

Lema 11

Cătălin Răzvan

1) Cifru 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:  $\mu = 1100111011$

$\nu_1 = 1000100101$ ,  $\nu_2 = 0011101101$ ,  $\nu_3 = 1011101101$ .  
Determinați cifrul

$\mu$	1	1	0	0	1	1	1	0	1	1
$\nu_1$	1	0	0	0	0	1	0	0	1	1
$\nu_2$	0	0	1	1	1	0	1	0	0	1
$\nu_3$	1	0	1	1	1	0	1	1	0	1
$c$	1	1	0	0	0	1	1	1	1	0

2) Profesorul de la disciplina Criptografie comun cu reș și secretariatul nota de la disciplina Criptografie folosind protocolul Shamir de reș și splitting cu  $n=6$  și pragul  $m=3$ . El alege corpul  $\mathbb{Z}_{31}$  și comunică următoarele  $(1, 13), (3, 9), (2, 18), (29, 4), (3, 25), (28, 3)$ . Determinați secretul

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

$$F(x) = ax^2 + bx + m \quad \text{pt } 1, 30, 2$$

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

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

$$31 = 1 \cdot 28 + 3 \Rightarrow X_3 = X_{31} - X_{28} = (1, 0) - (0, 1) = (1, -1)$$

$$28 = 3 \cdot 9 + 1 \Rightarrow X_1 = X_{28} - 9 \cdot X_3 = (0, 1) - (9, -9) = (-9, 10)$$

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

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

$$31 = 1 \cdot 29 + 2 \Rightarrow X_2 = X_{31} - X_{29} = (1, 0) - (0, 1) = (1, -1)$$

$$29 = 14 \cdot 2 + 1 \Rightarrow X_1 = X_{29} - 14 \cdot X_2 = (0, 1) - 14 \cdot (1, -1) = (-14, 15)$$