Tema L 8

3. Fie (53, 2, 30) cheia publică a lui Alice într-un criptosistem El Gamal. Bob utilizează această cheie ca să genereze mesajul criptat (24, 37). Determinați mesajul în clar corespunzător

A	B
(53, 2, 30) = (p, g, d)	$u = 24 = g^k \pmod p$ $V = 37 = m \cdot g^d \pmod p$ $\Rightarrow m = 37 \cdot 2^{-30} \pmod{53}$ $2^{-1} \pmod{53} = 27$ $27 \cdot 2^{30} = 45$ $45 \cdot 37 = 22 \pmod{53}$

$m = 22$