Tema 6

Bob foloseşte sistemul El Gamal pentru a trimite un mesaj criptat lui Alice. Cheia publică a lui Alice este $(37, 2, 19)$.

Oscar interceptează mesajele cifrate $(30, 35)$ şi $(25, 30)$. Folosind algoritmul Pohlig-Hellman ajutaţi-l pe Oscar să decripteze cele două mesaje. Răspunsul vă va spune dacă aţi lucrat corect!

Soluție

$p=37$, $g=2$, cheia privată a a.î. $2^a \equiv 19 \pmod{37}$

Oscar folosește alg Pohlig-Hellman pentru a găsi pe a

$p-1 = 2^2 \cdot 3^2$

$\boxed{q=2,\ c=2}$ (cu notațiile din curs) căutăm $a \bmod 2^2$ $\quad a = a_0 + 2a_1$

$h=19$, $h^{\frac{p-1}{2}} = 19^{18} \pmod{37} = 36$.

$g^{\frac{p-1}{2}} = 2^{18} \equiv 36 \pmod{37} \Rightarrow \boxed{a_0 = 1}$

$h_1 = h \cdot g^{-a_0} = 19 \cdot 2^{-1} = 19 \cdot 19 = 28 \pmod{37}$

$h_1^{\frac{p-1}{q^2}} = 28^9 \equiv 36 \pmod{37} \Rightarrow \boxed{a_1 = 1}$

$\Rightarrow a \equiv 3 \pmod 4$

$\boxed{q=3,\ c=2}$ căutăm $a \bmod 3^2$ $\quad a = a_0 + 3a_1$

$h^{\frac{p-1}{q}} = 19^{12} \equiv 10 \pmod{37}$

$g^{\frac{p-1}{q}} = 2^{12} \equiv 26 \pmod{37}$

$26^2 \equiv 10 \pmod{37} \Rightarrow \boxed{a_0 = 2}$

$h_1 = h \cdot g^{-a_0} = 19 \cdot 2^{-2} \equiv 14 \pmod{37}$

$h_1^{\frac{p-1}{3^2}} = 14^4 \equiv 10 \pmod{37} \Rightarrow \boxed{a_1 = 2}$

$\Rightarrow a \equiv 8 \pmod 9$.

Folosim lema chineză a resturilor pentru a rezolva sistemul de congruențe $\begin{cases} a \equiv 3 \pmod 4 \\ a \equiv 8 \pmod 9 \end{cases}$ ale cărui modul $4 \cdot 9 = 36$.

$N_1 = \frac{36}{n_1} = 9 \quad 9 \cdot y_1 \equiv 1 \pmod 4 \quad \boxed{y_1 = 1}$

$N_2 = \frac{36}{n_2} = 4 \quad 4 \cdot y_2 \equiv 1 \pmod 9 \rightarrow \boxed{y_2 = 7}$

$\Rightarrow a = 3 \cdot 9 \cdot 1 + 8 \cdot 4 \cdot 7 \pmod{36} = 35$

$\Rightarrow \boxed{a = 35}$

$(v_1, c_1) = (30, 35) \qquad 30 = \Sigma^{b_1} = 30 \quad c_1 = m_1 \cdot u^{b_1}$

$(v_2, c_2) = (25, 30) \qquad x_1 = p - 1 - a = 37 - 1 - 35 = 1$

$m = v_1^{x} \cdot c_1 = 30 \cdot 35 = 14 \pmod{37}$

analog $c_2 = m_2 \cdot u^{b_2} \quad x_2 = p - 1 - a = 1 \Rightarrow m = v_2^{x} \cdot c_2 = 25 \cdot 30 \pmod{37}$

$= 10.$

$14 \rightarrow O$

$10 \rightarrow K$

OK