Tema 7 - Cripto

Percy și Charlie comunică folosind criptosistemul RSA. Percy are cheia publică: $n=187$ și $e=107$

a) Află cheia privată lui Percy

$K_p=(187,107)$

$\sqrt{1.87}$ | 13

$2\cdot 3\times 3=69$

1

$=87$

69

$=18$

$F(1)=(1+[\sqrt{187}])^2-187=196-187=9=3^2$

$n=14^2-3^2$

$f(n)=10\cdot 16=160$

$d\cdot e\equiv 1 \pmod{f(n)} \Rightarrow d=107^{-1} \pmod{160}$

$107^{-1} \pmod{160}\equiv 3 \Rightarrow d=3$

b) Charlie îi transmite lui Percy mesajul

AB AC FP FP

$FP=5\cdot 30+15=165 \Rightarrow m=165^3 \pmod{187}=11=L$

$AC=0\cdot 30+2=2 \Rightarrow m=2^3=8 \pmod{187}=I$

$AB=0\cdot 30+1=1 \Rightarrow m=1^3=1 \pmod{187}=B$

Mesaj: BILL

Exerciții

1. Ana și Bob utilizează un criptosistem RSA, în care textele în clar sunt împărțite în blocuri de două caractere, iar textele criptate în blocuri de trei caractere. Cheia publică a Anei este $(2501, e)$, cu e minimal

a) Determinați cheia privată a Anei

b) Bob dorește să-i trimită Anei mesajul „DA"

$K_{e_A} = (2501, e)$

$F(1) = \left(1 + [\sqrt{2501}]\right)^2 - 2501 = 2601 - 2501 = 100^2 = 10$

$2501 = 51^2 - 10^2 = 41 \cdot 61$

$\sqrt{25.01}$ | 50 (25, =01, 00, 1) | $100 \cdot 0 = 0$

$f(n) = 40 \cdot 60 = 2400$

$e_A = 7 \Rightarrow 7 \cdot d \equiv 1 \pmod{2400}$

$d \equiv 7^{-1} \pmod{2400}$

$7 \cdot b \equiv 1 \bmod 2400$ deci $7x + 2400y = (7, 2400)$

$2400 = 7 \cdot 342 + 6 \Rightarrow 6 = 2400 - 7 \cdot 342$

$7 = 6 \cdot 1 + 1 \Rightarrow 1 = 7 - 6 \cdot 1 \Rightarrow 1 = 7 - 2400 \cdot 7 \cdot 342 \Rightarrow$

$6 = 1 \cdot 6 + 0$ $\Rightarrow 1 = 7 \cdot 343 - 2400$

$\Rightarrow$ Inversul lui 7 este $\underline{343} = d_A$

b) „DA" $= 3 \cdot 30 + 0 = 90$

$c \equiv m^e \pmod{f(n)} = 90^7 \pmod{2501} = 9^7 \cdot 10^7 \pmod{2501}$

$= 1191$

$1191 = 1 \cdot 30^2 + 9 \cdot 30^1 + 21 = BJV$

2. Ana și Bob comunică folosind criptosistemul RSA. Bob are cheia publică $K_e = (n = 5893, e = 3827)$

a) Aflați cheia privată a lui Bob

$F(1) = \left(1 + [\sqrt{5893}]\right)^2 = 5893 = 5929 - 5893$

$= 36 = 6^2$

$\sqrt{58.93}$ | 76 (49, =993) | $146 \cdot 6$

$n = 77^2 \cdot 6^2$

$f(n) = 70 \cdot 82 = 5740$

$(3827, 5740)$