Tema 11. Criptografie

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

1. Profesorul de la disciplina criptografie comunică cu voi și secretariatul nata de la disciplina criptografie folosind protocolul Shamir de secret splitting cu $n = 6$ și pragul $m = 3$. El alege corpul 231 și comunică unele (1, 13), (30, 9), (2, 18), (23, 4), (3, 25), (28, 13). Determinați secretul.

---

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

XOR
$0 \oplus 0 = 0$
$1 \oplus 1 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$

$p \oplus v_1$:
$$\begin{array}{r} 1100111011 \\ 1000100101 \\ \hline 0100011110 \end{array}$$

$(0100011110) \oplus v_2$:
$$\begin{array}{r} 0100011110 \\ 0011101101 \\ \hline 0111110011 \end{array}$$

$(0111110011) \oplus v_3$:
$$\begin{array}{r} 0111110011 \\ 1011101101 \\ \hline 1100011110 \end{array}$$

cifrul = 1100011110

Scanat cu CamScanner