UNIVERSITATEA DIN BUCUREȘTI
FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ
DEPARTAMENTUL DE INFORMATICĂ
SERIA 33 – GRUPELE 333/334

EXAMEN LA DISCIPLINA "CRIPTOGRAFIE ȘI SECURITATE"

- Sesiunea mai/iunie 2017 –

1. Cifrul Vigenère. (1 punct)
2. Folosind cifrul Playfair, criptați-vă numele folosind primul prenume ca parolă. (1 punct)
3. Definiți noțiunea de securitate perfectă. (1 punct)
4. Cifrul Vernam. (1 punct)
5. Calculați o cheie pentru un sistem de criptare RSA cu $n = 65$. (1 punct)
6. Considerăm schema de criptare ElGamal, în care:
   - p – număr prim mare
   - g – generator pentru $\mathbb{Z}_p$
   - x – un număr din $\mathbb{Z}_p^*$
   - $y \equiv g^x (\mathrm{mod}\, p)$
   - $K_{priv} = \{x\}$
   - $K_{pub} = \{p, g, y\}$

   a) Scrieți funcțiile de criptare și decriptare corespunzătoare. (1 punct)
   b) Demonstrați corectitudinea funcției de decriptare. (1 punct)
   c) Pentru $p = 11, g = 7$ și $x = 5$ criptați mesajul $M = 3$ și decriptați mesajul $M' = (2,2)$. (2 puncte)

Notă:
Se acordă 1 punct din oficiu.

SUCCES!