Tema 11 - Criptografie

1. protocolul Shamir de secret splitting

$n = 6$
pragul $m = 3$

$\mathbb{Z}_{31}$.

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

dat secretul

$m = 3 \Rightarrow$ este suficient să folosim doar 3 puncte. pt polinom

fie $(1,13)$; $(2,18)$; $(3,25)$ $\qquad F(X) = aX^2 + bX + M$

$x_1 = 1 \qquad \Delta_1 = F(x_1) = 13$

$x_2 = 2 \qquad \Delta_2 = F(x_2) = 18$

$x_3 = 3 \qquad \Delta_3 = F(x_3) = 25$

$$\begin{cases} a + b + M = 13 & (1) \\ 4a + 2b + M = 18 & (2) \\ 9a + 3b + M = 25 & (3) \end{cases}$$

$$\Rightarrow \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 9 & 3 & 1 \end{pmatrix}}_{\Delta} \cdot \begin{pmatrix} a \\ b \\ M \end{pmatrix} = \begin{pmatrix} 13 \\ 18 \\ 25 \end{pmatrix}$$

$$\Delta = \begin{vmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 9 & 3 & 1 \end{vmatrix} = 1\cdot 2\cdot 1 + 1\cdot 1\cdot 9 + 1\cdot 4\cdot 3 - 1\cdot 2\cdot 9 - 1\cdot 3\cdot 1 - 1\cdot 4\cdot 1 = 2 + 9 + 12 - 18 - 3 - 4$$

$\Rightarrow \Delta = -2$ în $(\mod 31) \Rightarrow \Delta = 29$

$$\Delta a = \begin{vmatrix} 13 & 1 & 1 \\ 18 & 2 & 1 \\ 25 & 3 & 1 \end{vmatrix} = 13\cdot 2 + 25 + 18\cdot 3 - 25\cdot 2 - 13\cdot 3 - 18$$

$$= 26 + 25 + 54 - 50 - 39 - 18$$

$\Delta a = -2 \Rightarrow \Delta a = 29 \pmod{31}$

$$\Delta b = \begin{vmatrix} 1 & 13 & 1 \\ 4 & 18 & 1 \\ 9 & 25 & 1 \end{vmatrix} = 18 + 13\cdot 9 + 4\cdot 25 - 18\cdot 9 - 25 - 4\cdot 13$$

$$= 18 + 117 + 100 - 162 - 25 - 52$$

$\Delta b = -4 \pmod{31} \Rightarrow \Delta b = 27$

$$\Delta_M = \begin{vmatrix} 1 & 1 & 13 \\ 4 & 2 & 18 \\ 9 & 3 & 25 \end{vmatrix} = 2\cdot 25 + 18\cdot 9 + 4\cdot 3\cdot 13 - 13\cdot 2\cdot 9 - 18\cdot 3 - 4\cdot 25$$

$$= 50 + 162 + 156 - 234 - 54 - 100$$

$$\Delta_M = -20 \pmod{31} \Rightarrow \underline{\Delta_M = 11}$$

aplicăm form. lui Cramer:

$$a = \frac{\Delta_a}{\Delta} = \frac{29}{29} = 1 \Rightarrow \underline{a = 1}$$

$$b = \frac{\Delta_b}{\Delta} = \frac{27}{29} \equiv 27 \cdot 29^{-1} \pmod{31} = 27 \cdot 15 \pmod{31} = 2 \Rightarrow \underline{b = 2}$$

$31 = 1 \cdot 29 + 2 \Rightarrow x_2 = (1,0) - (0,1) = (1,-1)$

$29 = 14 \cdot 2 + 1 \Rightarrow x_1 = (0,1) - 14(1,-1) = (-14, 15)$

$$M = \frac{\Delta_M}{\Delta} = \frac{11}{29} = 11 \cdot 29^{-1} \pmod{31} = 11 \cdot 15 \pmod{31} = 10 \Rightarrow \underline{M = 10}$$