Seminar 11 - Criptografie

Temă

1. $p = 1100 . 1110 . 11 := S_1$

$V_1 = 1000 . 1001 . 01 := S_2$

$V_2 = 0011 . 1011 . 01 := S_3$

$V_3 = 1011 . 1011 . 01 := S_4$

$M = ?$

~~$S_2 = S_1 \oplus V_1$~~

$S_1 = p = R_1$

$S_2 = R_1 \oplus R_2$

$S_3 = R_2 \oplus R_3$

$S_4 = R_3 \oplus M$

$S_1 \oplus S_2 = R_1 \oplus (R_1 \oplus R_2) =$

$= (R_1 \oplus R_1) \oplus R_2 = 0 \oplus R_2$

$= R_2$

$S_1 \oplus S_2 \oplus S_3 = R_2 \oplus (R_2 \oplus R_3) = (R_2 \oplus R_2) \oplus R_3$

$= 0 \oplus R_3 = R_3$

$$S_1 \oplus S_2 \oplus S_3 \oplus S_4 = R_3 \oplus (R_3 \oplus M) = M$$

$\oplus$	
S_1	1100 . 1110 . 11
S_2	1000 . 1001 . 01
S_3	0011 . 1011 . 01
S_4	1011 . 1011 . 01
M	1100 . 0111 . 10

$\Rightarrow$ $M = 1100 . 0111 . 10$