Chiffrement affine

Chaque lettre $A, B \ldots, Z$ est codé par son rang entre 0 et 25.

On choisit deux nombres a et b. (On peut se restreindre entre 0 et 25 au sens large car on retrouve ensuite les même résultats).

On note x le rang d'une lettre et $r(x)$ le reste de la division euclidienne de $y = ax + b$ par 26. La lettre correspondante est la lettre codée.

Exemple : *On se fixe* $a = 17$ *et* $b = 2$. *On veut coder la lettre* K, *elle correspond au rang* 10.
$17 \times 10 + 2 \equiv 16[26]$. *La lettre codée est donc* Q.

- ✓ **Si a n'est pas premier avec 26**
  Deux lettres différentes ($x \neq x'$) peuvent avoir le même codage. Dans ce cas, cela ne permettra pas un décodage.
  En effet, $r(x) - r(x') = 26(q - q') + a(x - x')$ (q et q' étant les quotients respectifs dans la division euclidienne de a et de a' par 26). En choisissant deux nombres x et x' tels que $x - x' = \frac{26}{pgcd(a\,;26)}$, on obtient $r(x) - r(x') = 26k$.
  Or, $-25 \leq r(x) - r(x') \leq 25$ donc $r(x) = r(x')$.

- ✓ **Si a est premier avec 26**
  Soient deux nombres x et x' tels que $r(x) = r(x')$.
  Alors $a(x - x') = 26(q - q')$. Or $pgcd(a\,;26) = 1$, donc d'après le théorème de Gauss, $26/\, x' - x$.
  Or $-25 \leq r(x) - r(x') \leq 25$ donc $x = x'$.
  Deux lettres différentes ($x \neq x'$) ne peuvent donc pas avoir le même codage. On a donc une injection de $[\![0\,;25]\!]$ dans lui-même et par suite (de par les cardinaux), une bijection, ce qui rend le décodage possible.

Pour décoder :

On peut appliquer le même principe avec un chiffrement affine de clé $(a'; b')$ tels que
$\begin{cases} aa' \equiv 1[26] & a' \text{est l'inverse de } a \text{ modulo } 26 \\ b' \text{ est le reste de la division euclidienne de } a'(26 - b) \text{ par } 26 \end{cases}$

Exemple : *On se fixe* $a = 17$ *et* $b = 2$. *L'inverse de* $a = 17$ *modulo* 26 *est* $a' = 23$.
$a'(26 - b) \equiv 6\ [26]$.
On veut décoder la lettre S, *elle correspond au rang* 18.
$23 \times 18 + 6 \equiv 4\ [26]$. *La lettre décodée est donc* E.

Fichier tableur automatisant codage et décodage