Vježba 1. ***SIMETRIČNI KRIPTOSUSTAVI***

Zadatak 1. *DES (Data Encryption Standard)*

- U aplikaciji *CrypTool* realizirati sustav za šifriranje i dešifriranje pomoću DES kriptosustava.
- Šifrirati svoje ime i prezime (npr. „PETARPETROVIC“), uz proizvoljno izabrani ključ
- Ucrtati kreirani sustav, zajedno sa pripadajućim ulazom i izlazom:

- Pomoću DES kriptosustava šifrirati sljedeće pojmove, uz proizvoljno izabrani ključ (ključ i šifrat upisati u heksadekadskom obliku):
  - SIGURNOSTRACUNALNIHSUSTAVA (ključ: _____)

    _____
  - KLASICNAKRIPTOGRAFIJA (ključ: _____)

    _____
  - ELEKTROTEHNICKIFAKULTET (ključ: _____)

    _____

- Dešifrirati sljedeće šifrate, ako se zna da su šifrirani pomoću DES kriptosustava, uz ključ 0x1234567890ABCDEF:
    - 8F 9A 68 A2 E8 E2 C3 7D 83 5A C7 E0 57 24 FC AE B0 F6 BC 5F 65 39 1C 3B:

      _____
    - 10 50 39 C6 0A 9A 10 33 BC CB B1 04 7E B7 71 0E:

      _____
    - F6 25 0B C0 6F 42 81 0A 90 C1 B1 A6 48 F9 27 8A:

      _____
    - E1 43 55 2A 91 F9 34 9E 48 7A B5 65 F7 7A D1 B1 BE 70 3F D6 97 D8 03 6E:

      _____

- Objasnite sličnosti i razlike u pojedinim modusima rada DES kriptosustava:

Zadatak 2. *AES (Advanced Encryption Standard)*

- U aplikaciji *CrypTool* realizirati sustav za šifriranje i dešifriranje pomoću AES-128 kriptosustava.
- Šifrirati svoje ime i prezime (npr. „PETARPETROVIC“), uz proizvoljno izabrani ključ
- Ucrtati kreirani sustav, zajedno sa pripadajućim ulazom i izlazom:

- Pomoću AES-128 kriptosustava šifrirati sljedeće pojmove, uz proizvoljno izabrani ključ (ključ i šifrat upisati u heksadekadskom obliku):
    - NAPREDNOSIFRIRANJE (ključ: _____)

      _____
    - TEKSTZAENKRIPCIJU (ključ: _____)

      _____
    - SVEUCILISTEUOSIJEKU (ključ: _____)

      _____

- Dešifrirati sljedeće šifrate, ako se zna da su šifrirani pomoću AES-128 kriptosustava, uz ključ 0x11223344556677889900AABBCCDDEEFF:

    - 8D 19 3D 2F 35 1A C0 9E 5D E3 88 95 73 27 83 E2 01 34 42 06 47 34 AF 0B C4 6D 1E 58 42 1E 6E 89:

      _____

    - 96 61 11 EA 62 3A B8 41 99 EE 20 76 EA B2 F1 2E 60 A6 10 F8 C1 9E 8A 7A D1 6F EC F6 21 F1 02 9C:

      _____

    - D0 13 03 EB B4 69 F6 7E 8D 0F 50 ED 48 0B 81 37 91 2C 55 13 9E 84 48 BC 86 A0 B1 66 76 F5 77 5D:

      _____

    - 7E C4 F1 A1 E7 65 E2 02 83 EC 1B 0D 5F E4 5B D0 FD 53 E4 34 6F 15 D2 2C 97 97 AC 84 36 4C C8 78:

      _____

- Objasnite sličnosti i razlike između DES i AES kriptosustava:

ZAKLJUČAK

Popunjava student	***Popunjava nastavnik***	
Ime i prezime:	Datum pregleda:	Potpis: