Masterand:_____
Grupa:_____
Data predării temei:

TEMA[1] 1

1. Să se cifreze textul reprezentat de numele dumneavoastră de familie, prin algoritmul Cezar. Cheia utilizata este numărul de litere din numele de familie. Verificați rezultatul prin descifrare.

2. Să se cifreze textul reprezentat de numele dumneavoastră de familie, prin metoda substituției. Cheia utilizată este prenumele dumneavoastra. Verificați rezultatul prin descifrare.

3. Să se cifreze textul reprezentat de numele dumneavoastra de familie, prin metoda Playfair. Cheia utilizată este prenumele dumneavoastră. Verificați rezultatul prin descifrare.

4. Să se cifreze textul reprezentat de numele dumneavoastră de familie, cu ajutorul algoritmului Hill 2 x 2. Cheia utilizata este reprezentată de o matrice aleasa de dumneavoastra. Verificați rezultatul prin descifrare.

5. Să se cifreze textul reprezentat de numele dumneavoastră de familie, prin metoda transpoziției. Cheia utilizată în generarea permutării este data de numele şi prenumele dumneavoastră. Verificați rezultatul prin descifrare.

6. Să se cifreze textul reprezentat de prenumele dumeavoastră, cu ajutorul algoritmului Vigenere. Cheia utilizată este data de numele dumneavoastră de familie. Verificați rezultatul prin descifrare.

7. Prenumele dumneavoastră se converteşte în format ASCII şi devine intrare în algoritmul RIJNDAEL 128/128. Numele de familie se va converti similar numai că devine intrare în algoritmul de generare a subcheilor de rundă. Care este ieşirea din rutinele: SubBytes, ShiftRows, MixColumn si AddRoundKey, la iterația 5?

[1] Fiecare exercițiu va fi rezolvat după metoda pen&paper şi verificat prin intermediul aplicațiilor software dezvoltate de către dumneavoastră şi/sau disponibile pe www.

TEMA[2] 2

1. Fie a_1 numărul de litere din numele de familie şi a_2 numărul de litere din prenumele de familie.
Utilizand lema chinezească a resturilor (CRT) să se rezolve sistemul de ecuaţii:
$x=a_1 \bmod 17$,
$x=a_2 \bmod 19$,
$x= \max(a_1,a_2) \bmod 37$.

2. Fie p primul număr prim după numărul de litere din numele de familie şi *q* următorul număr prim. Să se cifreze mesajul $M=4$ cu ajutorul algoritmului RSA specificat de $n=pq$, exponentul de cifrare $e=3$. Verificaţi rezultatul prin descifrare.

3. O aplicaţie la metoda de cifrare ElGamal, similară exerciţiului rezolvat din TEMA 1. Mesajul ce urmeaza a fi cifrat fiind reprezentat de numărul de litere din numele de familie. Verificaţi rezultatul prin descifrare.

[2] Fiecare exerciţiu va fi rezolvat după metoda pen&paper şi verificat prin intermediul aplicaţiilor software dezvoltate de către dumneavoastră şi/sau disponibile pe www.