TEMA 11

protocol Shamir de secret splitting

$n = 6$

prag $m = 3$

$\mathbb{Z}_{31}$; (1,13) (30,9) (2,18) (29,4) (3,25), (28,13)

secretul?

prag = 3 $\Rightarrow$ alet. un pol. F de gr. $m-1=2$

$F(X) = aX^2 + bX + M$

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

$\Rightarrow$

$a + b + M = 13 \mid \cdot 2$
$4a + 2b + M = 18$
$9a + 3b + M = 25$

$\Rightarrow 4a + 2b + 8$

$6a + 2b = 10$

$2a + 2b + 2M = 26$
$4a + 2b + M = 18$

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

$5a + b = 7$
$5a + 13 - a - M = 7$
$4a - M = -6$

$9a + 3b + 8 + 2a = 25$
$11a + 3b = 17 \mid \cdot 2 \Rightarrow 22a + 6b = 34$
$6a + 2b = 10 \mid \cdot 3 \Rightarrow 18a + 6b = 30$

$4a = 4 \Rightarrow a = 1$

$M = 10$ | secretul este 10