Tema 7 – Criptografie

1. $n = 12827$
$d = 2291$

cheia publică

criptare mesaj „IERI" ← lung blocuri în clar = 2
lung blocuri criptate = 3

$\sqrt{12827} = 113$

128.27	113
1	21 × 1 = 21
=28	223 × 3 = 669
21	
=727	
669	
=58	

$[\sqrt{12827}] = 113$

$\Rightarrow x = 114$

$x^2 - n = 114^2 - 12827 = (113+1)^2 - 12827 = 113^2 + 226 + 1 - 12827$

$= -58 + 227 = 169 = 13^2$

$\Rightarrow n = 114^2 - 13^2 = (114-13)(114+13) = \underbrace{101}_{p} \cdot \underbrace{127}_{q}$

$\Rightarrow \varphi(n) = 100 \cdot 126 = 12600 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7$

126	2	
63	3	$> 3^2$
21	3	
7	7	-7
1		

100	2	$> 2^2$
50	2	
25	5	$> 5^2$
5	5	
1		

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

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

$12600 = 5 \cdot 2291 + 1145 \Rightarrow 1145 = 12600 - 5 \cdot 2291$

$X_{1145} = (1,0) - 5(0,1) = (1,-5)$

$2291 = 2 \cdot 1145 + 1$

$1 = 2291 - 2 \cdot 1145 \rightarrow X_1 = (0,1) - 2(1,-5)$

$X_{12600} = (1,0)$

$X_{2291} = (0,1)$

$X_1 = (-2, 11) \Rightarrow e = 11$

$\Rightarrow$ criptăm mesajul „IERI"

$N = 30$

$m = \text{IERI} = (8)(4)(17)(8)$ în baza 30

$\Rightarrow 8 \cdot 30^3 + 4 \cdot 30^2 + 17 \cdot 30^1 + 8 \cdot 30^0 =$

$216000 + 3600 + 510 + 8 = 220118$ în baza 10

știm deja că $f = 2$ și $l = 3$

$c = m^e \pmod{n}$

$c = 220118^{11} \pmod{12827}$

$\Rightarrow c = 220118 \cdot (220118^2)^5$

$= 2059 \cdot (2059^2)^5 = 2059 \cdot 6571 \cdot (6571^2)^2$

$= 10031 \cdot 2359^2$

$= 2796 \cdot 10780 = 2796 \cdot 2054 = 264$

$264 : 30 = 8$ $\quad$ $8 : 30 = 0$

240 $\quad$ 0

$= 24$ $\quad$ 8

$\Rightarrow$ mesajul criptat: $(0)(8)(24) = AiY$

2. $n = 2733$

e minim

$j = 2$

$l = 3$

---

criptare mesaj „OK"

$\sqrt{2733} = 52$

25 $\quad$ $102 \times 2 = 204$

$= 233$

204

$= 29$

$[\sqrt{2733}] = 52$

$\Rightarrow x = 53$

$x^2 - n = 53^2 - 2733 = (52+1)^2 - 2733 = 52^2 + 104 + 1 - 2733$

$= -29 + 105 = 76$

$x = 54$

$x^2 - n = 54^2 - 2733 = (53+1)^2 - 2733 = 53^2 + 106 + 1 - 2733$

$= 76 + 107 = 183$

$x = 55$

$x^2 - n = 55^2 - 2733 = (54+1)^2 - 2733 = 54^2 + 108 + 1 - 2733$

$= 183 + 109 = 292$

↳ După mai multe încercări am observat că această var. nu funcționează.

$2732 = \underbrace{3}_{p} \cdot \underbrace{911}_{q}$

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

$\Rightarrow e = 3$ minimal

OK (14)(10) $\rightarrow$ în baza 30 $\Rightarrow$ $14 \cdot 30^1 + 10 \cdot 30^0 = 420 + 10 = 430_{(10)}$

$\Rightarrow m = 430$

$c = m^e \pmod n$

$c = 430^3 \pmod{2732}$

$c = 430 \cdot 430^2 = 430 \cdot 1789 = 1297$

transf în baza 30:

$1297 : 30 = 43$ (120, rest 97; 90, rest 7)

$43 : 30 = 1$ (30, rest 13)

$\Rightarrow (1)(13)(7) = B\,N\,H$

3 $n = 187$

$e = 107$

a) cheia privată

b) mesaj = ABACFPFP

$j = 1$, $l = 2$

decriptare mesaj

a)

$\sqrt{187}$	13
1	$23 \cdot 3 = 69$
87	
69	
18	

$\lfloor \sqrt{187} \rfloor = 13$

$\Rightarrow x = 14$

$\Rightarrow x^2 - n = 14^2 - 187 = 13^2 + 26 + 1 - 187 = -18 + 27 = 35$

$x = 15 \Rightarrow x^2 - n = 15^2 - 187 = (14+1)^2 - 187 = 87 + 28 + 1 = 66$

$x = 16 \Rightarrow x^2 - n = 66 + 30 + 1 = 97$

$x = 17 \Rightarrow x^2 - n = 97 + 32 + 1 = 130$

$x = 18 \Rightarrow x^2 - n = 130 + 34 + 1 = 165$

$x = 19 \Rightarrow x^2 - n = 165 + 36 + 1 = 202$

$x = 20 \Rightarrow x^2 - n = 202 + 38 + 1 = 241$

$x = 21 \Rightarrow x^2 - n = 241 + 40 + 1 = 282$

$x = 22 \Rightarrow x^2 - n = 282 + 42 + 1 = 325$

AC. variantă nu funcționează aici.

$187 = \underbrace{11}_{p} \cdot \underbrace{17}_{q}$

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

aflăm d:

$d \equiv e^{-1} \pmod{\varphi(n)}$

$= 107^{-1} \pmod{160}$

$160 = 1 \cdot 107 + 53 \Rightarrow 53 = 160 - 1 \cdot 107 \Rightarrow X_{53} = (1,0) - (0,1) - (1,-1)$

$107 = 2 \cdot 53 + 1 \Rightarrow 1 = 107 - 2 \cdot 53 \Rightarrow X_1 = (0,1) - 2(1,-1) = (-2,1)$

$\Rightarrow \underline{d = 1}$

b) A B A C F P F P

(0) (1) (0) (2) (5) (15) (5) (15) $\longrightarrow 1 \cdot 30^6 + 2 \cdot 30^4 + 5 \cdot 30^3 + 15 \cdot 30^2 + 5 \cdot 30^1 + 15 \cdot 30^0$

$= 729958665$

$m' = 729958665^1 \pmod{187}$

$= 51$

729958665 : 187 = 3903522

561

1689

1683

658

561

976

935

416

374

425

374

51

transf în baza 30:

51 : 30 = 1

30

21

mesajul decriptat este:

(1) (21) = "BV"

4] $p = 7$

$q = 11$

$d > 1$ minim

a) (n, e)

b) decriptare mesaj "B!BT BL"

$j = 1, l = 2$

$n = p \cdot q = 7 \cdot 11 = 77$

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

$e \equiv d^{-1} \pmod{\varphi(n)} \Rightarrow e \equiv 7^{-1} \pmod{60}$

d = minim $\Rightarrow d = 7$

$x_{60} = (1,0)$, $x_7 = (0,1)$

$60 = 8 \cdot 7 + 4 \Rightarrow 4 = 60 - 8 \cdot 7 \Rightarrow x_4 = (1,0) - 8(0,1) = (1,-8)$

$7 = 1 \cdot 4 + 3 \Rightarrow 3 = 7 - 4 \Rightarrow x_3 = (0,1) - (1,-8) = (-1,9)$

$4 = 1 \cdot 3 + 1 \Rightarrow 1 = 4 - 3 \Rightarrow x_1 = (1,-8) - (-1,9) = (2,-17)$

$\Rightarrow e = -17 \pmod{60} = 43$

$\Rightarrow (n, e) = (77, 43)$

b) B ! B T B L $\rightarrow 1 \cdot 30^5 + 28 \cdot 30^4 + 1 \cdot 30^3 + 19 \cdot 30^2 + 1 \cdot 30^1 + 11 \cdot 30^0 =$

(1) (28) (1) (19) (1) (11) $= 47024141$

$m' = 47024141^{43} \pmod{77}$

$= 10 \cdot (10^2)^{21} = 10 \cdot 100 \cdot 100^2 = 1000 \cdot 100 = 76 \cdot 23 = (-1) \cdot 23 = -23$

$= 54$

transf în baza 30:

$54 : 30 = 1$

30

24

$\Rightarrow$ mesajul descriptat este:

(1)(24) = "BY"

5] $K_e = (n = 1189, e = 747)$

a) cheia privată

b) descriptați textul "BFCAFNBIW"

a) $N = 1189$

$e = 747$

$\sqrt{1189} \mid 34$

9 | $64 \times 4 = 266$

$= 289$

256

$= 33$

$\Rightarrow [\sqrt{1189}] = 34$

$\Rightarrow t = 35 \Rightarrow t^2 - n = 35^2 - 1189 = 34^2 + 68 + 1 - 1189 = 33 + 69$

$= 36 = 6^2$

$\Rightarrow n = 35^2 - 6^2 = (35+6)(35-6) = \underbrace{41}_{p} \cdot \underbrace{29}_{q}$

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

$d \equiv e^{-1} \pmod{\varphi(n)} = 747^{-1} \pmod{1120}$

$x_{1120} = (1,0)$; $x_{747} = (0,1)$

$1120 = 1 \cdot 747 + 373 \Rightarrow 373_1 = 1120 - 1 \cdot 747 \Rightarrow X_{373} = (1,0) - (0,1) = (1,-1)$

$747 = 2 \cdot 373 + 1 \Rightarrow 1 = 747 - 2 \cdot 373 \Rightarrow X_1 = (0,1) - 2(1,-1) = (-2,3)$

$\Rightarrow \underline{d = 3}$

b) $m' = 766\,912\,402\,162^3 \pmod{1189}$

B F C A F N B I W

(1) (5) (2) (0) (5) (13) (1) (8) (22)

↳ transf în baza 10:

$1 \cdot 30^8 + 5 \cdot 30^7 + 2 \cdot 30^6 + 0 \cdot 30^5 + 5 \cdot 30^4 + 13 \cdot 30^3 + 1 \cdot 30^2 + 8 \cdot 30^1 + 22 \cdot 30^0$

$= 766\,912\,402\,162$

$766\,912\,402\,162 : 1189 = 645\,006\,225$

7134

$= 5351$

4756

$= 5952$

5945

$= = = 7402$

7134

$= 2681$

2378

$= 3036$

2378

$= 6582$

5945

$= 637$

$m' = 637^3 \pmod{1189}$

$m' = 637 \cdot 637^2 \pmod{1189}$

$m' = 637 \cdot 735 \pmod{1189}$

$m' = 918 \pmod{1189}$

$\underline{m' = 918}$

transf în baza 30:

$918 : 30 = 3$

90

$= 18$

⇒ mesajul decriptat este:

(3)(18) = "Δ 3"

6] $g = 1$, $l = 2$

$p = 23$, $q = 17$

$(n, e = 3)$,

a) criptare mesaj "HELP_ME!"

b) decriptare mesaj "EBMMAAF OMMLIEBAIHi"

a) $n = p \cdot q = 23 \cdot 17 = 391$

$c = m^e \pmod n =$

H E L P _ M E !

(7) (4) (11) (15) (26) (12) (4) (28)

↳ în baza 10:

$7\cdot 30^7 + 4\cdot 30^6 + 11\cdot 30^5 + 15\cdot 30^4 + 26\cdot 30^3 + 12\cdot 30^2 + 4\cdot 30^1 + 28\cdot 30^0 =$

$= 156\,286\,162\,948$

$c = 156\,286\,162\,948^3 \pmod{391}$

$= 252\cdot 252^2 = 252\cdot 162 = 160$

transformăm în baza 30:

$160 : 30 = 5$ ⇒ mesajul criptat este:

150

$= 10$ (5)(10) = "F K"

b) $d \equiv e^{-1} \pmod{\varphi(n)}$ ⇒ $d \equiv 3^{-1} \pmod{352}$

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

$352 = 117\cdot 3 + 1$ ⇒ $X_1 = (1,0) - 117\cdot(0,1) = (1,0) + (0,-117) = (1,-117)$

⇒ $d = -117 = \underline{\underline{235}} \pmod{352}$

$m' = c^d \pmod n$

E B M M A A F _ O M M L ! E B A i H i

(4) (1) (12) (12) (0) (0) (5) (26) (14) (12) (12) (11) (28) (4) (1) (0) (8) (7) (8)

transf în baza 10:

$8\cdot 30^0 + 7\cdot 30^1 + 8\cdot 30^2 + 30^4 + 4\cdot 30^5 + 28\cdot 30^6 + 11\cdot 30^7 + 12\cdot 30^8 + 12\cdot 30^9 + 14\cdot 30^{10} + 26\cdot 30^{11}$

$+ 5\cdot 30^{12} + 12\cdot 30^{15} + 12\cdot 30^{16} + 30^{17} + 4\cdot 30^{18} = c$

⇒ $m' \equiv e^{235} \pmod{391}$

⇒ $m' = 8^{235} \pmod{391}$

$m' = 8\cdot(8^2)^{117} = 8\cdot 64\cdot(64^2)^{58} =$

$= 121\cdot(186^2)^{29} = 121\cdot 188\,(188^2)^{14}$

$= 70\cdot(154^2)^7 = 70\cdot 256\,(256^2)^3$

$= 325\cdot 239\cdot 239^2 = 257\cdot 35$

$= 2$ ⇒ "C"

calc fiecare comp (mod 391):

$c = 8 + 210 + 162 + 280 + 137 + 224 + 78 + 29$

$+ 105\cdot 12 + 105\cdot 30\cdot 14 + 105\cdot 30^2\cdot 26 +$

$+ 105\cdot 30^3\cdot 5 + 105\cdot 30^6\cdot 12 + 105\cdot 30^7\cdot 12$

$+ 105\cdot 30^8 + 105\cdot 30^9$

$c = 1090 + 87 + 308 + 347 + 77 + 49 +$

$+ 147 + 172 + 77$

$\underline{c = 8 \pmod{391}}$

calc fiecare comp mod 391

$8 \cdot 30^0 \pmod{391} = 8$

$1 \cdot 30^1 \pmod{391} = 210$

$8 \cdot 30^2 \pmod{391} = 8 \cdot 118 = 162$

$30^4 \pmod{391} = 118 \cdot 118 = 239$

$4 \cdot 30^5 \pmod{391} = 4 \cdot 239 \cdot 30 = 137$

$28 \cdot 30^6 \pmod{391} = 28 \cdot 239 \cdot 118 = 227$

$11 \cdot 30^7 \pmod{391} = 11 \cdot 239 \cdot 118 \cdot 30 = 78$

$12 \cdot 30^8 \pmod{391} = 12 \cdot 239 \cdot 239 = 12 \cdot 35 = 29$

$12 \cdot 30^9 \pmod{391} = 29 \cdot 30 = 88$

$14 \cdot 30^{10} \pmod{391} = 14 \cdot 35 \cdot 118 = 343$

$26 \cdot 30^{11} \pmod{391} = 26 \cdot 220 \cdot 30 = 26 \cdot 344 = 342$

$5 \cdot 30^{12} \pmod{391} = 5 \cdot 344 \cdot 30 = 150 \cdot 344 = 379$

$12 \cdot 30^{15} \pmod{391} = 12 \cdot 344 \cdot 239 = 99$

$12 \cdot 30^{16} \pmod{391} = 99 \cdot 30 = 233$

$30^{17} \pmod{391} = 106 \cdot 118 = 387$

$4 \cdot 30^{18} \pmod{391} = 4 \cdot 387 \cdot 30 = 302$

$c = 8 \cdot 210 \cdot 162 \cdot 239 \cdot 137 \cdot 227 \cdot 78 \cdot 29 \cdot 88 \cdot 343 \cdot 342 \cdot 379 \cdot 99 \cdot 233 \cdot 387 \cdot 302$

$c = 313 \cdot 346 \cdot 333$

$c = 131 \Rightarrow (4)(11) \rightarrow$ "EL"

$131 : 30 = 4$

120

$=11$

4 $n = 9991$

$e = 3917$

a) cheia privată

b) decriptare "BMHA_X"

a)
$\sqrt{9991} \mid 99$

$81 \mid 189 \cdot 9 = 1701$

1891

1701

$=190$

$[\sqrt{9991}] = 99$

$t = 100 \Rightarrow t^2 - n = 99^2 + 198 + 1 - 9991 = 190 + 199 = 9 - 3^2$

$\Rightarrow n = 190^2 - 3^2 = \underbrace{97}_{p} \cdot \underbrace{103}_{q}$

$\Rightarrow \varphi(n) = 96 \cdot 102 = 9792$

$d \equiv e^{-1} \pmod{\varphi(n)}$

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

$9792 = 2 \cdot 3917 + 1958 \Rightarrow 1958 = 9792 - 2 \cdot 3917 \Rightarrow X_{1958} = (1,0) - 2(0,1) = (1,-2)$

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

$\Rightarrow X_1 = (0,1) - 2 \cdot (1,-2) = (-2,5)$

$\Rightarrow \underline{d = 5}$

b)

B	M	H	A	_	X
(1)	(12)	(7)	(0)	(26)	(23)

transf în baza 10:

$23 \cdot 30^0 + 26 \cdot 30^1 + 0 \cdot 30^2 + 7 \cdot 30^3 + 12 \cdot 30^4 + 1 \cdot 30^5 =$

$= 23 + 780 + 0 + 189000 + 9720000 + 24300000$

$= 34209803$

$m' = 34209803^5 \pmod{9991}$

$= 619^5 \pmod{9991}$

$= 619 \cdot (619^2)^2 = 619 \cdot 3503^2$

$= 619 \cdot 2061 = 6902$

34209803 : 9991 = 3424

29973

= 42368

39964

= 24040

19982

= 40583

39964

== 619

transf în baza 30:

6902 : 30 = 230

60

= 90

90

== 2

230 : 30 = 7

210

= 20

(7)(20)(2) = HUC