Criptografie-Tema8

guzurazvan

May 2024

24. 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.

$(p, g, \alpha) = (53, 2, 30)$.

(u,v) = (24, 37)

$u = 24 = g^k(modp)$

$24 = 2^k(mod53)$

$2^6(mod53) = 64(mod53) = 11(mod53)$

$2^{12}(mod53) = 11 \cdot 11(mod53) = 121(mod53) = 15(mod53)$

$2^{14}(mod53) = 15 \cdot 2^2(mod53) = 60(mod53) = 7(mod53)$

$2^{17}(mod53) = 7 \cdot 2^3(mod53) = 3(mod53)$

$2^{20}(mod53) = 3 \cdot 2^3(mod53) = 24(mod53)$

$\Rightarrow 24 = 2^{20}(mod53) \Rightarrow k = 20$

$v = m \cdot \alpha^k(modp) \Leftrightarrow 37 = m \cdot 30^{20}(mod53)$

$\Rightarrow m = 37 \cdot 30^{-20}(mod53) = 37 \cdot (30^{-1})^{30}(mod53)$

$(53, 30) = 1 \Rightarrow \exists 30^{-1}(mod53)$

$53 = 1 \cdot 30 + 23$
$30 = 1 \cdot 23 + 7$
$23 = 3 \cdot 7 + 2$
$7 = 3 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

$x_{53} = (1, 0)$
$x_{30} = (0, 1)$
$x_{23} = x_{53} - 1 \cdot x_{30} = (1, 0) - (0, 1) = (1, -1)$
$x_7 = x_{30} - x_{23} = (0, 1) - (1, -1) = (-1, 2)$
$x_2 = x_{23} - 3 \cdot x_7 = (1, -1) - 3 \cdot (-1, 2) = (1, -1) - (-3, 6) = (4, -7)$
$x_1 = x_7 - 3 \cdot x_2 = (-1, 2) - 3 \cdot (4, -7) = (-1, 2) - (12, -21) = (-13, 23).$
$1 = 53 \cdot (-13) + 30 \cdot 23 \Rightarrow 30^{-1}(mod 53) = 23(mod 53)$

$\Rightarrow m = 37 \cdot 23^{30}(mod 53) = 37 \cdot 529^{15}(mod 53) = 37 \cdot (-1)^{15}(mod 53)$
$= -37(mod 53) = 16(mod 53)$
$m = 16.$