

César

Algorithme

← PUBLIC

RSA

DH

AES

Clef

← PRIVÉ

César $f: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$

clef: $c \in \mathbb{Z}_{26}^*$

25 clefs

BONJOUR

César, $c = 11$

↓
M

1
A B C D E F G H I J K L M N O ...
L M N ...

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

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

lettre
↓
 $f(z) = (z + c) \bmod 26$

↑
A B C ...
↓ ↓ ↓
0 1 2

11
↑
clef

↓
MZ

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

$$f_c: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

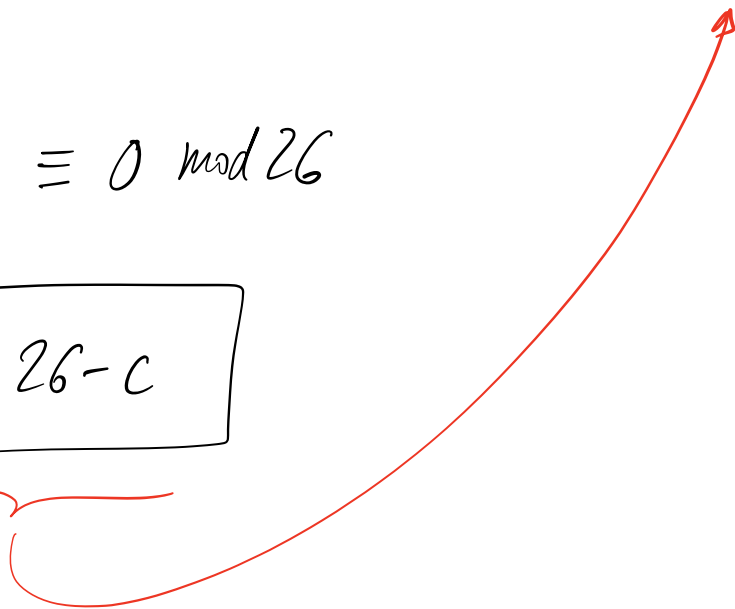
$$z' = f(z) = (z + c) \pmod{26}$$

$$\text{avec } c \in \mathbb{Z}_{26}^*$$

$$z = f^{-1}(z') = (z' - c) \pmod{26} = (z' + c') \pmod{26}$$

$$(c + c') \equiv 0 \pmod{26}$$

$$c' = 26 - c$$



Chiffrement affine

Monalphabétique

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

$$z \longmapsto (2 \cdot z + 6) \bmod 26 \quad 2, 6 \in \mathbb{Z}_{26}$$

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

$$2 \cdot 2' \equiv 1 \pmod{26}$$

$$2z + 6 = z'$$

mod 26

$$2z = z' - 6$$

$$\exists ? \ 2' \text{ tq. } 2' \cdot 2 \equiv 1 \pmod{26}$$

$$z = 2' \cdot (z' - 6) \quad ?$$