Laborator 3 Criptografie si securitate

1. Data Encryption Standard (DES)

   (a) Cifraţi mesajul **HORST FEISTEL**, folosind cheia de cifrare **AB CD EF 01 23 45 67 89**. Uţilizaţi atât modul ECB cât şi CBC.

   (b) Descifraţi mesajul **C6 C4 EB DC 90 D3 42 F5 48 FD 7E C5 15 9A 87 4F 1A FF A2 13 A5 9B E7 F7 49 5E F4 44 39 DB 63 61**, folosind cheia anterioară. În ce mod de lucru a fost realizată criptare?

   (c) Se consideră următoarele chei:

   1F E0 1F E0 0E F1 0E F1
   E0 1F E0 1F F1 0E F1 0E
   FE E0 FE E0 FE F1 FE F1
   1F 1F 1F 1F 0E 0E 0E 0E

   Care dintre acestea este o cheie slabă ($e_k(e_k(m)) = m$ pentru orice mesaj m? Puteţi găsi o pereche de chei semi-slabe ((k_1, k_2) astfel încât $e_{k_1}(e_{k2}(m)) = m$ pentru orice m mesaj?

   (d) Se dă textul clar:

   ATTACK

   şi textul cifrat corespunzător:

   85 41 46 B5 0D 89 AF 7A

   Ştiind că textul clar a fost criptat cu dublu DES în modul de lucru ECB şi ambele chei sunt de forma:

   X0 00 00 00 00 00 00 00 determinaţi cele 2 chei.

2. Advanced Encryption Standard

   (a) Folosind cheia de criptare de 128 de biţi:

   AB 89 CD 01 EF 23 AB 45 CD 01 AB 23 CD 45 EF 67

   criptaţi mesajul:

   Advanced Encryption Standard

(b) Folosind cheia de la punctul anterior şi padding mode $1-0$ decriptaţi mesajul:

14 5F 5D 4C F4 B9 20 0F 7E BD 56 53 19 96 9A 1B 5A 08 75 29 08 18 4E 79 13 7C B7 F6 12 9A 93 D4

(c) Se consideră următoarea intrare într-o rundă AES:

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

şi 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 ieşirea din rundă?