

WDXSHVHFUHW
TAUPE SECRET

Vient d'un message

Décalage de César

XHFWDSHVUXS
VEC

Aléatoire

A' déchiffrer

A → D
B → E
C → F
D → G
E → H
⋮

ABCDEF GHIJKL MN¹⁵OP¹⁹QR²⁰STUV²³W²⁴XYZ
← DEFGHIJKL MNOPQR¹⁵STUV¹⁹W²⁰XYZ ABC →

X → A
Y → B
Z → C

Cadre théorique

26 lettres

$$\mathbb{Z}_{26} = \{ 0, 1, 2, \dots, 25 \}$$

↑ modulo 26

ABCDEF... Z
0 1 2 3 4 5 25

TAUPE SECRET

$$[19; 0; 20; 15; \dots] \downarrow f$$

$$f(n) = n + 3 \pmod{26}$$

$$f: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$
$$n \mapsto n + 3 \pmod{26}$$

$$X$$
$$\downarrow$$
$$23$$

$$f(23) = 23 + 3 \pmod{26}$$
$$= 26 \pmod{26}$$
$$= 0 \pmod{26}$$
$$\downarrow$$
$$A$$

$$\square \square \quad \dots \quad \square \square$$
$$26 \cdot 25 \quad \dots \quad 2 \cdot 1 = 26!$$

→ Lundi 30/03/2026:

3.3.1 et 3.3.13