1. Cifrul secret pentru utilizarea unei baze de date este partajat, folosind protocolul de divizarea a secretului, între președinte și cei trei vicepreședinti, fiecare dintre ei, deținând următoarea informație: p = 1100111011, v1 = 1000100101, v2 = 0011101101 și v3 = 1011101101. Determinați cifrul.

① $p = 1100111011$
$v_1 = 1000100101$
$v_2 = 0011101101$
$v_3 = 1011101101$

la fel → 0
dif → 1

p	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

1. 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 Z31 și comunică urmele (1, 13), (30, 9), (2, 18), (29, 4), (3, 25), (28, 13). Determinați secretul.

① Shamir, $n=6$, $m=3$, corpul $\mathbb{Z}_{31}$, $(1,13)$, $(30,9)$, $(2,18)$, $(29,4)$, $(3,25)$, $(28,13)$ => secretul?

Având în vedere că $m=3$ => F de grad 2
$F(x) = ax^2 + bx + M$ pt $1, 30, 2$
$f(1)=13$, $f(30)=9$, $f(2)=18$

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

$31 = 1 \cdot 28 + 3 \Rightarrow x_3 = x_{31} - x_{28} = (1,0) - (0,1) = (1,-1)$
$28 = 3 \cdot 9 + 1 \Rightarrow x_1 = x_{28} - 9 \cdot x_3 = (0,1) - (9,-9) =$
$= (-9, 10)$

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

$$p_2 = \frac{(x-1)(x-30)}{1-30} = \frac{x^2-31x+30}{-29}$$

$$29.1 \equiv$$