CHIFFRE DE VIGENERE

Niveau : terminale générale maths expertes.
Lien avec le programme : congruences.
Lien avec *Les maths au quotidien* : **Codages**.

Le **chiffre de Vigenère** est une méthode de cryptographie utilisant un chiffrement par substitution poly-alphabétique dans laquelle une même lettre du message à coder peut, suivant sa position dans le texte, être remplacée par des lettres différentes, contrairement à un chiffrement mono-alphabétique comme le simple chiffre de César ou le carré de Polybe. Ce chiffre résiste ainsi à l'analyse des fréquences (voir « Déchiffrage fréquentiel »), ce qui est un avantage précieux sur les chiffrements mono-alphabétiques.
Il est nommé ainsi au XIX^{e} siècle en référence au diplomate du XVI^{e} siècle Blaise de Vigenère, qui le décrit (intégré à un chiffrement plus complexe) dans son *traité des chiffres* paru en 1586.

Ce chiffrement utilise une clé, qui est un mot ou groupe de mots. On écrit la clé autant de fois que nécessaire en dessous du texte à coder, lettre à lettre. On attribue à chaque lettre de l'alphabet un nombre entre 0 et 25 (0 pour A, …, 25 pour Z).

A. Chiffrement

On note x le nombre correspondant à la lettre à chiffrer, y le nombre correspondant à la lettre de la clé.
La lettre chiffrée sera obtenue avec le nombre z tel que $z \equiv x + y\ [26]$.

Voyons un exemple et chiffrons le mot « quotidien » avec la clé « modulo ».
Remplir le tableau suivant :

Clair	Q	U	O	T	I	D	I	E	N
x									
clé	M	O	D	U	L	O	M	O	D
y									
z									
Codé									

B. Déchiffrement

On veut déchiffrer « OFBJECSFDJSWQ », codé avec la clé MODULO.
Pour déchiffrer la lettre, on connaît z et y et on cherche x tel que $z \equiv x + y\ [26]$ soit $x \equiv z - y\ [26]$.

Codé																
z																
clé																
y																
x																
Clair																

C- Utilisation d'un tableur

On veut chiffrer « VIGENERE, ON LUI DIT ″CIMER″ » avec la clé MODULO à l'aide d'un tableur.
Pour cela, on utilise :

- La fonction **CODE**, qui associe à la lettre son code ASCII dans lequel A prend la valeur 65, B la valeur 66, ..., Z la valeur 90 ;
- La fonction **MOD(N;M)**, qui calcule le reste dans la division euclidienne de N par M ;
- La fonction **CAR**, qui retranscrit les nombres entiers compris entre 65 et 90 en lettres majuscules.

1. Saisir dans la zone de cellules **A1:H1** les lettres de la phrase, et dans la zone **A2:H2** la clé **MODULO** en répétant les lettres.

2. Expliquer pourquoi l'instruction saisie en **A3:H3** : =CAR(MOD(CODE(A1)-65 + CODE(A2)-65;26)+65) permet de chiffrer la lettre **V**.

3. Chiffrer alors la phrase à l'aide du tableur.

Voici un message crypté :

E C Y U R E C A W K S R P M T E W O W M H P B I K U U W V R V F M

4. a. Entrer-le dans la zone de cellules **A6:H6**.

b. Dans la zone **A7:H7,** vous rentrerez la clé (en la répétant), **une fois que vous l'aurez.**

c. Quelle formule, modifiée à partir de celle de la question 2., faut-il entrer en A8, à étirer vers la droite jusqu'à H8**,** pour déchiffrer le message ?

5. Déchiffrer le message et répondre. Pour cela, il faut le « précieux sésame ».

Point info :

Il y a eu une période où des passages entiers d'œuvres littéraires étaient utilisés comme clé pour chiffrer les plus grands secrets : les deux correspondants avaient bien sûr un exemplaire du même livre.
Il existe des méthodes pour tenter de déchiffrer un texte crypté par le chiffre de Vigenère sans connaitre la clé. On peut citer la méthode de Kasiski ou bien celle de l' « indice de coïncidence » (voir sur le net pour plus de détails). Ces méthodes demandent un texte suffisamment long vis-à-vis de la clé.
Dans le cas où la clé est de longueur égale à celle du message, aléatoire, et n'est utilisée qu'une seule fois, tous les textes de longueur égale à celle du message chiffré sont équiprobables : le chiffre ne peut être cassé ; c'est le ***chiffre de Vernam***, ou ***masque jetable***.
Hélas, le chiffre de Vernam est compliqué en pratique à mettre en œuvre et il ne l'a été que dans des cas très particuliers. D'abord, il exige qu'une clé ne serve qu'une seule fois, car sinon on peut extraire une certaine quantité d'information. Ensuite, le chiffre de Vernam exige des clés extrêmement longues, et l'échange des clés entre protagonistes, qui doit être ultra sécurisé, est donc difficile à réaliser. Enfin, les clés utilisées doivent être parfaitement aléatoires, ce qui n'est pas facile à garantir.
Il fut par exemple utilisé pour sécuriser le téléphone rouge, ligne directe entre la Maison Blanche et le Kremlin du temps de la guerre froide. Les clés circulaient dans les valises diplomatiques, transportées dans des avions bourrés d'agents secrets. Et on raconte que pour produire des clés aléatoires, les Soviétiques employaient des "lanceurs de dés" : leur travail consistait à lancer des dés toute la journée et à noter le résultat.
Un chiffrement à la main par la méthode du masque jetable fut notamment utilisé par Che Guevara pour communiquer avec Fidel Castro.