

Correction du DM d'arithmétique sur le chiffrement affine

Partie A

1) $W \rightarrow 22 \rightarrow g(22) = 11 \times 22 + 8 = 250 \rightarrow 250 \equiv 16(26) \rightarrow Q$
donc la lettre W est codée en la lettre Q

2) si $11x \equiv z(26)$ donc $19 \times 11x \equiv 19z(26)$ On $19 \times 11 = 209 \equiv 19 \times 11 + 1$
donc $209 \equiv 1(26)$ d'où $19 \times 11x \equiv 1x \equiv x(26)$
donc $x \equiv 19z(26)$

Réciproquement si $x \equiv 19z(26)$ alors $11x \equiv 11 \times 19z(26)$
d'où $11x \equiv z(26)$ car $11 \times 19 \equiv 1(26)$ Ainsi $11x \equiv z(26) \Leftrightarrow x \equiv 19z(26)$

b) $11x + 8 \equiv y(26)$ d'où $11x \equiv y - 8(26) \Leftrightarrow x \equiv 19(y - 8)(26)$
d'après la question précédente

d'où $x = 19y - 19 \times 8 = 19y - 152 \equiv 19y - 22(26)$

donc $g^{-1}(y) = 19y - 22$

Partie B

1) $E \hookrightarrow 4$ et $J \hookrightarrow 9 = x$
 $N \hookrightarrow 13 = y$
d'où $\begin{cases} 4a + b \equiv 4(26) \\ 9a + b \equiv 13(26) \end{cases}$

Comme E est chiffrée en E $g(4) \equiv 4(26)$
Comme J est chiffrée en N $g(9) \equiv 13(26)$

2) $\begin{cases} L_1: 4a + b \equiv 4(26) \\ L_2: 9a + b \equiv 13(26) \end{cases}$

donc en faisant $L_2 - L_1$ on a :
 $9a + b - 4a - b \equiv 13 - 4(26)$
d'où $5a \equiv 9(26)$

On $5 \times 21 = 105 = 26 \times 4 + 1$ donc $5 \times 21 \equiv 1(26)$

donc $21 \times 5a \equiv 21 \times 9(26)$ d'où $a \equiv 21 \times 9 \equiv 189 \equiv 7(26)$ car $189 = 7 \times 26 + 7$

b) $b \equiv 4 - 4a \equiv 4 - 4 \times 7 \equiv -24 \equiv 2(26)$

d'où $g(x) = 7x + 2$ car $b \equiv 2(26)$ et $a \equiv 7(26)$ et a et b doivent être des entiers entre 0 et 25 donc $a = 7$ et $b = 2$

c) si $7x \equiv z(26)$ alors $15 \times 7x \equiv 15z(26)$

On $15 \times 7 = 105 = 4 \times 26 + 1$ donc $15 \times 7x \equiv x(26)$

d'où $x \equiv 15z(26)$

Réciproquement : si $x \equiv 15z(26)$ alors $7x \equiv 7 \times 15z(26)$

On $7 \times 15 = 105 = 4 \times 26 + 1$ donc $7 \times 15z \equiv z(26)$

d'où $7x \equiv z(26)$

Ainsi $7x \equiv z(26) \Leftrightarrow x \equiv 15z(26)$

d) prenons $z = y - 2$ alors $7x \equiv y - 2(26) \Leftrightarrow x \equiv 15(y - 2)(26)$

c'est à dire $7x + 2 \equiv y(26) \Leftrightarrow x \equiv 15y - 30(26)$

d'où $g^{-1}(y) = 15y + 22$ car $-30 \equiv 22(26)$

e) $F \rightarrow 5 \rightarrow g^{-1}(5) = 15 \times 5 + 22 = 97 \rightarrow 97 \equiv 19(26) \rightarrow T$

$M \rightarrow 12 \rightarrow g^{-1}(12) = 15 \times 12 + 22 = 202 \rightarrow 202 \equiv 20(26) \rightarrow U$

$E \rightarrow 4 \rightarrow g^{-1}(4) = 15 \times 4 + 22 = 82 \rightarrow 82 \equiv 4(26) \rightarrow E$

$Y \rightarrow 24 \rightarrow g^{-1}(24) = 15 \times 24 + 22 = 382 \rightarrow 382 \equiv 18(26) \rightarrow S$

$S \rightarrow 18 \rightarrow g^{-1}(18) = 15 \times 18 + 22 = 292 \rightarrow 292 \equiv 6(26) \rightarrow G$

$E \rightarrow 4 \rightarrow g^{-1}(4) = 15 \times 4 + 22 = 82 \rightarrow 82 \equiv 4(26) \rightarrow E$

$P \rightarrow 15 \rightarrow g^{-1}(15) = 15 \times 15 + 22 = 247 \rightarrow 247 \equiv 13(26) \rightarrow N$

$G \rightarrow 6 \rightarrow g^{-1}(6) = 15 \times 6 + 22 = 112 \rightarrow 112 \equiv 8(26) \rightarrow I$

$C \rightarrow 2 \rightarrow g^{-1}(2) = 15 \times 2 + 22 = 52 \rightarrow 52 \equiv 0(26) \rightarrow A$

$B \rightarrow 1 \rightarrow g^{-1}(1) = 15 \times 1 + 22 = 37 \rightarrow 37 \equiv 11(26) \rightarrow L$

Le message décodé est "TU ES GÉNIAL"