Temă ~ protocolul Shamir

1.

$n=6$

$m=3$

$\mathbb{Z}_{31}$

$(1,13)$; $(30,9)$; $(2,18)$; $(29,4)$; $(3,25)$; $(28,13)$

Determinați secretul #

$F(X)=ax^2+bx+c$

$F(1)=13 \Leftrightarrow a+b+c=13$

$F(\underset{-1}{\underset{\|}{30}})=9 \Leftrightarrow (-1)^2a-b+c=9$

$F(2)=18 \Leftrightarrow 4a+2b+c=18$

$F(\underset{-2}{\underset{\equiv}{29}})=4 \Leftrightarrow 4a-2b+c=4$

$F(3)=25 \Leftrightarrow 9a+3b+c=25$

$F(\underset{-3}{\underset{\|}{28}})=13 \Leftrightarrow 9a-3b+c=13$

$$\begin{cases} a+b+c=13 \\ a-b+c=9 \\ 4a+2b+c=18 \end{cases} \Rightarrow \begin{cases} 2b=4 \quad |2^{-1}=16 \\ a-b+c=9 \\ 4a+2b+c=18 \end{cases} \Rightarrow \begin{cases} b=64=2 \\ a-2+c=9 \\ 4a+4+c=18 \end{cases}$$

$2\cdot 16 \equiv 1 \bmod 31 \Rightarrow 2^{-1}=16$ (în $\mathbb{Z}_{31}$)

$$\Rightarrow \begin{cases} b=2 \\ a+c=11 \\ 4a+c=14 \end{cases} (-)$$

$3a=3 \quad |3^{-1}=$

$a=1$

$b=2$

$c=10$

$F(X)=X^2+2X+10 \hookrightarrow$ mesajul secret

~~$4=4+10$~~