TEMA 8

25. Alice primește mesajul (30,7), obținut cu ajutorul unui criptosistem El Gamal. Descriptați mesajul, cunoscând cheia publică lui Alice ($p=43, g=3$).

$u=30, v=7$

$m = v \cdot w \bmod p$

$w = u^{-a} \bmod p$

$0 < a < 42$

Alegem $a=1 \Rightarrow w = u^{-1} \bmod p = 30^{-1} \bmod 43 = 33$

$m = 7 \cdot 33 \bmod 43 = 231 \bmod 43 = 16$