

Tema 11

1. $p = 1100111011$

$v_1 = 1000100101$

$v_2 = 0011101101$

$v_3 = 1011101101$

cifru secret = ?

$v_4 = p \oplus v_1 \oplus v_2 \oplus v_3$

1. $D_1 = p \oplus v_1$

$$\begin{array}{r} 1100111011 \\ 1000100101 \\ \hline 0100011110 \end{array}$$

2. $D_2 = D_1 \oplus v_2$

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

3. $D_3 = D_2 \oplus v_3$

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

cifru secret $\{v_4\} = D_3 = 1100011110$