Crypto

Affine

message "BONJOUR"

clef $(a;b)$ $\quad a \in \mathbb{Z}_{26}^* \quad b \in \mathbb{Z}_{26}$

chiffrer $f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$

$z \longmapsto (a \cdot z + b) \bmod 26$

On note $a\_$ l'inverse de a mod 26.

$az+b = z'$

$az = z' - b$

$(a\_ \cdot a)z \overset{?}{=} a\_(z'-b)$

$\downarrow \bmod 26$

$1 \cdot z = a\_(z'-b) \bmod 26$

Dechiffrer $f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$

$z \longmapsto a\_ \cdot (z'-b) \bmod 26$

Exemple : $(a;b) = (3;13)$

$3 \in \mathbb{Z}_{26}$

$3 \cdot 9 = 27 \equiv 1 \bmod 26$

L'inverse de 3 mod 26 est 9.

Chiffrer: $z \longmapsto (3 \cdot z + 13) \bmod 26$

Déchiffrer: $z \longmapsto 9 \cdot (z - 13) \bmod 26$

$C \leftarrow 2$

$f(2) = 3 \cdot 2 + 13 = 19 \bmod 26$ (mod 26)

Chiffrer

$19 \rightarrow ?$

$\rightarrow 19$

$f(19) = 9 \cdot (19 - 13) \bmod 26$

$= 9 \cdot 6 \bmod 26$

$= 54 \bmod 26$

$= (2 \cdot 26 + 2) \bmod 26 = 2 \bmod 26$

$2 \rightarrow C$