Tema 7

Nr. 22

$\sqrt{12827} = 113$

$\sqrt{12827}$	113
1	$21 \cdot 1 = 21$
=28	$223 \cdot 3 = 669$
21	
==727	
669	
58	

$t = 114$

$114^2 - 12827 = 12996 - 12827$

$= 169 = 13^2$

$114^2 - m = 13^2$

$m = 114^2 - 13^2$

$m = (114 - 13)(114 + 13)$

$m = 101 \cdot 127$

$n_A = 101 \cdot 127$ $\quad p_A = 101 \quad q_A = 127$

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

$= 100 \cdot 126$

$= 12600$

$d_A \cdot e_A \equiv 1 \mod (12600)$

$d_A = 2291$

$2291 \cdot e_A \equiv 1 \mod (12600)$

folosind algoritmul extins al lui Euclid aflăm e_A ☺

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

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

~~$12600 : 2291 =$~~

$12600 = 2291 \cdot 5 + 1145$ $\quad x_{1145} = x_{12600} - 5 \cdot x_{2291} = (1,0) - 5(0,1)$

$2291 = 1145 \cdot 2 + 1$ $\quad = (1,0) - (0,5)$

$= (1,-5)$

$x_1 = x_{2291} - 2 \cdot x_{1145} = (0,1) - 2(1,-5) = (0,1) - (2,-10)$

$= (-2, 11)$

$x_{1145} = (1, -5)$ $x_1 = (-2, 11)$ $1 = -2 \cdot 12600 + 11 \cdot 2291$

$Q_A = 11$

$k_{e_A} = (11, 12827)$

$k_{d_A} = (2291, 12827)$

$i = 8$

$E = 4$

$R = 17$

$i = 8$

Textul "iERi" este impărțit în blocuri de 2 caractere:

"iE" = 84

"Ri" = 178

$iE = 84 \Rightarrow m = 84 \Rightarrow c = 84^{11} \pmod{12827}$

$= 84 \cdot (84^2)^5 \pmod{12827}$

$\equiv 84 \cdot (7056)^5 \pmod{12827}$

$\equiv 84 \cdot 7056 \cdot (7056^2)^2 \pmod{12827}$

$\equiv 592704 \cdot (49727136)^2 \pmod{12827}$

$\equiv 2662 \cdot 5549^2 \pmod{12827}$

$\equiv 2662 \cdot 30791101 \pmod{12827}$

$\equiv 2662 \cdot 6601 \pmod{12827}$

$\equiv 17571262 \pmod{12827}$

$\equiv 11699$

$Ri = 127 \Rightarrow m = 127 \Rightarrow c = 127^{11} \pmod{12827}$

$c = 127^{8+2+1} \pmod{12827}$

$c = 127 \cdot 127^2 \cdot 127^8 \pmod{12827}$

$c = 127 \cdot 16129 \cdot 127^8 \pmod{12827}$

$c = 127 \cdot 3302 \cdot (127^4)^2 \pmod{12827}$

$c = 127 \cdot 3302 \cdot 11226 \pmod{12827}$

$c = 47447174 \bmod 12827$

$c = 7118$

$c = 127 \cdot 3302 \cdot 254^2 \pmod{12827}$

$c = 127 \cdot 3302 \cdot 381 \pmod{12827}$

$c = 159\,773\,874 \pmod{12827}$

$c = 762$

Astfel, textul "IERI" criptat folosind (11, 12827) este reprezentat de blocurile 11699 și 762.