

Exemple de codage par exponentiation

On affecte à chaque entier compris entre 0 et 30 une lettre de l'alphabet ou un autre symbole (on affecte A à 0, B à 1, ..., Z à 25, α à 26, β à 27, γ à 28, δ à 29 et ε à 30), puis on fait subir à chacun de ces entiers x la transformation f suivante : $x \mapsto y$, où y est le reste dans la division euclidienne par 31 de x^7 .

On note $\mathcal{E} = \{0 ; 1 ; 2 ; \dots ; 30\}$.

La clé de ce codage est 31.

a) Coder le mot GERMAINE.

b) Montrer que 7 et 30 sont premiers entre eux et écrire l'égalité de Bézout correspondante.

c) En utilisant le petit théorème de Fermat, montrer que, si $f(x) = f(x')$, alors $x = x'$.
En déduire que deux éléments différents de \mathcal{E} ont deux images différentes par f

d) Soient x et y éléments de \mathcal{E} tels que $y \equiv x^7 \pmod{31}$.
Montrer que $y^{13} \equiv x \pmod{31}$.

La clé de décodage est donc 13.

e) Décoder alors le mot YCE γ QN.