Cătălin Răpeanu

Exerciții

Seminar 1

6) $(67891, 98713) = ?$

$98713 = 1 \cdot 67891 + 30822$

$67891 = 2 \cdot 30822 + 6247$

$30822 = 4 \cdot 6247 + 5834$

$6247 = 1 \cdot 5834 + 413$

$5834 = 14 \cdot 413 + 52$

$413 = 7 \cdot 52 + 49$

~~$413 = 8 \cdot 49 + 21$~~ $52 = 1 \cdot 49 + 3$

~~$49 = 2 \cdot 21 + 7$~~ $49 = 3 \cdot 16 + 1$

~~$21 = 3 \cdot 7 + 0$~~

$(67891, 98713) = 1$

$x_{67891} = (0, 1)$ $x_{98713} = (1, 0)$

$X_{30822} = (1, 0) - (0, 1) = (1, -1)$

$x_{6247} = (0, 1) - 2 \cdot (1, -1) = (-2, 3)$

$x_{5834} = (1, -1) - 4 \cdot (-2, 3) = (1, -1) - (-8, 12) = (9, -13)$

$x_{413} = (-2, 3) - (9, -13) = (-11, 16)$

$x_{52} = (9, -13) - 14 \cdot (-11, 16) = (163, -237)$

$x_{49} = (-11, 16) - 7 \cdot (163, -237) = (-1152, 1675)$

$x_{3} = (163, -237) - (-1152, 1675) = (1315, -1912)$

$x_{1} = (-1152, 1675) - 16 \cdot (1315, -1912) = (-22192, 32267$

10) $(33223, 11227) = ?$

$33223 = 11227 \cdot 2 + 10769$

$11227 = 10769 \cdot 1 + 458$

$10769 = 458 \cdot 23 + 235$

$458 = 235 \cdot 1 + 223$

$235 = 223 \cdot 1 + 12$

$223 = 12 \cdot 18 + 7$

$12 = 7 \cdot 1 + 5$

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + 1$

$(33223, 11227) = 1$

$x_{33223} = (1, 0)$ $\quad x_{11227} = (0, 1)$

$x_{10769} = (1, -2)$

$x_{458} = (0, 1) - (1, -2) = (-1, 3)$

$x_{235} = (1, -2) - 23(-1, 3) = (24, -51)$

$x_{223} = (-1, 3) - (24, -51) = (-25, 54)$

$x_{12} = (24, -51) - (-25, 54) = (49, -105)$

$x_7 = (-25, 54) - 18(49, -105) = (-907, 1944)$

$x_5 = (49, -105) - (-907, 1944) = (956, -2049)$

$x_2 = (-907, 1944) - (956, -2049) = (-1861, 3993$

$x_1 = (956, -2049) - 2 \cdot (-1861, 3993) = (4676, -1003$

12) $13^{-1} \bmod 47 = ?$

$$47 = 13 \cdot 3 + 8$$
$$13 = 8 \cdot 1 + 5$$
$$8 = 5 \cdot 1 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$

$$(47, 13) = 1 \Rightarrow \exists\, 13^{-1} \bmod 47$$

$$X_{47} = (1, 0), \quad X_{13} = (0, 1)$$
$$X_8 = (1, 0) - 3 \cdot (0, 1) = (1, -3)$$
$$X_5 = (0, 1) - (1, -3) = (-1, 4)$$
$$X_3 = (1, -3) - (-1, 4) = (2, -7)$$
$$X_2 = (-1, 4) - (2, -7) = (-3, 11)$$
$$X_1 = (2, -7) - (-3, 11) = (5, -18)$$

$$1 = 47 \cdot 5 - 18 \cdot 13$$

$$\Rightarrow 13^{-1} \equiv -18 \pmod{47}$$
$$13^{-1} \equiv 29 \pmod{47}$$

Seminar 2

10) a) $11000_{(2)} = ?_{(10)}$

$11000_{(2)} = 0 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 = 8 + 16 = 24_{(10)}$

(b) $2D_{(16)} = ?_{(10)}$

$2D_{(16)} = 16^0 \cdot 15 + 16^1 \cdot 2 = 15 + 32 = 47_{(10)}$

(c) $543_{(5)} = ?_{(4)}$

$\searrow ?$

(d) $2F_{(16)} = 16^0 \cdot 15 + 16^1 \cdot 2 = 47$

$47 = 8 \cdot 5 + 7$

$5 = 8 \cdot 0 + 5$ $\uparrow$ $= 57_{(8)}$

$13_{(10)} = 8 \cdot 1 + 5$

$5 = 8 \cdot 0 + 5$ $\uparrow$ $= 55_{(8)}$

$$\begin{array}{r} 57 - \\ 55 \\ \hline = 2 \end{array} \quad = 2_{(8)}$$

12) $41^{103} (\text{mod } 107) \equiv 41 \cdot (41^2)^{51} \equiv 41 \cdot 1681 \cdot 1681^{50} \equiv$

$\equiv 41 \cdot 76 \cdot 76^{50} \equiv 13 \cdot 76^{50} \equiv 13 \cdot (76^2)^{25} \equiv 13 \cdot 5776 \cdot 5776^2$

$\equiv 13 \cdot 105 \cdot (105^2)^{12} \equiv 1365 \cdot (11025)^{12} \equiv 81 \cdot 4^{12} \equiv$

$\equiv 81 \cdot (4^3)^4 \equiv 81 \cdot 64^4 \equiv 81 \cdot 4096^2 \equiv 81 \cdot 30^2 \equiv$

$\equiv 81 \cdot 900 \equiv 81 \cdot 44 \equiv 3564 \equiv 33 (\text{mod } 2021$

Seminar 3

121) $n = 40289 \Rightarrow n-1 = 40288 = 2^5 \cdot 1259$

$$\begin{array}{r|l} 40288 & 2 \\ 20144 & 2 \\ 10072 & 2 \\ 5036 & 2 \\ 2518 & 2 \\ 1259 & 1259 \\ 1 & \end{array}$$

$2^{1259} (\bmod 40289) \equiv$

$\equiv 2 \cdot 2^{1258} (\bmod 40289) \equiv$

$\equiv 2 \cdot 4 \cdot 4^{628} \equiv 8 \cdot 16^{314} \equiv$

$\equiv 8 \cdot (16^2)^{157} \equiv 8 \cdot 256 \cdot (256^2)^{78} \equiv$

$\equiv 2048 \cdot (65536)^{78} \equiv 2048 \cdot (25247)^{78} \equiv$

$\equiv 2048 \cdot (25247^2)^{36} \equiv 2048 \cdot 39029^{36} \equiv$

$\equiv 2048 \cdot (-1260)^{36} \equiv 2048 \cdot (1260^2)^{18} \equiv$

$\equiv 2048 \cdot 16329^{18} \equiv 2048 \cdot (16329^2)^{9} \equiv$

$\equiv 2048 \cdot 3639^{9} \equiv 2048 \cdot 3639 \cdot (3639^2)^{4} \equiv$

$\equiv 39496 \cdot 27529^{4} (\bmod 40289) \equiv$

$\equiv -793 \cdot (-12760^2)^2 \equiv -793 \cdot 9751^2 \equiv$

$\equiv -793 \cdot 40250 \equiv (-793) \cdot (-39) \equiv$

$\equiv 30927$

$\equiv -9362$

$2^{2\cdot 1259} \equiv (-9362)^2 \equiv 18469$

$2^{4\cdot 1259} \equiv 18469^2 \equiv 17287$

~~$2^{8\cdot 1259} \equiv 17287^2 \equiv 16856$~~ $2^{2^3\cdot 1259} \equiv 17287^2 \equiv 16856$

~~$2^{16\cdot 1259} \equiv 16856^2 \equiv$~~ $2^{2^4\cdot 1259} \equiv$

Seminar 4

12) Descompuneți numărul 14107 în factorii săi primi.

```
√1.41.07 | 118
 1       |----------------
 =41     | 21·1 = 21
  21     |----------------
  2007   | 228·8 = 1824
  1824   |----------------
  =183
```

$[\sqrt{14107}] = 118$

$t = 119$

$t^2 - n = 119^2 - 14107 = 14161 - 14107 = 54 = 6\cdot 9$
$= 6\cdot 3^2$

$t = 120$

$t^2 - n = 120^2 - 14107 = 14400 - 14107 = 293$

$t = 121$

$t^2 - n = 14641 - 14107 = 534$

```
   119·
   119
  ------
  1071
  119
 119
 -------
 14161
```

```
534 | 2
267 | 3
 89 |
```

$x = 122$

$x^2 - n = 14884 - 14107 = 777$

$$\begin{array}{r|l} 777 & 7 \\ 111 & 3 \\ 37 & \end{array}$$

14107 e prim

14) 14551

$$\begin{array}{l|l} \sqrt{1.45.51} & 120 \\ 1 & 22\cdot 2 = 44 \\ =45 & 240\cdot 0 = 0 \\ 44 & \\ =151 & \end{array}$$

$$\begin{array}{r|l} 578 & 2 \\ 289 & 17 \\ 17 & 17 \\ 1 & \end{array} \qquad \begin{array}{r|l} 333 & 3 \\ 111 & 3 \\ 37 & \end{array} \qquad \begin{array}{r|l} 90 & 2 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

$$\begin{array}{r|l} 825 & 5 \\ 185 & 5 \\ 37 & 37 \\ 1 & \end{array}$$

$[\sqrt{14551}] = 120$

$x = 121$

$x^2 - n = 121^2 - 14551 = 14641 - 14551 =$
$= 90 = 2\cdot 3^2\cdot 5$

$x = 122$

$x^2 - n = 14884 - 14551 = 333 = 3^2\cdot 37$

$x = 123$

$x^2 - n = 15129 - 14551 = 578 = 2\cdot 17^2$

$x = 124$

$x^2 - n = 15376 - 14551 = 825 = 5^2\cdot 37$

$(122^2 - 14551)(124^2 - 14551) =$

$= 3^2 \cdot 37 \cdot 5^2 \cdot 37 = 3^2 \cdot 5^2 \cdot 37^2 = (3 \cdot 5 \cdot 37)^2 \; / \bmod 1455$

$122^2 \cdot 124^2 \equiv (37 \cdot 15)^2 \; (\bmod 14551)$

$(122 \cdot 124)^2 \equiv (37 \cdot 15)^2 \; (\bmod 14551)$

$(123^2 - 1)^2 \equiv 555^2 \; (\bmod 14551)$

$577^2 \equiv 555^2 \; (\bmod 14551)$

$577^2 - 555^2 \; \vdots \; 14551$

$(577 - 555)(577 + 555) \; \vdots \; 14551$

$22 \cdot 1132 \; \vdots \; 14551$

$(22, 14551)(1132, 14551) = 14551$

$(11, 14551)(566, 14551) = 14551$

Seminar 5

3)

c	H	W	D	U	Y	T	L	W	F	U	M	D
C	7	22	3	20	24	19	11	22	5	20	12	3
K	5	5	5	5	5	5	5	5	5	5	5	5
m (mod 26)	2	17	$-2 = 24$	15	19	14	6	17	0	15	7	24
M	C	R	Y	P	T	O	G	R	A	P	H	Y

7) $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}_{26})$

F W M D I Q

$A^t = \begin{pmatrix} 2 & 7 \\ 3 & 8 \end{pmatrix} \Rightarrow A^* = \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix}$

$\Rightarrow A^{-1} = \frac{1}{\det A} \cdot A^* = (16 - 21)^{-1} \cdot A^* = (-5)^{-1} (\mathrm{mod}\ 26) \cdot A^*$

$= 5 (\mathrm{mod}\ 26)$

$-5^{-1} (\mathrm{mod}\ 26) \equiv 21^{-1} (\mathrm{mod}\ 26) \equiv 5 (\mathrm{mod}\ 26)$

$26 = 21 \cdot 1 + 5$

$21 = 5 \cdot 4 + 1$

$x_5 = (1,0) - (0,1) = (1,-1)$

$x_1 = (0,1) - (4,-4) = (-4,5)$

$\Rightarrow A^{-1} = 5 \cdot \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} (\mathrm{mod}\ 26) =$

$$= \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \cdot \begin{pmatrix} F & M & i \\ W & D & Q \end{pmatrix} =$$

$$= \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 5 & 12 & 8 \\ 22 & 3 & 16 \end{pmatrix} (\text{mod } 26) =$$

$$= \begin{pmatrix} 70 + 242 & 168 + 33 & 112 + 176 \\ 85 + 220 & 204 + 30 & 136 + 160 \end{pmatrix} =$$

$$= \begin{pmatrix} 18 + 8 & 12 + 7 & 8 + 20 \\ 7 + 12 & 22 + 4 & 6 + 4 \end{pmatrix} =$$

$$= \begin{pmatrix} 26 & 19 & 28 \\ 19 & 26 & 10 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 19 & 2 \\ 19 & 0 & 10 \end{pmatrix} = \text{ATTACK}$$

10/ cheia ACUM

P R E F E R _ C R I P T O S I S T E M U L _ V I G E N E R E

5 17 4 5 4 17 26 2 17 8 15 19 14 18 8 18 19 4 12 20 11 26 21 8 6 4 13 4 17 4

A C U M A C U M A C U M A C U M A C U M A C U M A C U M A C

0 2 20 12 0 2 20 12 0 2 20 12 0 2 20 12 0 2 20 12 0 2 20 12 0 2 20 12 0 2

5 15 -16 -7 4 15 6 -10 17 6 -5 -7 14 16 -12 6 19 2 -8 8 11 24 1 6 6 2 -7 -8 17 2

P P L U E P G R R G W V Q Q P G T G T I L Y A G G C U T R C

Seminar 7

7) Iulia şi Andrei fol. criptosistemul RSA. Iulia are cheia publică $K_{e_1} = (n_1 = 9991, e_1 = 3917)$

(a) det. cheia privată

$$9991 = 97 \cdot 103$$

$$\varphi(9991) = 96 \cdot 102 = 9792$$

$$(9792, 3917) = 1$$

$$d\, e \equiv 1 \pmod{9792}$$

$$d \equiv 3917^{-1} \pmod{9792}$$

$$9792 = 3917 \cdot 2 + 1958$$

$$3917 = 1958 \cdot 2 + 1$$

$$x_{1958} = (1,0) - 2(0,1) = (1,-2)$$

$$x_1 = (0,1) - 2(1,-2) = (-2,5)$$

$$\Rightarrow 3917^{-1} \equiv 5 \pmod{9792}$$

$\Rightarrow d \equiv 5 \pmod{9792}$

$(5, 9991)$

(b)

12) $K_e = (n = 1189, e = 747)$

(a)

$$\begin{array}{l|l} \sqrt{11.89} & 34 \\ \hline \ \ 9 & 64 \cdot 4 = 256 \\ \hline = 289 & \\ \ \ 256 & \end{array}$$

$[\sqrt{1189}] = 34$

$t = 35$

$t^2 - n = 35^2 - 1189 = 1225 - 1189 = 36 = 6^2 \Rightarrow s^2 = 6^2$

$\Rightarrow n = (t-s)(t+s) = (35-6)(35+6) = \underbrace{29}_{p} \cdot \underbrace{41}_{q}$

$\varphi(n) = (p-1)(q-1) = (28)(41) = 28 \cdot 41 = 1120$

$de \equiv 1 (\text{mod } \varphi(n)) \Rightarrow d \cdot 747 \equiv 1 \pmod{1120}$

$1120 = 1 \cdot 747 + 373$

$747 = 2 \cdot 373 + 1$

$x_3 z_3 = (1,-1)$

$x_1 = (0,1) - 2(1,-1) = (-2,3)$

$\Rightarrow 747^{-1} = 3$

$\Rightarrow d = 3 \pmod{1120}$

(d) $N = 30$, $n = 1189$, $\varphi(n) = 1120$, $e = 747$, $d = 3$

BF CA FN BiW

$\underbrace{BFC}, \underbrace{AFN}, \underbrace{BiW} = \underbrace{152}, \underbrace{05(13)}, \underbrace{18(22)}$

$j = 3$, $l = 4$

- $BFC = 152 = 1 \cdot 30^2 + 5 \cdot 30^1 + 2 \cdot 30^0 = 900 + 150 + 2 =$

$= 1052 = c$

$m' = c^d \pmod{n} = 1052^3 \pmod{1189} = 454$

- $AFN = 05(13) = 0 \cdot 30^2 + 5 \cdot 30^1 + 13 \cdot 30^0 = 0 + 150 + 13$

$= 163 = c$

$m' = c^d \pmod{1189} = 163^3 \pmod{1189} = 409$

• BIW $= 1\,8(22) = 1\cdot 30^2 + 8\cdot 30^1 + 22\cdot 30^0 =$

$= 900 + 240 + 22 = 1162$

$m' = 1162^3 \pmod{1189} = 530$

$454 = 0\cdot 30^2 + 15\cdot 30^1 + 4\cdot 30^0 = 0(15)4 = APE$

$409 = 0\cdot 30^2 + 13\cdot 30^1 + 19\cdot 30^0 = 0(13)(19) = ANT$

$530 = 0\cdot 30^2 + 17\cdot 30^1 + 20\cdot 30^0 = 0(17)(20) = ARU$

$\Rightarrow$ PENTRU

Seminar 8

10) Criptosistemul El Gamal

(53, 2, 30) cheie publică

(24, 37) - mesaj criptat

mesaj în clar

$p = 53, \quad g = 2, \quad \alpha = 30$

$u = 24, \quad v = 37$

$30 = 2^a \pmod{\cancel{p}\ 53}$

$2^{17} = 30 (\bmod 53) \Rightarrow a = 17$

$w = u^{p-1-a} = 24^{53-1-17} = 24^{35} (\bmod 53) =$

$\equiv 24 \cdot (24^2)^{17} \equiv 24 \cdot 46 \cdot (46^2)^8 \equiv 44 \cdot (49^2)^4 \equiv$

$\equiv 44 \cdot (16^2)^2 \equiv 44 \cdot 44^2 \equiv 44 \cdot 28 \equiv 13 (\bmod 53$

$m' = v \cdot w \ (\bmod p)$

$m' = 37 \cdot 13 \ (\bmod 53) = 4 \ (\bmod 53)$

7) El Gamal

$K_d = (p = 71, g = 33, a = 34)$

(a) cheia publică

$A = g^a (\bmod p) = 33^{34} (\bmod 71) = (33^2)^{17} (\bmod 71) \equiv$

$\equiv 1089^{17} \equiv 24^{17} \equiv 24 \cdot (24^2)^8 \equiv 24 \cdot 576^8 \equiv 24 \cdot 8^8 \equiv$

$\equiv 24 \cdot (8^2)^4 \equiv 24 \cdot (64^2)^2 \equiv 24 \cdot 4096^2 \equiv 24 \cdot 49^2 \equiv$

$\equiv 24 \cdot 2401 \equiv 24 \cdot 58 \equiv 1392 \equiv 43 (\bmod 71)$

(1) $k=3$, AZi, $A=1$, $Z=26$, $i=9$

A $\left\{\begin{array}{l} c_1 = 33^3 \pmod{71} \equiv 11 \\ c_2 = 1\cdot 43^3 \pmod{71} \equiv 58 \end{array}\right\} (11,58)$

Z $\left\{\begin{array}{l} c_1 = 33^3 \pmod{71} \equiv 11 \\ c_2 = 26\cdot 43^3 \pmod{71} \equiv 17 \end{array}\right\} (11,17)$

i $\left\{\begin{array}{l} c_1 = 11 \\ c_2 = 9\cdot 43^3 \pmod{71} = 25 \end{array}\right\} (11,25)$

Seminar 9

1 2) Alice utilizează un criptosistem Merkle-Hell pe un alfabet cu 26 de caractere (A - Z), unitățile de mesaj având un caracter. Cheia publică a lui Alice este șirul $\{8, 24, 3, 14, 57\}$ iar cheia secretă este $(b=23, m=61)$. Bob dorește să-i trimită lui Alice mesajul HELLO. Criptați mesajul

$H = 7 = 2^2+3 = 2^2+2^1+1 = 2^2+2^1+2^0 \rightarrow 00111 \Rightarrow$

$\Rightarrow 1\cdot 8 + 1\cdot 24 + 1\cdot 3 + 0\cdot 14 + 0\cdot 57 = 35$

$E = 4 = 2^2 \Rightarrow 1\cdot 3 = 3$

$L = 11 = 2^3+3 = 2^3+2^1+2^0 \rightarrow 01011$

$\Rightarrow 8 + 24 + 0 + 14 + 0 = 46$

$O = 14 = 2^3+2^2+2^1 \rightarrow 01110$

$\Rightarrow 0 + 24 + 3 + 14 + 0 = 41$

$\{35, 3, 46, 46, 41\}$

$K_e = \{8, 24, 3, 14, 57\}$

$K_d = \{k = 23, m = 61\}$