TEMA 7

1. $m = 12827$

$d = 2291$

$\sqrt{1.28.27}$ | 113

1 | $21 \cdot 1 = 21$

$=28$ | $223 \cdot 3 = 669$

21

669

$=58$

$[\sqrt{m}] = 113$

$t = 114$

$t^2 - m = 114^2 - m = (113+1)^2 - m = 113^2 + 226 + 1 - m = 227 - 58 =$

$= 169 = 13^2 \Rightarrow 114^2 - m = 13^2 \Rightarrow m = 114^2 - 13^2 =$

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

$\varphi(m) = (p-1)(q-1) = 100 \cdot 126 = 12600 = 10^2 \cdot 2 \cdot 63 = 5^2 \cdot 2^3 \cdot 3^2 \cdot 7$

$e = d^{-1} \bmod \varphi(m) = 2291^{-1} \pmod{12600}$

$(12600, 2291) = 1$

$12600 = 2291 \cdot 5 + 1145$

$2291 = 2 \cdot 1145 + (1)$

$1145 = 1145 \cdot 1 + 0$

$x_{12600} = (1,0) \quad x_{2191} = (0,1)$

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

$x_1 = x_{2191} - 2x_{1145} = (0,1) - 2(1,-5) = (0,1) - (2,-10) = (-2, 11)$

$\Rightarrow 2291^{-1} \equiv 11 \pmod{12600} \Rightarrow \boxed{e = 11} \Rightarrow (n = 12827, e = 11)$

cheia publică

$|ERI| = (8)(4)(17)(8)_{(30)}$

$|E| = (8)(4)_{(30)} = 8 \cdot 30 + 4 = 244 \rightarrow 4831$

$RI = (17)(8)_{(30)} = 17 \cdot 30 + 8 = 518 \rightarrow 1595$

$C = m^e \pmod n = 244^{11} \bmod 12827 = 244 \cdot (244^2)^5 =$

$= 244 \cdot \underbrace{59536}_{8228}{}^5 = 244 \cdot (-4599) \cdot (4599^2)^2 =$

-4599

$= -122 \cdot \underbrace{9198}_{-3629} \cdot (4599^2)^2 =$

$= \underbrace{442738}_{6620} \cdot \underbrace{21150801}_{11905}{}^2 = 6620 \cdot \underbrace{9212}_{-3615} = -8945 =$

-992

244	<
122	2
61	

$C = m^e \pmod n = 244^{11} \pmod{12827} = 244 \cdot (244)^5 =$

$= 244 \left[(2^2 \cdot 61)^2 \right]^5 = 244 \cdot (2^4 \cdot 61^2)^5 = 244 \cdot 2^4 \cdot 61^2 \cdot (2^4 \cdot 61^2)$

$= 2^6 \cdot 61^3 \cdot 2^{16} \cdot 61^8 = 2^{22} \cdot 61^{11} = 2048 \cdot 2048 \cdot 61^{11} =$

$= 1024 \cdot 4096 \cdot 61^{11} = 512 \cdot 8192 \cdot 61^{11} = 256 \cdot \underbrace{16384}_{+5557} \cdot 61^{11} =$

$= +256 \cdot 3557 \cdot 61^{11} = +128 \cdot 7114 \cdot 61^{11} = +64 \cdot \underbrace{14228}_{+1401} \cdot 61^{11}$

$= \cancel{64} \cdot 64 \cdot 1401 \cdot 61^{11} = 32 \cdot 2802 \cdot 61^{11} =$

$= 16 \cdot 5604 \cdot 61^{11} = 8 \cdot \underbrace{11208}_{-1619} \cdot 61^{11} = -\underbrace{12952}_{125} \cdot 61^{11} =$

$= \underbrace{-125 \cdot 61}_{5202} \cdot (61^2)^5 = 5202 \cdot 3721 \cdot (3721^2)^2 =$

$+7625$

$= 1734 \cdot \underbrace{11163}_{} \cdot (3721^2)^2 =$

$= \underbrace{-1734 \cdot 1664}_{699} \cdot \underbrace{5508}_{2209}{}^2 = 699 \cdot 2209 = 4851$

12128

$C = m^e \pmod n = 518^{11} \pmod{12824} =$

518	2
259	4
37	

$= \cancel{518 \cdot (518^2)^5} \cdot 518^{11} = 2^{11} \cdot 7^{11} \cdot 37^{11} =$

$= 2048 \cdot 7 \cdot (7^2)^5 \cdot 37 \cdot (37^2)^5 =$

$= \underbrace{2048}_{19336} \cdot 7 \cdot 49 \cdot (49^2)^2 \cdot 37 \cdot 1369 \cdot (1369^2)^2$

$= \underbrace{1509 \cdot 49}_{9806} \cdot \underbrace{2401}^2 \cdot \underbrace{37 \cdot 1369}_{12549} \cdot \underbrace{1919}^2$

$= 9806 \cdot 5478 \cdot 12172 \cdot$

$= (-3021) \cdot 5478 \cdot (-655) \cdot (-278)$

$= -2208 \cdot 2512$

$= -5232 = \underline{7595}$

9851 : 30 = 161
30
185
180
51
30
21

161 : 30 = 5
150
11

5 : 30 = 0
0
5

$\Leftrightarrow 9851 = (5)(11)(21) = FLV$

7595 : 30 = 255
60
159
150
95
90
5

255 : 30 = 8
240
15

8 : 30 = 0
0
8

$7595 = (8)(15)(5) = INF$

IERi $\longrightarrow$ FLVINF

2. $n = 2733$

ℓ - minim

$j = 2,\ l = j+1 = 3$.

Ok

$\lfloor \sqrt{2733} \rfloor = 52$

$t = 53$

$t^2 - n = 53^2 - n = (52+1)^2 - n = 52^2 + 104 + 1 - n = 105 - 29 =$

$= 76 = 2^2 \cdot 19$

$t = 54$

$t^2 - n = (53+1)^2 - n = 53^2 + 106 + 1 - n = \cancel{107 - 29 = 78 = 2 \cdot 39}$

$= 107 + 76 = 183$

$t = 55$

$t^2 - n = 54^2 + 109 - n = 109 - 29 = 80 = 2^4 \cdot 5$

$t = 56$

$t^2 - n = 55^2 + 110 + 1 - n = 111$

$t = 55$

$t^2 - n = 54^2 + 109 - n = 109 + 183 = 292$

$t = 56$

$t^2 - n = 55^2 + 111 - n = 111 + 292 = 403$

$t = 57$

$Ok = (14)(10)_{(20)} = 14 \cdot 30 + 10 =$

$= 420 + 10 = 430$

$n = 2733 = 3 \cdot 911$

$p \quad q$

$\varphi(n) = (p-1)(q-1) = 2 \cdot 910 = 1820$

$= 2^2 \cdot 5 \cdot 91$

$\Rightarrow \ell \neq 2, 5, 91 \Rightarrow \boxed{\ell = 3}$

$1820 = 2^2 \cdot 5 \cdot 91$

$910 = 2 \cdot 5 \cdot 91$

$455 = 5 \cdot 91$

91

$c = m^l \pmod n = 430^3 \pmod{2733} = 430 \cdot 430^2 =$

$= 430 \cdot 43^2 \cdot 100 = 430 \cdot 1849 \cdot 100 = 4300 \cdot 18490 =$

$= +1567 \cdot \underbrace{2092}_{-641} = -641 \cdot 1567 = -1436 = 1297$

1297 : 30 = 43 | 43 : 30 = 1 | 1 : 30 = 0

120 | 30 | 0

97 | (13) | (1)

90

(7)

$c = (7)(13)(1) = (1)(13)(7) = B\ N\ H$

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

a) $d = ?$

b) $i = 1, l = 2 \Rightarrow ABACFAFA = ?$

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

$n = 187 = \underset{p}{17} \cdot \underset{q}{11}$

$\varphi(n) = (p-1)(q-1) = 16 \cdot 10 = 160$

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

$(160, 107) = 1$

$160 = 1 \cdot 107 + 53$

$107 = 2 \cdot 53 + (1)$

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

$x_{53} = (1, 0) - (0, 1) = (1, -1)$

$x_1 = x_{107} - 2 x_{53} = (0, 1) - (2, -2) = (-2, (3)) \Rightarrow \underline{d = 3}$

$\Rightarrow (n = 187, d = 3)$ cheia privată