Tema 11
Valachi Emilia, M532

Profesorul de criptografie folosește protocolul Shamir de secret splitting cu $n = 6$ și pragul $m = 3$.
El alege corpul $\mathbb{Z}_{31}$, și comunică unele:

$(1, 13^{11})$ $(30, 9^{12})$ $(2, 18^{13})$ $(29, 4^{14})$ $(3, 25^{15})$ $(28, 13^{16})$

Determinați secretul.

$$F(x) = a_2 x^2 + a_1 x + \underbrace{M}_{?}, \quad a_i \in \mathbb{Z}_{31}$$

Vom folosi primele 3 umbre: (3 puncte sunt suficiente)

$$\begin{cases} F(1) = a_2 \cdot 1^2 + a_1 \cdot 1 + a_0 = 13 \\ F(30) = a_2 \cdot 30^2 + a_1 \cdot 30 + a_0 = 9 \\ F(2) = a_2 \cdot 2^2 + a_1 \cdot 2 + a_0 = 18 \end{cases} \iff$$

$$\begin{cases} a_2 + a_1 + a_0 = 13 \\ 900 a_2 + 30 a_1 + a_0 = 9 \\ 4 a_2 + 2 a_1 + a_0 = 18 \end{cases} \xrightarrow[(\text{mod } 31)]{\text{aplic.}} \begin{cases} a_2 + a_1 + a_0 = 13 \\ a_2 - a_1 + a_0 = 9 \\ 4 a_2 + 2 a_1 + a_0 = 18 \end{cases} \quad (-)$$

$$\Rightarrow \begin{cases} 2a_1 = 4 \Rightarrow \boxed{a_1 = 2} \\ a_2 + a_0 = 11 \\ 4a_2 + a_0 = 14 \end{cases} (-) \Rightarrow \begin{cases} a_1 = 2 \\ 3a_2 = 3 \Rightarrow \boxed{a_2 = 1} \\ a_0 = 10 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} a_1 = 2 \\ a_2 = 1 \\ a_0 = 10 \end{cases} \Rightarrow F(x) = x^2 + 2x + \boxed{10} = M$$

$\Rightarrow$ secretul este 10.