Et s'il n'en reste qu'un ... (Source : math'x)

Question : Savez-vous comment se termine ce célèbre vers de Victor Hugo, titre de l'activité ?
Réponse : **wrfrenvpryhvyn**
Cette réponse est cryptée, le chiffrement a été effectué en ROT13, système souvent employé sur Internet pour donner la fin du nom d'un film ou la réponse à une énigme.
Quel est le principe de ce chiffrement et du déchiffrement ? Comment l'automatiser ?

Fonctions « tableur » pour passer d'une lettre en majuscule à son rang dans l'alphabet et inversement :


## Chiffrement de César

Dans le chiffrement de Jules César, chaque lettre est remplacée par la lettre qui la suit trois rangs plus loin dans l'alphabet, les trois dernières lettres étant remplacées par les trois premières lettres de l'alphabet.

Réaliser une feuille de tableur permettant de coder la célèbre phrase de Socrate : « connais-toi toi-même ».
Vous ferez apparaître une ligne avec la légende « Texte en clair », une autre avec le rang de la lettre, puis le rang après chiffrement et pour terminer une ligne correspondant au texte chiffré.
Réaliser un tableau pour le décodage.

## le ROT 13

Le ROT 13 consiste en un décalage de 13 rangs. Modifier la feuille de calcul précédente pour trouver la fin du vers de Victor Hugo en déchiffrant la réponse. Vérifier que dans le cas du ROT 13, chiffrer un message ou le déchiffrer revient au même. Expliquer ce résultat.

## Le chiffrement de Vigenère

Blaise Vigenère (1523-1596), traducteur, diplomate et cryptographe, expose dans son « traité des chiffres » une méthode de chiffrement qui repose sur une clé (constituée d'un ou plusieurs mots). On répète les lettres de cette clé sous le texte à chiffrer, écrit sans accent ni ponctuation, ni séparation. Pour chiffrer une lettre du texte, on la décale dans l'alphabet d'autant de lettres que le rang -entre 0 et 25- de la lettre correspondante de la clé.
Prenons comme clé : **VICTORHUGO**

Réaliser une feuille de calcul pour chiffrer le vers complet de Victor Hugo.
Quels sont les avantages de ce chiffrement ? Peut-on envisager un décodage simple comme dans les méthodes précédentes ?

## Le chiffrement affine

Chaque lettre en majuscule est remplacée par son rang entre 0 et 25 dans l'alphabet, les autres signes sont supprimés (espace, trait d'union, etc.). On nomme $x$ le rang de la lettre en clair, $0 \leqslant x \leqslant 25$.
Le rang $r(x)$ de la lettre chiffrée est alors le reste dans la division euclidienne de $y = ax + b$ par 26.
Le couple d'entiers $(a, b)$ s'appelle la clé du codage.

1. On choisit $a = 7$ et $b = 17$.
   Réaliser un tableau pour coder le vers de Victor HUGO. Les valeurs de $a$ et de $b$ doivent pouvoir être changées dans les cellules $C1$ et $F1$ et le tableau être recalculé automatiquement.
2. Le chiffrement est-il modifié si l'on prend $a = 5$ et $b = 11$ ? $a = 31$ et $b = 11$ ? $a = 265$ et $b = 37$ ? Soit $a, a', b, b'$ des entiers. Démontrer que si $a \equiv a'\ (26)$ et $b \equiv b'\ (26)$, les chiffrages avec les clés $(a, b)$ et $(a', b')$ sont identiques. De combien dispose-t-on de clés en prenant $1 \leqslant a \leqslant 25$ et $1 \leqslant b \leqslant 25$ ?
3. Cas $a = 13$.
   (a) Tester ce cas sur le tableur.
   (b) Soit $x$ et $x'$ les rangs de deux lettres de l'alphabet. Démontrer que $r(x) - r(x')$ est un multiple de 13. Quelle en est la conséquence sur le codage du texte ?
   (c) Pour quelle autre valeur de $a$ peut-on rencontrer un problème similaire ? Tester votre réponse sur tableur.