Tema 11

1. Cifrul secret pt utilizarea unei bare de date este protejat, folosind protocolul de divizare a secretului. Se define trei informații

$p = 11001110 11$

$v_1 = 1000100101$

$v_2 = 0011101101$

$v_3 = 1011101101$

Det cifrul

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

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

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

cifrul este: 1100011110

2. Profesorul de la disciplina criptografie comunică cu voi și secretariatul notă de la disciplina criptografie folosind protocolul Shamir de secret splitting cu $n = 6$ și pragul $m = 3$. El alege corul z_{31} și comunică urmele (1,13) (30,9) (2,18) (29,4) (3,25) (28,13).

Determinați secretul.

prag = 3 => determinăm un poligon de forme $m-1=2$

$F(x)=ax^2+bx+M$ pt 1, 2, 3

$f(1)=13$
$f(2)=18$
$f(3)=25$

$$\Rightarrow \begin{cases} a+b+M=13 \,/\cdot 2 \Rightarrow 2a+2b+2M=26 \\ 4a+2b+M=18 \\ 9a+3b+M=25 \end{cases}$$

$$\begin{cases} 2a+2b+2M=26 \\ 4a+2b+M=18 \end{cases} \ (-)$$

$-2a+M=8 \Rightarrow M=8+2a$

$9a+3b+8+2a=25$ $\qquad 4a+2b+8+2a=18 \Rightarrow 6a+2b=10$

$$\begin{cases} 11a+3b=17 \,/\cdot 2 \\ 6a+2b=10 \,/\cdot 3 \end{cases} \Rightarrow \begin{cases} 22a+6b=34 \\ 18a+6b=30 \end{cases} \ (-)$$

$4a=4 \Rightarrow a=1$

$M=8+2=10 \Rightarrow \boxed{M=10}$ este secretul.