# Criptografie și securitate CTI

## Laborator 7

**Sisteme de cifrare bloc. Advanced Encryption Standard (AES)**

1. (a) Care este structura generică a unui cifru de tip Substitution Permutation Network (SPN)?

   (b) Cum considerați din punct de vedere al eficienței implementarea structurilor de tip SPN în hardware, respectiv în software? Argumentați.

   Link suplimentar `https://en.wikipedia.org/wiki/Substitution-permutation_network`

2. Vizualizați în Cryptool 2 modul de funcționare al sistemului de cifrare bloc AES sau la link-ul `https://www.youtube.com/watch?v=Z_7aOkS8tOA`. Folosind Cryptool 2 sau un tool online

   (a) Cifraţi mesajul **Substitution Permutation Network**, folosind cheia de cifrare pe 128 biți **AB CD EF 01 23 45 67 89 AB CD EF 01 23 45 67 89**.

   (b) Descifraţi mesajul **A4 97 8C 1E A6 38 AD A4 1A 6A 11 79 C1 F0 CD DD E1 D5 1B 09 4F AF C2 C9 47 B6 25 FA 9D 7A 62 4C**, folosind cheia de cifrare anterioară, modul de lucru ECB și modalitatea de padding cu zerouri.

3. Se consideră următoarea intrare în runda finală de AES:

$$\begin{pmatrix} 04 & 07 & E2 & 49 \\ F2 & 78 & 2F & C5 \\ CA & 28 & 01 & D7 \\ 97 & 45 & 96 & 10 \end{pmatrix}$$

   și cheia de rundă

$$\begin{pmatrix} 21 & 35 & AC & 6C \\ 75 & 50 & AF & 1B \\ 17 & 62 & 6B & F0 \\ 87 & 0B & 3C & 9B \end{pmatrix}.$$

   Care este ciphertext-ul?

4. (a) Un inginer software vrea să implementeze cifrul AES în modul de lucru ECB. Știind că aplicația pe care dorește să o realizeze va fi utilizată doar pentru cifrare de date cu caracter aleator (de exemplu, chei de cifrare), poate fi considerată aceasta sigură?

(b) Un inginer software vrea să implementeze cifrul AES în modul de lucru CBC. Pentru simplitate, acesta decide să utilizeze vectorul de inițializare 0. Există vulnerabilităţi ale sistemului respectiv (independent de input)?

5. Proprietatea de difuzie

   (a) Alegeţi atât un text clar cât și o cheie oarecare (dar nu trivială). Cifraţi textul în mod ECB cu ajutorul cheii alese şi păstraţi textul cifrat obţinut.

   (b) Modificaţi un singur bit din cheia de cifrare. Cifraţi din nou textul, utilizând această nouă cheie. Ce observaţi?