ignorée. Isman frappe fort. L'issue du blocus donne des prétextes pour un embargo sur certains produits, mis à part graisses animales et huiles végétales.

En prenant la deuxième lettre de chaque mot, on obtient : « Pershing sails from NY June 1 ». Que peut bien vouloir dire ce message ? .....

.....

EXERCICE 4

Aide Tintin à trouver le message caché !

.....

.....

.....

.....

.....

.....

Solution : `https://utc.fr/ wschon/sr06/crypto/steganographie_1.htm`.