TEMA - SII

Secret Sharing

1. $p = 1100111011$

$v_1 = 1000100101$

$v_2 = 0011101101$

$v_3 = 1011101101$

$m = 3$ ~~4~~

~~$p = r_1$~~

~~$v_1 = r_1 + r_2 = p + r_2$~~

~~$v_2 = r_2 + r_3$~~

~~$v_3 = r_3$~~ +

$p = s_1 = r_1$

$v_1 = s_2 = r_1 \oplus r_2 = s_1 \oplus r_2$

$v_2 = s_3 = r_2 \oplus r_3$

$v_3 = s_4 = r_3 \oplus m$

$s_1 \oplus s_2 = r_1 \oplus (r_1 \oplus r_2) = (r_1 \oplus r_1) \oplus r_2 = r_2$

$(s_1 \oplus s_2) \oplus s_3 = r_2 \oplus (r_2 \oplus r_3) = (r_2 \oplus r_2) \oplus r_3 = r_3.$

$(s_1 \oplus s_2 \oplus s_3) \oplus s_4 = r_3 \oplus (r_3 \oplus m) = (r_3 \oplus r_3) \oplus m = m$

$\Rightarrow \boxed{m = 1100011110}$

Protocolul Shamir

$\Rightarrow$ pol. de gr. 2.

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

1. $n = 6$, $m = 3$

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

$F(x) = ax^2 + bx + c \in \mathbb{Z}_{31}[x]$

$x_1 = 1 \quad s_1 = F(x_1) = 13$

$x_2 = 30 = -1 \quad s_2 = F(x_2) = 9$

$x_3 = 2 \quad s_3 = F(x_3) = 18$

$x_4 = 29 = -2 \quad s_4 = F(x_4) = 4$

$x_5 = 3 \quad s_5 = F(x_5) = 25 = -6$

$x_6 = 28 = -3 \quad s_6 = F(x_6) = 13.$

$b + c = 13 \qquad + 2c = 22$

Fol. pol. Lagrange pt. punctele $(1,13),(30,9),(2,18)$.

$$F(X) = \sum_{i=1}^{3} \prod_{j\neq i} \frac{x-x_j}{x_i-x_j} \cdot y_i$$

$$= \frac{x-30}{1-30}\cdot\frac{x-2}{1-2}\cdot 13 + \frac{x-1}{30-1}\cdot\frac{x-2}{30-2}\cdot 9 + \frac{x-1}{2-1}\cdot\frac{x-30}{2-30}\cdot 18 =$$

$$= \frac{x-30}{-29}\cdot\frac{x-2}{-1}\cdot 13 + \frac{x-1}{29}\cdot\frac{x-2}{28}\cdot 9 + \frac{x-1}{1}\cdot\frac{x-30}{-28}\cdot 18 =$$

$$= (x-30)(x-2)\cdot 13\cdot 29^{-1} + (x-1)(x-2)\cdot 9\cdot 29^{-1}\cdot 28^{-1} + (x-1)(x-30)\cdot 18\cdot \underset{3}{(-28)}^{-1}$$

$$= (x-30)(x-2)\cdot 13\cdot 15 + (x-1)(x-2)\cdot 9\cdot 15\cdot 10 + (x-1)(x-30)\cdot 18\cdot 21 =$$

$$= (x-30)(x-2)\cdot 9 + (x-1)(x-2)\cdot 17 + (x-1)(x-30)\cdot 6 =$$

$$= (x^2-2x-30x+60)\cdot 9 + (x^2-2x-x+2)\cdot 17 + (x^2-30x-x+30)\cdot 6 =$$

$$= \cancel{(9x^2}\ 9(x^2-32x+60) + 17(x^2-3x+2) + 6(x^2-31x+30) =$$

$$= 9(x^2-x+60) + 17(x^2-3x+2) + 6(x^2-1) =$$

$$= x^2(9+17+6) + x(-9-51) + (9\cdot 60 + 17\cdot 2 - 6).$$

$$= x^2 + 2x + \underline{\underline{10}}$$