Tema L7

3. 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

AB AC 7P 7P

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

b) $K_{e_p} = (187, 107)$

$187 \mid 13$
$1 \quad 23\ 3 =$
$= 87$

$f(1) = (14 + \lceil \sqrt{187} \rceil)^2 - 187 = 1096 - 187 = 09 = 3^2$

$n = 14^2 - 3^2 = 11 \cdot 17$

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

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

$d = 3$

(b) $7P = 5 \cdot 30 + 15 = 165 \Rightarrow m = 165^3 \pmod{187} = 11 = L$

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

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

Mesaj: BILL

Exercitii Laborator 7

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 3 caractere. Cheia publică a Anei este $(2501, e)$, cu e minimal.

(a) Determinați cheia privată a Anei

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

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

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

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

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

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

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

$2401 : 7 = 343 \Rightarrow d_A = 343$

(b) (B) → (A) "ΔA"

$\Delta A = 3 \cdot 30 + 0 = 90$

$c \equiv m^{e_A} \pmod{\varphi(n)} = 90^7 \pmod{2401} = 9^7 \cdot 10^7 \pmod{2401} = 1191$

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

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.

$\sqrt{5893}\ |\ 76$
$49\ \ |\ 146 \cdot 6 = \ldots$
$= 993$

$f(1) = (1 + [\sqrt{5893}])^2 - 5893 = 5929 - 5893 = 36 = 6^2$

$n = 77^2 - 6^2 = 71 \cdot 83$

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

$(3827, 5740) = 1$
$\exists (e, \varphi(n))$

$e \cdot d = 1 \pmod{\varphi(n)}$

$d = 3827^{-1} \pmod{5740} = 1403$

(a) (A) → (B)

"BM" / $\Delta\Delta O$"

$\Delta\Delta O = 3 \cdot 30^2 + 3 \cdot 30 = 2790 \rightsquigarrow m = 2790^{1403} \pmod{5740} = 960 = 32 \cdot 30 + 0 = CA$

$BM = 1 \cdot 30^2 + 12 \cdot 30 + 23 = 1283 \rightsquigarrow m = 1283^{1403} \pmod{5740} = 2112 = 70 \cdot 30 + 12 = KM$