Tema 9

23. Alice utilizează criptosistemul Robin cu modulul n=713 și primește mesajul criptat c=289. Determinați cele 4 posibilități pentru mesajul in clar

$$\begin{array}{l|l} \sqrt{7.13} = & 26 \\ \underline{4} & 46 \times 6 \\ 313 & \end{array}$$

$n = [\sqrt{713}] = 26$

$t = n+1 \Rightarrow t = 27$

$t^2 - n = 729 - 713 = 16 = 4^2$

$n = (27-4)(27+4) = \underset{\substack{\uparrow \\ p}}{23} \cdot \underset{\substack{\uparrow \\ q}}{31}$

$u \cdot p + v q = 1$

$u \cdot 23 + v \cdot 31 = 1$

$x_{31} = (1,0)$

$x_{23} = (0,1)$

$31 : 23 = 1$ rest 8

$x_8 = x_{31} - x_{23} = (1,0) - (0,1) = (1,-1)$

$23 : 8 = 2$, rest 7

$x_7 = x_{23} - 2x_8 = (0,1) - 2(1,-1) = (-2,3)$

$8 : 7 = 1$ rest 1

$x_1 = x_8 - x_7 = (1,-1) - (-2,3) = (3,-4)$

$\boxed{u=-4}$. $\boxed{v=3}$

- $r = c^{\frac{p+1}{4}} \pmod p = 289^{\frac{24}{4}} \pmod{23} = 289^6 \pmod{23} = 13^6 \pmod{23}$

$= (13^2)^3 \pmod{23} = 169^3 \pmod{23} = 8^3 \pmod{23} = 64 \cdot 8 \pmod{23} = -40 (\bmod 23$

$= 6$

- $s = c^{\frac{q+1}{4}} \pmod q = 289^8 \pmod{31} = 10^8 \pmod{31} = (10^4)^2 \pmod{31} = 18^2 \pmod{31}$

$= 324 \pmod{31} = 14$

$x = u \cdot p \cdot s + v \cdot q \cdot r \pmod n = -4 \cdot 23 \cdot 14 + 3 \cdot 31 \cdot 6 \pmod{713} =$

$= -1288 + 558 \pmod{713} = 696$

$-x = -696 \pmod{713} = 17$

- $y = ups - v \cdot g \cdot r \pmod{n} = -1288 - 558 \pmod{713} = -1846 \pmod{713}$
  $= 293$

- $y = -293 \pmod{713} = 420$

Transformăm rezultatele în baza 2:

$$\begin{cases} 696_{(10)} = 1010111000_{(2)} \\ 17_{(10)} = 10001_{(2)} \\ 293_{(10)} = 100100101_{(2)} \\ 420_{(10)} = 110100100_{(2)} \end{cases}$$