UNIVERSITATEA DIN BUCUREȘTI
FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ
DEPARTAMENTUL DE INFORMATICĂ
SERIA 33 – GRUPELE 331/332

EXAMEN LA DISCIPLINA "CRIPTOGRAFIE ȘI SECURITATE"

- Sesiunea mai/iunie 2017 –

1. Cifrul Vigenère. (1 punct)

2. Folosind cifrul Playfair, criptați-vă primul prenume utilizând numele ca parolă. (1 punct)

3. Definiți noțiunile de confuzie și difuzie. (1 punct)

4. Cifrul Vernam. (1 punct)

5. Calculați o cheie pentru un sistem de criptare RSA cu $n = 77$. (1 punct)

6. Considerăm schema de criptare ElGamal pentru curbe eliptice, în care:

- p – număr prim mare
- E – curbă eliptică peste $\mathbb{Z}_p$
- A – un punct de ordin mare al curbei eliptice E
- n – un număr aleator din $\mathbb{Z}_p^*$
- $B = nA$
- $K_{priv} = \{n\}$
- $K_{pub} = \{p, E, A, B\}$

a) Scrieți funcțiile de criptare și decriptare corespunzătoare. (1 punct)
b) Demonstrați corectitudinea funcției de decriptare. (1 punct)
c) Fie curba eliptică $E: y^2 \equiv x^3 + x + 5 (\mathrm{mod}\ 19)$ peste $\mathbb{Z}_{19}$, având 15 puncte:

$\mathcal{O}, A_1(0,9), A_2(0,10), A_3(1,8), A_4(1,11), A_5(3,4), A_6(3,15), A_7(4,4), A_8(4,15), A_9(11,6),$
$A_{10}(11,13), A_{11}(12,4), A_{12}(12,15), A_{13}(13,7), A_{14}(13,12)$

Punctul $A_1(0,9)$ este un generator al grupului asociat curbei eliptice, deoarece:

$\mathcal{O} = 15A_1, A_2 = 14A_1, A_3 = 13A_1, A_4 = 2A_1, A_5 = 3A_1, A_6 = 12A_1, A_7 = 4A_1, A_8 = 11A_1,$
$A_9 = 6A_1, A_{10} = 9A_1, A_{11} = 8A_1, A_{12} = 7A_1, A_{13} = 10A_1, A_{14} = 5A_1$

Pentru $A = A_5$ și $n = 7$ criptați mesajul $M = A_{13}$ și decriptați mesajul $M' = (A_{10}, A_6)$. (2 puncte)

Notă:
Se acordă 1 punct din oficiu.

SUCCES!