Tema 11

Cătălin Răreanu

1) Cifrul secret pentru utilizarea unei baze de date este partajat, folosind protocolul de divizare a secretului, între președinte și cei trei vicepreședinți, fiecare dintre ei, deținând următoarea informație: $r = 1100111011$

$v_1 = 1000100101$; $v_2 = 0011101101$; $v_3 = 1011101101$.

Determinați cifrul

r	1	1	0	0	1	1	1	0	1	1
v_1	1	0	0	0	1	0	0	1	0	1
v_2	0	0	1	1	1	0	1	1	0	1
v_3	1	0	1	1	1	0	1	1	0	1
c	1	1	1	0	1	1	1	1	1	0

2) Profesorul de la disciplina Criptografie comunică cu voi și secretariatul nota de la disciplina Criptografie folosind protocolul Shamir de secret splitting cu $n = 6$ și pragul $m = 3$. El alege corpul Z_{31} și comunică umbrele $(1, 13)$, $(30, 9)$, $(2, 18)$, $(29, 4)$, $(3, 25)$, $(28, 13)$. Determinați secretul.

$m=3 \Rightarrow$ F este de grad 2

$F(x) = ax^2 + bx + M$ pt $1, 30, 2$

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

$$l_1 = \frac{(x-30)(x-2)}{30-2} = \frac{x^2-32x+60}{28} = 10(x^2-32x+60$$

$31 = 1 \cdot 28 + 3 \Rightarrow x_3 = x_{31} - x_{28} = (1,0) - (0,1) = (1,-1)$

$28 = 3 \cdot 9 + 1 \Rightarrow x_1 = x_{28} - 9 \cdot x_3 = (0,1) - (9,-9) =$

$= (-9, 10)$

$$l_{30} = \frac{(x-1)(x-2)}{1-2} = \frac{x^2-3x+2}{-1} = -1(x^2-3x+2)$$

$$l_2 = \frac{(x-1)(x-30)}{1-30} = \frac{x^2-31x+30}{-29} = -15(x^2-31x+30$$

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

$29 = 14 \cdot 2 + 1 \Rightarrow x_1 = x_{29} - 14 \cdot x_2 = (0,1) - 14 \cdot (1,-1) =$

$= (0,1) - (14,-14) = (-14, 15)$