TEMA 9

~~n=713~~

n=713
c=289 criptat

msj în clar?

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

31
322

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

Deci ~~n = (t-s)(t+s) = (27-6)(27+6) = 21·32~~

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

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

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

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

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

$31:23=1, r.8$

$X_8=X_{31}-X_{23}=(1,0)-(0,1)=(1,-1)$

$23:8=2, r.7$

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

$8:7=1, r.1$

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

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

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

$p = 23$
$q = 31$

$= (13^2)^3 \pmod{23} = 169^3 \pmod{23} = 8^3 \pmod{23}$

$= 64 \cdot 8 \pmod{23} = -40 \pmod{23} = \underline{6}$

• $S = c^{\frac{q+1}{4}} \pmod q = 289^8 \pmod{31} =$

$= 10^8 \pmod{31} = \underbrace{(10^4)^2}_{10000} \pmod{31} = 18^2 \pmod{31}$

$= 324 \pmod{31} = \underline{14}$

• $X = ups + vgr \pmod n = -4 \cdot 23 \cdot 14 + 3 \cdot 31 \cdot 6 \pmod{713}$

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

$-X = -696 \pmod{713} = \underline{17}$

• $y = ups - vgr \pmod n = -1288 - 558 \pmod{713}$

$= -1846 \pmod{713} = \underline{293}$

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

transf. în baza 2

$696_{(10)} = 1010111000_{(2)}$

$17_{(10)} = 10001_{(2)}$

$293_{(10)} = 100100101_{(2)}$

$420_{(10)} = 110100100_{(2)}$