Ident:

1 ⇒ $n = 12827 \quad d = 2291$

IERI

$(\varphi(n), e) = 1$

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

$2291 = e^{-1} \pmod{\varphi(n)}$

$\sqrt{12827} \mid 113$

$1 \mid 113 \cdot 1$

$= 28 \mid 223 \cdot 3$

21

$= 727$

669

$= 58$

113

113

339

113

113

12769

$x = 114$

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

$= 12769 + 226 + 1 - 12827 = 226 + 1 - 58 = 169$

$n = 114^2 - 13^2 \Rightarrow n = (114 - 13)(114 + 13) =$

$= (\cancel{101}) \; 101 \cdot 127$

$\varphi(n) = (101 - 1)(127 - 1) = 100 \cdot 126 = 12600$

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

$2291 = e^{-1} \pmod{12600}$

$(2291, 12600) = 1$

$12600 : 2291 = 5$
11455
1145

$12600 = 5 \cdot 2291 + 1145$

$2291 = 2 \cdot 1145 + 1$

~~$45 = 225 - 2 \cdot (1200 - \ldots$~~

~~x, x~~

$x_{2291} = (1, 0)$
$x_{12600} = (0, 1)$

$1145 = 12600 - 5 \cdot 2291$
$(0, 1) - 5 \cdot (1, 0) = (-5, 1)$

$1 = 2291 - 2 \cdot 1145$
$(1, 0) - 2(-5, 1) = (1, 0) - (-10, 2) = (11, -2)$

$1 = 11 \cdot 2291 - 2 \cdot 12600$

deci

$2291 = 11^{-1} \pmod{12600}$ $\Rightarrow d = 11$

cheia publică (12827, 11)

~~IE RI~~

~~I = 8~~

~~8 (17)~~

84 (17) 8

2 caractere => IE și RI

$IE = 8 \cdot 30 + 4 = 244_{(10)}$

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

~~$c = m^e \pmod{n_A}$~~

$c_1 = 244^{11} \pmod{12827}$

$244 \cdot 244^{10} = 244 \cdot (244^2)^5 =$

$= 244 \cdot (59536)^5 = 244 \cdot (8228)^5 =$

$= 244 \cdot 8228 \cdot (8228^2)^2 =$

$= 244 \cdot 8228 \cdot (67699984)^2 =$

$= 244 \cdot 8228 \cdot (11905)^2$

$= 244 \cdot 8228 \cdot 141729025 =$

$= 244 \cdot 8228 \cdot 3502 =$

$= 7347686280 = 8697$

244

244 ·
244
976
976
488
59536

$x = 8967 \pmod{12827}$

$x_2 = 518^{11} \pmod{12827}$

$= 7595$

(8967) (7595)

~~8967 : 30 = 2~~
~~60~~

$8967 = x \cdot 30^2 + b \cdot 30 + c$

8967 : 900 = 9
8100
= 867

867 : 30 = 28
60
267
240
= 27

~~27~~

$8967 = 9 \cdot 30^2 + 28 \cdot 30 + 27$

iE → j!?

$7595 = a \cdot 30^2 + b \cdot 30 + c$

7595 : 900 = 8
7200
= 395

395 : 30 = 12
30
= 95
90
= 5

$7595 = 8 \cdot 30^2 + 12 \cdot 30 + 5$

RI → 1 M F

IERI → ? ? 1 M F

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

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

IE → F L V

$518^{11} \mod 12827 = 7595 \mod 12827$

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

RI → I M F

IERI → F L V I M F

2. $n = 2733$

exponentul de criptare cel mai mic => $l = 3$

$(\varphi(n), l) = 1$

$\sqrt{2733}$ | $5 \quad 2$

25 | $5 \quad 4 \quad 4$

233 | $25 \quad 21$

204 | $102 \quad 2$

29

$x = 53$

$x^2 - n = 53^2 - 2733 = 2809 - 2733 = 76$

$n = 53^2 - \sqrt{76}$

$2733 : 3 = 911 \Rightarrow 2733 = 911 \cdot 3$

$\varphi(n) = (3-1)(911-1) = 2 \cdot 910 = 1820$

$(3, 1820) = 1$ $\Rightarrow e = 3$ cheie

$1820 : 3 = 606$ rest 2

cheie publică $(2733, 3)$

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

1410

$x = 430^3 \pmod{2733} \equiv 1297$

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

OK $\longrightarrow$ BNH

3. $n = 187$ $e = 107$

a)

187	13
169	3·3
87	
69	
18	

$t = 14$

$t^2 - n = 14^2 - 187 = 196 - 187 = 9$

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

$\varphi(n) = (11-1)(17-1) = 10 \cdot 16 = 160$

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

$107 \cdot x_{107} + 160 \cdot x_{160} = (1, 0)$

$160 - 107 = 53$

$107 - 53 \cdot 2 = 1$ $\Rightarrow 1 = 107 - 53 \cdot 2$

$53 = 160 - 107 \cdot 1$

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

$(1,0) - 2 \cdot (-1,1) = (1,0) - (-2,2) =$

$= (3, -2)$

$d \equiv 3 \pmod{160}$

$d = 3$

$\text{cmmdc}(187, 3)$

b) $\overline{A}\,\overline{B}\,\overline{A}\,\overline{C}\,\overline{F}\,\overline{P}\,\overline{E}\,\overline{P}$

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

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

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

$2^3 \pmod{187} \equiv 8 = I$

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

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

$AB\,AC\,FPEP \rightarrow BILL$

4 A $p = 7$ $q = 11$

$a > 1$

a. $\varphi(n) = 7 \cdot 11 = 77$

$\varphi(n) = (8-1) \cdot (12-1) \Rightarrow$

$\Rightarrow n = 8 \cdot 12 = 96$

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

$n = 77$

$\varphi(n) = (7-1)(11-1) = 6 \cdot 10 = 60$

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

$d \equiv e^{-1} \pmod{60} \Rightarrow 7 \equiv e^{-1} \pmod{60}$

~~60 7~~

$60 = 7 \cdot 8 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

$x_7 = (1, 0)$

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

$4 = 60 - 7 \cdot 8$

$3 = 7 - 4$

$1 = 4 - 3$

$(0, 1) - (1, 0) \cdot 8 = (-8, 1)$

$(1, 0) - (-8, 1) = (9, -1)$

$(-8, 1) - (9, -1) = (-17, 2)$

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

cheia $(77, 43)$

b) B! BT BL

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

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

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

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

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

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

B! BT BL $\rightarrow$ JON

5. (1189, 747)

$n = 1189$

$\sqrt{1189} = 34$

9

289

256

33

$6 \quad 4 \quad 4$

$t = 35$

$t^2 - n = 35^2 - 1189 = 1225 - 1189 = 36$

$n = 35^2 - 6^2 \Rightarrow n = (35-6)(35+6)$

$n = 29 \cdot 41$

$\varphi(n) = (29-1)(41-1) = 28 \cdot 40 = 1120$

$d \equiv e^{-1} \pmod{1120}$

$d \equiv 747^{-1} \pmod{1120}$

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

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

$1120 : 747 = 1 \quad +373$

$747 : 373 = 2 \quad +1$

$1 = 747 - 373 \cdot 2$

$373 = 1120 - 747$

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

$(1,0) - (-1,1) \cdot 2 = (1,0) - (-2,2) = (3,-2)$

$d = 3$

$(1189, 3)$ cheia privată

4)

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

$1 = j + 1 = 3$

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

$1052^3 \bmod 1189 = 454$

$454 = 15 \cdot 30 + 4$

BFC → PE

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

$163^3 \bmod 1189 \equiv 409$

$409 = 13 \cdot 30 + 19$

AFH → HT

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

$1162^3 \bmod 1189 \equiv 530$

$530 = 17 \cdot 30 + 20$

BIW → RU

BFCAFHBIW → PENTRU

6.

— → — 1 cuvant → 2 blocuri

$p = 23$ $q = 17$ $(n, e = 3)$

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

$7^3 \bmod 391 \equiv 343$

$343 = 11 \cdot 30 + 13$

$E = 4$

$4^3 \bmod 391 \equiv 64$

$64 = 2 \cdot 30 + 4$

HELP_ME !

74 (11) (15) (26) (12) (28)

$11^3 \mod 391 \equiv 158$

$158 = 5 \cdot 30 + 8$

$15^3 \mod 391 \equiv 247$

$247 = 8 \cdot 30 + 7$

$26^3 \mod 391 = 372$

$372 = 12 \cdot 30 + 12$

$12^3 \mod 391 = 164$

$164 = 5 \cdot 30 + 14$

$28^3 \mod 391 = 56$

$56 = 1 \cdot 30 + 26$

HELP_ME! -> LNCEFIIHMMMFOCEB_

b) $\varphi(n) = (23-1)(17-1) = 22 \cdot 16 = 352$

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

$352 : 3 = 117$

3

$= 5$

3

22

21

$= 1$

$1 = 352 - 117 \cdot 3$

$(1,0) - 117 \cdot [0,1)$

$(1,0) - (0, -117) = (1, -117)$

$352 - 117 = 255$

$d = 235$

chiba (391, 235)

EB = 4·30 + 1 = 121

$121^{235} \bmod 391 \equiv 8 = \overline{1}$

EB → I

MM = 12·30 + 12 = 372

$\bar{3}72^{235} \bmod 391 \equiv 26 =$ _

MM → _

AA = 0·30 + 0 = ~~372~~ 0

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

$121^{235} \bmod 391 \equiv 8 = 1$

EB → I

$AI = 0 \cdot 30 + 8 = 8$

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

AI → C

$HI = 7 \cdot 30 + 8 = 218$

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

HI → K

EB MAMAAFOMML!EBAIHI → I_AM_SICK

7. $n = 9991,\ e = 3917$

$\sqrt{9991}$

99 91 81 18 91 17 01 = 190	99 18 9 · 9

$t = 100$

$t^2 - n = 100^2 - 9991 = 10000 - 9991 = 9$

$n = 100^2 - 3^2 \Rightarrow (100-3)(100+3) \Rightarrow$

$\Rightarrow n = 97 \cdot 103$

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

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

$9792 : 3917 = 2 + 1958$

$3917 : 1958 = 2 + 1$

$1 = 3917 - 2 \cdot 1958$

$1 = 3917 - 2 \cdot (9792 - 2 \cdot 3917) = 5 \cdot 3917 - 2 \cdot 9792 \Rightarrow$

$\Rightarrow d = 5$

cheia privată (9991, 5)

a) BMHA_X

1 (12) 7 0 (26) (23)

$BMH = 1 \cdot 30^2 + 12 \cdot 30 + 7 = 1267$

$1267^5 \mod 9991 \equiv 404$

$404 = 13 \cdot 30 + 14$

BMH → NO

A_X = ~~21~~ $0 \cdot 30^2 + 26 \cdot 30 + 23 = 803$

$803^5 \mod 9991 \equiv 570$

$570 = 19 \cdot 30 + 0$

A_X → ~~T~~A

BMHA_X → NOTA