

Activité 1 : Le Chiffre de César

En Cryptographie, le chiffrement par décalage, aussi connu sous le nom de chiffre de CÉSAR, est une méthode de chiffrement très simple utilisée par JULES CÉSAR (100 av. J.-C. - 44 av. J.-C.) dans ses correspondances secrètes. Elle consiste à remplacer chaque lettre d'une phrase par une lettre à distance fixe dans l'ordre de l'alphabet.

Par exemple, avec un décalage de trois lettres, la A devient D, le B devient E, etc.

1. Coder le nom OLYMPE à l'aide du décalage de trois lettres. On pourra pour cela compléter le tableau ci-dessous.

Texte original	O	L	Y	M	P	E
Texte codé	R					

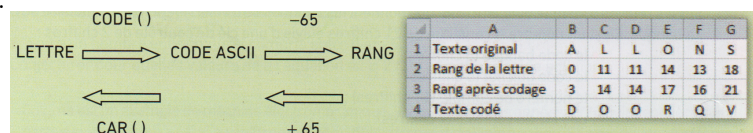
2. On veut automatiser cette méthode sur un tableur. Pour cela, on associe à chaque lettre son rang dans l'alphabet, en convenant que le rang de A est 0, celui de B est 1 et ainsi de suite jusqu'au rang de Z qui est 25.

On utilise le code ASCII : dans un tableur, la formule `=CODE("lettre")` permet d'obtenir le code ASCII d'une lettre donnée. Par exemple, la formule `=CODE("C")` donne 67.

La formule `=CAR(nombre)` donne le caractère correspondant au code ASCII donné. Ainsi `=CAR(67)` affiche la lettre C.

Les lettres majuscules ont un code ASCII compris entre 65 (pour A) et 91 (pour Z).

Pour avoir le rang d'une lettre de l'alphabet avec la convention rang 0 pour A et rang 25 pour Z, on suit le schéma suivant :



On souhaite coder le message ALLONS CONQUÉRIR LA GAULE en utilisant une feuille de tableur.

- (a) Quelles formules doit-on entrer dans les cellules B2, B3 et B4 et copier vers la droite ?
 - (b) Compléter le tableau pour coder le message.
 - (c) Utiliser ce tableau pour coder le mot OLYMPE. Quel problème apparaît ? Expliquer.
 - (d) Modifier la formule de la cellule B3 pour permettre le codage de ce mot. Vérifier ensuite avec le mot EGYPTÉ.
3. On souhaite décoder le message MHWHC'OHDXAOLRQV.
 - (a) Quelle formule de tableur permettra de passer du rang de la lettre codée au rang de la lettre décodée ?
 - (b) Décoder le message.

Activité 2 : Chiffrement affine

Chaque lettre, en majuscule, est remplacée par son rang entre 0 et 25 dans l'alphabet. On note x ce rang, avec $0 \leq x \leq 25$.

Le rang $r(x)$ de la lettre chiffrée est alors le reste de la division euclidienne de $y = ax + b$ par 26.

Le couple d'entiers (a, b) s'appelle la clé du codage.

1. En utilisant le tableur et en vous inspirant de l'activité 1, construire un tableau permettant de coder le vers de VICTOR HUGO : « ET S'IL N'EN RESTE QU'UN JE SERAI CELUI-LÀ ».

Les valeurs de a et de b doivent pouvoir être changées facilement et le tableau doit être recalculé automatiquement. On commencera par $a = 7$ et $b = 17$.
2. (a) Le chiffrement est-il modifié si l'on prend $a = 5$ et $b = 11$? $a = 31$ et $b = 11$? $a = 265$ et $b = 37$? Que peut-on conjecturer ?
 - (b) Soient a, b, a' et b' des entiers. Démontrer que si $a - a'$ et $b - b'$ sont des multiples de 26, les chiffrements avec les clés (a, b) et (a', b') sont identiques.
 - (c) De combien de clés dispose-t-on en prenant $1 \leq a \leq 25$ et $0 \leq b \leq 25$.
3. Le cas $a = 13$.
 - (a) Tester ce cas sur le tableur. Que remarque-t-on ?
 - (b) Soient x et x' les rangs de deux lettres de l'alphabet. Démontrer que $r(x) - r(x')$ est un multiple de 13. Quelle est la conséquence sur le codage du texte ?
 - (c) Pour quelle autre valeur de a peut-on avoir un problème similaire ? Tester votre réponse sur tableur.