DOSOFTEI GEORGIANA-PARASCHEVA

TEMA 11

1. Profesorul de la disciplina criptografie comunică cu voi și secretariat nota de la disciplina criptografie folosind protocolul Shamir de secret splitting cu $n=6$ și prag $m=3$. El alege corpul $\mathbb{Z}_{31}$ și comunică urmele $(1,13), (30,9), (2,18), (29,4), (3,25), (28,13)$. Determinați secretul.

$$f(x) = a_0 + a_1 x + a_2 x^2$$

$$f(x) = y_1 \frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)} + y_2 \frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)} + y_3 \frac{(x-x_1)(x-x_2)}{(x_3-x_1)(x_3-x_2)}$$

$(1,13)$
$(30,9)$
$(2,18)$

$$f(0) = 13 \cdot \frac{(0-30)(0-2)}{(1-30)(1-2)} + 9 \cdot \frac{(0-1)(0-2)}{(30-1)(30-2)} + 18 \cdot \frac{(0-1)(0-30)}{(2-1)(2-30)} =$$

$$L_1(0) = \frac{-30 \cdot (-2)}{-29 \cdot (-1)} = \frac{60}{29} \bmod 31 = 60 \cdot 29^{-1} \bmod 31 =$$

$$= 60 \cdot 15 \bmod 31 = 900 \bmod 31 = 1$$

$$L_2(0) = \frac{-1 \cdot (-2)}{29 \cdot 28} = \frac{2}{812} \bmod 31 = 2 \cdot 812^{-1} \bmod 31 = 2 \cdot 26 \bmod 31 =$$

$$= 52 \bmod 31 = 21 \bmod 31$$

$$L_3(0) = \frac{-1 \cdot (-30)}{1 \cdot (-28)} = \frac{30}{-28} \bmod 31 = \frac{30}{3} \bmod 31 = 10 \bmod 31$$

$f(0) = 13 \cdot 1 + 9 \cdot 21 + 18 \cdot 10 \bmod 31 =$

$= 13 + 189 + 180 \bmod 31 = 382 \bmod 31 = 10 \bmod 31$

Secretul este <u>10</u>.