Criptografie-Tema8

guzurazvan

May 2024

24. Percy și Charlie comunică folosind criptosistemul RSA. Percy are cheia publică: n = 187 și e =107.
a) Aflați cheia privată a lui Percy.
b) Charlie îi transmite lui Percy mesajul

$$ABACFPFP$$

Știind că lungimea blocurilor mesajelor în clar este 1 și a mesajelor criptate este 2, decriptați textul.

a) $K_{e_p} = (187, 107)$
$F(1) = (1 + \left[\sqrt{(}187)\right])^2 - 187 = 196 - 187 = 9 = 3^2$
$n = 14^2 - 3^2 = 11 \cdot 17$
$\phi(n) = 10 \cdot 16 = 160$
$d \cdot e = 1(mod\phi(n)) \Rightarrow d = 107^{-1}(mod160)$.

$160 = 1 \cdot 107 + 53$
$107 = 2 \cdot 53 + 1$
$53 = 1 \cdot 53 + 0$

$x_{160} = (1, 0)$
$x_{107} = (0, 1)$
$x_{53} = x_{160} - x107 = (1, 0) - (0, 1) = (1, -1)$
$x_1 = x_{107} - 2 \cdot x_{53} = (0, 1) - 2 \cdot (1, -1) = (0, 1) - (2, -2) = (-2, 3)$.

$\Rightarrow 1 = 160 \cdot (-2) + 107 \cdot 3 \Rightarrow 107^{-1}(mod160) = 3(mod160)$.
$\Rightarrow d = 3(mod160)$

b)
$AB = 0 \cdot 30 + 1 = 1 \Rightarrow m = 1^3(mod187) = 1 = B$.
$AC = 0 \cdot 30 + 2 = 2m = 2^3 = 8(mod187) = I$
$FP = 5 \cdot 30 + 15 = 165 \Rightarrow m = 165^3(mod187) = 11 = L$

$\Rightarrow$ R: BILL