César

Algorithme ← PUBLIC

RSA
DH
AES

Clef ← PRIVÉ

César → $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$

→ clef : $e \in \mathbb{Z}_{26}^*$ 25 clefs

BONJOUR

↓

M

César, $c = 11$

A B C D E F G H I J K L M N ...

L M N ...

A B C ...

↓ ↓ ↓

0 1 2

$m = [1; 14; \dots]$

$ch = [12; 25; \dots]$

$f(z) = (z + c) \bmod 26$

lettre

n

clef

↓
MZ

$z \in \mathbb{Z}_{26}$ $\qquad f_c : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$

$z' = f(z) = (z + c) \bmod 26$ $\qquad$ avec $c \in \mathbb{Z}_{26}^*$

$z = f^r(z') = (z' - c) \bmod 26 = (z' + c') \bmod 26$

$(c + c') \equiv 0 \bmod 26$

$\boxed{c' = 26 - c}$

Chiffrement affine

Monoalphabétique

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

$$z \longmapsto (a \cdot z + b) \bmod 26 \quad a, b \in \mathbb{Z}_{26}$$

Quels sont les inversibles de $\mathbb{Z}_{26}$?

$$a \cdot a' \equiv 1 \bmod 26$$

$$az + b = z' \quad \bmod 26$$

$$az = z' - b$$

$$z = a' \cdot (z' - b) \quad ?$$

$\exists ? \, a'$ tq. $a' \cdot a \equiv 1 \bmod 26$