Nichita Bogdan Valentin

M531

TEMA 7

1. Ana și Bob folosesc RSA. Ana are cheia secretă (n = 12827, d = 2291). Determinați cheia sa publică și criptați textul IERI dacă lungimea blocurilor în clar este 2 și lungimea blocurilor criptate este 3.

$d \cdot e \equiv 1 \bmod \varphi(n)$

$n = 12827 = 101 \cdot 127 = p \cdot q \Rightarrow p = 101, q = 127$

$\varphi(n) = (p - 1)(q - 1) = 100 \cdot 126 = 12600$

$d \cdot e \equiv 1 \bmod \varphi(n) \Rightarrow 2291 \cdot e \equiv 1 \bmod 12600 \Rightarrow \cdot e \equiv 2291^{-1} \bmod 12600 \Rightarrow e = 11$

cheia publica (n = 12827, e = 11).

I=8

E=4

R=17

I=8

$IE = 8 \cdot 30 + 4 = 244$

$244^{11} \bmod 12827 \equiv 4851 \bmod 12827$

$4851 = 5 \cdot 30^2 + 11 \cdot 30 + 21$

IE → FLV

$RI = 17 \cdot 30 + 8 = 518$

$518^{11} \bmod 12827 \equiv 7595 \bmod 12827$

$7595 = 8 \cdot 30^2 + 13 \cdot 30 + 5$

RI → INF

IERI → FLVINF

2. Ana și Bob folosesc RSA. Ana are modulul n = 2733. Știind că exponentul de criptare este minim posibil și că lungimea blocurilor în clar este 2 și lungimea blocurilor criptate este 3, criptați textul OK.

$n = 3 \cdot 911$

$\varphi(n) = 2 \cdot 910 = 1820$

$(\varphi(n), e) = 1 \Rightarrow e = 3$ (cel mai mic numar coprim cu 1820)

$OK = 14 \cdot 30 + 10 = 430$

$430^3 \bmod 2733 \equiv 1297 \bmod 2733$

$1297 = 1 \cdot 30^2 + 13 \cdot 30 + 7$

OK → BNH

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

a. Aflați cheia privată a lui Percy.

$n = 187 = 11 \cdot 17$

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

$d \cdot e \equiv 1 \bmod \varphi(n) \Rightarrow d \cdot 107 \equiv 1 \bmod 160 \Rightarrow d \equiv 3 \bmod 160$

cheia privată a lui Percy (n = 187 , d = 3)

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.

$AB = 0 \cdot 30 + 1 = 1$

$1^3 \bmod 187 \equiv 1 = B$

$AC = 0 \cdot 30 + 2 = 2$

$2^3 \mod 187 \equiv 8 = I$

$FP = 5 \cdot 30 + 15 = 165$

$165^3 \mod 187 \equiv 11 = L$

ABACFPFP → BILL

4. Alice și Bob doresc să comunice folosind criptosistemul RSA. Alice alege numerele prime p = 7, q = 11 pentru a-și determina cheile de criptare/decriptare și alege exponentul de decriptare d > 1 minimul posibil.

a. Aflați cheia de criptare (n, e) a lui Alice.

$\varphi(n) = 6 \cdot 10 = 60$

$(\varphi(n), d) = 1$, d > 1 minimul posibil => d = 7

$d \cdot e \equiv 1 \mod \varphi(n) \Rightarrow 7 \cdot e \equiv 1 \mod 60 \Rightarrow e \equiv 43 \mod 60$

cheia de criptare a lui Alice (n = 77 , e = 43)

b. Bob îi transmite lui Alice mesajul B!BTBL Știind că lungimea blocurilor la citire este 1 și la scriere este 2, decriptați textul.

$B! = 1 \cdot 30 + 28 = 58$

$BT = 1 \cdot 30 + 19 = 49$

$BL = 1 \cdot 30 + 11 = 41$

$58^3 \mod 187 \equiv 9 = J$

$49^7 \mod 77 \equiv 14 = O$

$41^3 \mod 187 \equiv 13 = N$

B!BTBL → JON

5. Șeful vostru de grupă a decis să comunice cu voi folosind criptosistemul RSA. Ați ales cheia publică Ke = (n = 1189, e = 747).

a. Determinați-vă cheia privată.

n = 1189 = 29 · 41

$\varphi(n) = 28 \cdot 40 = 1120$

$d \cdot e \equiv 1 \bmod \varphi(n) \Rightarrow d \cdot 747 \equiv 1 \bmod 1120 \Rightarrow e \equiv 3 \bmod 1120$

cheia private (n = 1189 , d = 3)

b. Știind că lungimea j a blocurilor în clar verifică $N^j \leq n \leq N^{j+1}$ și lungimea blocurilor criptate este dată de l = j + 1, decriptați textul BFCAFNBIW, unde N este lungimea alfabetului.

$30^j \leq 1189 \leq 30^{j+1} \Rightarrow j = 2$

l = j +1 =3

$BFC = 1 \cdot 30^2 + 5 \cdot 30 + 2 = 1052$

$1052^3 \bmod 1189 \equiv 454$

454 = 15 · 30 +4

BFC → PE

$AFN = 0 \cdot 30^2 + 5 \cdot 30 + 13 = 163$

$163^3 \bmod 1189 \equiv 409$

409 = 13 · 30 +19

AFN → NT

$BIW = 1 \cdot 30^2 + 8 \cdot 30 + 22 = 1162$

$1162^3 \bmod 1189 \equiv 530$

$530 = 17 \cdot 30 + 20$

BIW → RU

BFCAFNBIW → PENTRU

6. Alice foloseste RSA. Blocurile mesajelor in clar au 1 caracter iar blocurile mesajelor criptate au 2 caractere. Pentru a determina cheile de criptare/decriptare, ea alege numerele prime p = 23, q = 17 si face publica cheia de criptare (n, e = 3).

a. Bob doreste sa-i trimita lui Alice mesajul HELP_ME! Criptati acest mesaj.

$n = 23 \cdot 17 = 391$

H = 7

$7^3 \bmod 391 \equiv 343$

$343 = 11 \cdot 30 + 13$

E = 4

$4^3 \bmod 391 \equiv 64$

$64 = 2 \cdot 30 + 4$

L = 11

$11^3 \bmod 391 \equiv 158$

$158 = 5 \cdot 30 + 8$

P = 15

$15^3 \bmod 391 \equiv 247$

$247 = 8 \cdot 30 + 7$

_ = 26

$26^3 \mod 391 \equiv 372$

$372 = 12 \cdot 30 + 12$

M = 12

$12^3 \mod 391 \equiv 164$

$164 = 5 \cdot 30 + 14$

! = 28

$28^3 \mod 391 \equiv 56$

$56 = 1 \cdot 30 + 26$

HELP_ME! → LNCEFIIHMMFOCEB_

b. Determinati cheia de decriptare a lui Alice si decriptati mesajul primit de aceasta EBMMAAFOMML!EBAIHI

$\varphi(n) = 22 \cdot 16 = 352$

$d \cdot e \equiv 1 \mod \varphi(n) \Rightarrow d \cdot 3 \equiv 1 \mod 352 \Rightarrow e \equiv 235 \mod 352$

cheia de decriptare (n = 391, d = 235)

$EB = 4 \cdot 30 + 1 = 121$

$121^{235} \mod 391 \equiv 8 = I$

EB → H

$MM = 12 \cdot 30 + 12 = 372$

$372^{235} \mod 391 \equiv 26 = \_$

MM → _

AA = 0 · 30 + 0 = 372

$0^{235} \bmod 391 \equiv 0 = A$

AA → A

FO = 5 · 30 + 14 = 164

$164^{235} \bmod 391 \equiv 12 = M$

FO → M

L! = 11 · 30 + 28 = 164

$164^{235} \bmod 391 \equiv 18 = S$

L! → M

EB = 4 · 30 + 1 = 121

$121^{235} \bmod 391 \equiv 8 = I$

EB → I

AI = 0 · 30 + 8 = 121

$8^{235} \bmod 391 \equiv 2 = C$

AI → C

HI = 7 · 30 + 8 = 218

$218^{235} \bmod 391 \equiv 10 = K$

HI → K

EBMMAAFOMML!EBAIHI → I_AM_SICK