DOSOFTEI GEORGIANA-PARASCHEVA

TEMA 7

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

$N = 30$

$\varphi(n) = (p-1)(q-1)$

$\lfloor \sqrt{n} \rfloor = \lfloor \sqrt{12827} \rfloor = 113$

$\sqrt{1.28.27}$ | 113

1 | $21 \cdot 1 = 21$

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

21

$=727$

669

$=58$

$t = \lfloor \sqrt{12827} \rfloor + 1 = 113 + 1 = 114$

$t^2 - n = 12\,996 - 12827 = 169 = 13^2$

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

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

$e \cdot d \equiv 1 \pmod{12600}$

$e \equiv d^{-1} \pmod{12600}$

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

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

$12600 : 2291 = 5 \quad x_{1145} = x_{12600} - 5 \cdot x_{2291} = (1,-5)$

$11\,455$

$1\,145$

$2291 \mid 1145$

$2290 \mid 2$

$=\!=\!=1$

$x_1 = x_{2291} - 2\, x_{1145} = (-2, 11) \Rightarrow$

$\Rightarrow e = 11. \quad K_e = (n = 12\,827,\ e = 11)$

$j = 2$
$l = 3$

iE

$m = 8 \cdot 30 + 4 = 240 + 4 = 244$

$c = 244^{11} \pmod{12\,827} = 244 \cdot 244^{10} \pmod{12\,827} =$

$= 244 \cdot (244^2)^5 \pmod{12\,827} = 244 \cdot 59\,536^5 \pmod{12\,827} =$

$= 244 \cdot 4599^5 \pmod{12\,827} = 244 \cdot 4599 \cdot (4599^2)^2 \pmod{12\,827} =$

$= 1\,122\,156 \cdot (4599^2)^2 \pmod{12\,827} = 6207 \cdot 21\,150\,801^2 \pmod{12\,827} =$

$= 6207 \cdot 11\,905^2 = 6207 \cdot 141\,729\,025 \pmod{12\,827} =$

$= 6207 \cdot 3502 \pmod{12\,827} = 21\,736\,914 \pmod{12\,827} =$

$= 8003 \pmod{12\,827}.$

$8003 : 30 = 266$ (60; 200; 180; $= 203$; 180; $= 23$)

$266 : 30 = 8$ (240; $= 26$)

$8 : 30 = 0$ (0; 8)

$8003 = 8 \cdot 30^2 + 26 \cdot 30 + 23$

Criptarea lui iE este i␣X.

Ri

$m = 17 \cdot 30 + 8 = 510 + 8 = 518$

$c = 518^{11} \pmod{12\,827} = 518 \cdot (518^2)^5 \pmod{12\,827} =$

$= 518 \cdot 268\,324^5 \pmod{12\,827} = 518 \cdot 11\,784^5 \pmod{12\,827} =$

$= 518 \cdot 11\,784 \cdot (11\,784^2)^2 \pmod{12\,827} = 6\,104\,112 \cdot (11\,784^2)^2 \pmod{12\,827} =$

$= 11\,287 \cdot 138\,862\,656^2 \pmod{12\,827} =$

$= 11\,287 \cdot 10\,381^2 \pmod{12\,827} = 11\,287 \cdot 107\,765\,161 \pmod{12\,827} =$

$= 11\,287 \cdot 5534 \pmod{12\,827} = 62\,462\,258 \pmod{12\,827} =$

$= 7595 \pmod{12\,827}$

7595 : 30 = 253
60

159
150

==95
90

=5

253 : 30 = 8
240

=13

8 : 30 = 0
0

8

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

Criptarea lui RI este INF.

IERI criptat este i␣X INF.