

ema 5. Criptografie

15. Un mesaj în clar în limba engleză este criptat cu un sistem de cifrare pe blocuri de un caracter, folosind un alfabet de 26 caractere (A-Z).
Interceptați mesajul

ΔT\X\A\X\A\JOGXN\X\X\A\ΔKPKXE\X\A\K

Descifrați mesajul știind că E, T sunt respectiv criptate în K, Δ.
Determinați apoi funcția de criptare și criptați mesajul

X\IONΔERFUL

E, T sunt criptate în K, Δ

$$\begin{cases} \alpha K + \beta = E \\ \alpha \Delta + \beta = T \end{cases} \Rightarrow \begin{cases} \alpha \cdot 10 + \beta = 4 \\ \alpha \cdot 3 + \beta = 13 \end{cases} \Rightarrow \begin{matrix} -7\alpha = 15 \\ \alpha = -15 \end{matrix}$$

$$\begin{matrix} \alpha \cdot 10 + \beta = 4 & / \cdot 13 \\ \alpha \cdot 3 + \beta = 13 & / \cdot 4 \end{matrix} \Rightarrow \begin{matrix} 130\alpha + 13\beta = 52 \\ 12\alpha + 4\beta = 52 \end{matrix} \Rightarrow 118\alpha + 9\beta = 0$$

$$\Rightarrow 7\alpha = 11 \Rightarrow \alpha = 7^{-1} \pmod{26} \Rightarrow \alpha = (7^{-1})^{11} \pmod{26} = 11^{11} \pmod{26}$$

$$1 = (7, 26) \Rightarrow 1 = u \cdot 7 + v \cdot 26$$

$$26 = 7 \cdot 3 + 5$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5) =$$

$$= 26 - 3 \cdot 7 - 2(7 - (26 - 7 \cdot 3)) = 26 - 3 \cdot 7 - 2 \cdot 7 + 2 \cdot 26 - 6 \cdot 7$$

$$= 3 \cdot 26 - 11 \cdot 7$$

$$\begin{aligned} 11^{11} \pmod{26} &= 11^{10} \cdot 11 \pmod{26} = (11^2)^5 \cdot 11 \pmod{26} = 121^5 \pmod{26} \\ &= 17^5 \cdot 11 \pmod{26} = 17^4 \cdot 17 \cdot 11 \pmod{26} = (17^2)^2 \cdot 11 \cdot 17 \pmod{26} = \\ &= 289^2 \cdot 11 \cdot 17 \pmod{26} = 3^2 \cdot 11 \cdot 17 \pmod{26} = 9 \cdot 11 \cdot 17 \pmod{26} \\ &= 19 \pmod{26} = \alpha \end{aligned}$$

$$3 \cdot 19 + \beta = 13 \Rightarrow \beta = 38 \pmod{26} \Rightarrow \beta = 12 \pmod{26}$$

$$19 K + 12 = E$$

$$19 \Delta + 12 = T$$

$\Delta T W A W A S O G X M W X A \Delta K P K X E W A K$