Criptografie-Tema11

guzurazvan

May 2024

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.

Cifrul c = p $\oplus v_1 \oplus v_2 \oplus v_3$
$p = 1100111011$
$v_1 = 1000100101$
$p \oplus v_1 = 0100011110$
$v_2 = 0011101101$
$p \oplus v_1 \oplus v_2 = 0111110011$
$v_3 = 1011101101$
$p \oplus v_1 \oplus v_2 \oplus v_3 = 1100011110$
$\Rightarrow c = 1100011110$

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.

m = 3 $\Rightarrow$Functia este de gradul 2.
$F_1(x) = ax^2 + bx + M$
$F_1(1) = 13 \Rightarrow a + b + M = 13$
$F_1(30) = 9 \Rightarrow 900a + 30b + M = 9 \Rightarrow 899a + a + 30b + M = 9 \Rightarrow a + 30b + M = 9$
$\Rightarrow a - b + M = 9$
$F_1(2) = 18 \Rightarrow 4a + 2b + M = 18$

Avem :
$a + b + M = 13$
$a - b + M = 9$
$4a + 2b + M = 18$
$\Rightarrow 2b = 4 \Rightarrow b = 2 \Rightarrow$

$a + 2 + M = 13$
$b = 2$
$4a + 4 + M = 18 \Rightarrow$

$a + M = 11$
$b = 2$
$4a + M = 14 \Rightarrow$

$a + M = 11$
$b = 2$
$3a = 3 \Rightarrow$

$a = 1$
$b = 2$
$M = 10$
$\Rightarrow F_1(x) = x^2 + 2x + 10$

$F_2(x) = ax^2 + bx + M$
$F_2(29) = 4 \Rightarrow 841a + 29b + M = 4 \Rightarrow 4a - 2b + M = 4$
$F_2(3) = 25 \Rightarrow 9a + 3b + M = 25$
$F_2(28) = 13 \Rightarrow 784a + 28b + M = 13 \Rightarrow 9a - 3b + M = 13$

Avem :
$4a - 2b + M = 4$
$9a + 3b + M = 25$
$9a - 3b + M = 13 \Rightarrow$

$4a - 4 + M = 4$
$9a + 6 + M = 25$
$b = 2 \Rightarrow$

$4a + M = 8$
$9a + M = 19$
$b = 2 \Rightarrow$

$a = 11/5$

$M = -4/5$

$b = 2$
$\Rightarrow F_2(x) = \frac{11}{5}x^2 + 2x - \frac{4}{5}$

$\mathrm{M}_1 = 10$
$M_2 = -\frac{4}{5}$
Nota = 10 - 4/5 = 9.20.