

~~n=713~~

TEMA 9

$$n=713$$

$$k=289 \text{ diptat}$$

msj sm dar?

$$\begin{array}{r} 31 \\ 322 \end{array}$$

$$m = \lceil \sqrt{713} \rceil = 26$$

$$\text{Fie } t=27 \Rightarrow t^2 - n = 729 - 713 = 16 = 4^2$$

Deci ~~$n = (t-s)(t+s) = (27-4)(27+4) = 23 \cdot 31$~~

$$n = (27-4)(27+4) = 23 \cdot 31$$

\neq

$$u \cdot p + v \cdot q = 1$$

$$31 : 23 = 1, r. 8$$

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

$$\begin{aligned} X_8 &= X_{31} - X_{23} = (1, 0) - (0, 1) = \\ &= (1, -1) \end{aligned}$$

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

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

$$23 : 8 = 2, r. 7$$

$$\begin{aligned} X_7 &= X_{23} - 2 \cdot X_8 = (0, 1) - 2 \cdot (1, -1) = \\ &= (-2, 3) \end{aligned}$$

$$8 : 7 = 1, r. 1$$

$$X_1 = X_8 - X_7 = (1, -1) - (-2, 3) = (3, -4)$$

$1-2$

$$u = -4 ; v = 3$$

$$\begin{aligned}
 \bullet k &= c^{\frac{p+1}{4}} \pmod{p} = \cancel{289} & \begin{cases} p=23 \\ q=31 \end{cases} \\
 &= 289^{\frac{2489}{4}} \pmod{23} = 289^6 \pmod{23} = 13^6 \pmod{23} \\
 &= (13^2)^3 \pmod{23} = 169^3 \pmod{23} = 8^3 \pmod{23} \\
 &= 64 \cdot 8 \pmod{23} = -40 \pmod{23} = \underline{\underline{6}}
 \end{aligned}$$

$$\begin{aligned}
 \bullet s &= c^{\frac{q+1}{4}} \pmod{q} = 289^8 \pmod{31} = \\
 &= 10^8 \pmod{31} = \underbrace{(10^4)^2}_{10000} \pmod{31} = 18^2 \pmod{31} \\
 &= 324 \pmod{31} = \underline{\underline{14}}
 \end{aligned}$$

$$\begin{aligned}
 \bullet X &= ups + vgr \pmod{n} = -4 \cdot 23 \cdot 14 + 3 \cdot 31 \cdot 6 \pmod{713} \\
 &= -1288 + 558 \pmod{713} = \underline{\underline{696}} \\
 -X &= -696 \pmod{713} = \underline{\underline{17}}
 \end{aligned}$$

$$\begin{aligned}
 \bullet y &= ups - vgr \pmod{n} = -1288 - 558 \pmod{713} \\
 &= -1846 \pmod{713} = \underline{\underline{293}}
 \end{aligned}$$

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

transf. in baza 2

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