Tema 8

(13) $p = 65537$, $g = 5$; mesaj: $(29095, 23856)$

(p, g, y_a) ← ~~mod~~. cheia publică

$a = 13908$

- blocuri de 3 caractere

$w = 29095^{-13908} \mod 65537 - 1 = 13908 \mod (65537) =$

$= 29095^{-13908} \pmod{2^{16}+1} = (5 \cdot 11 \cdot 23^2)^{-13908} \mod (2^{16}+1)$

$\Rightarrow 5 \cdot 5^{-1} - 131074 \equiv 1 \pmod{65537} \Rightarrow$

$\Rightarrow 5^{-1} \equiv 26215 \mod 2^{16}+1$

$11 \cdot 11^{-1} - 65537 \equiv 1 \mod (65537) \Rightarrow$

$\Rightarrow 11^{-1} \equiv 5958 \pmod{2^{16}+1}$

$\Rightarrow w \equiv (26215 \cdot 5958 \cdot 33326)^{13908} \mod (2^{16}+1)$

$\equiv 8947^{13908} \equiv 31543 \pmod{2^{16}+1}$

$\Rightarrow m \equiv 23856 \cdot 31543 \equiv 6229 \mod (2^{16}+1)$

$6229_{26} \cdot 30^2 + 27 \cdot 30 + 19 \Rightarrow$

$\Rightarrow$ mesajul este G!I.