Criptografie și securitate CTI

Laborator 6

Funcţii PPT neglijabile

1. Care dintre următoarele funcţii este PPT neglijabilă în n?

$$f(n) = \frac{1}{5};$$
$$f(n) = \frac{1}{2^{90}};$$
$$f(n) = \frac{1}{n^{80} + 3n + 1};$$
$$f(n) = \frac{1}{3^n};$$
$$f(n) = \frac{p(n)}{2^n}, \qquad p(n) \text{ fiind o funcție polinomială;}$$
$$f(n) = f_1(n) + \frac{1}{2}, \qquad f_1 \text{ funcție neglijabilă.}$$

Sisteme de cifrare bloc. Moduri de operare. Data Encryption Standard (DES)

2. Vizualizați modul de funcționare al sistemului de cifrare bloc DES folosind clipul `https://www.youtube.com/watch?v=Y61qn_SQl40` şi accesaţi pagina `https://ro.wikipedia.org/wiki/Data_Encryption_Standard`. Folosind un tool online:

   (a) Cifraţi mesajul **HORSTFEISTEL**, folosind cheia de cifrare **AB CD EF 01 23 45 67 89**. Utilizaţi atât modul de operare Electronic Codebook (ECB), cât și (CBC). Ce observați?

   (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 de cifrare anterioară. În ce mod de lucru (ECB sau CBC) a fost realizată cifrarea?

   Link suplimentar: `https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation`

3. Rezistenţa la erorile de transmisie – modurile de operare ECB, CBC și CTR:

   (a) Alegeţi atât un text clar cât și o cheie oarecare (dar nu trivială). Criptaţi textul clar în modul ECB. În textul cifrat obţinut modificaţi un singur bit și descifraţi textul astfel modificat.

(b) Criptaţi textul clar ales anterior în modul CBC. În textul cifrat obţinut modificaţi un singur bit și descifraţi textul astfel modificat.

(c) Criptaţi textul clar ales anterior în modul CTR. În textul cifrat obţinut modificaţi un singur bit și descifraţi textul astfel modificat.

Ce observaţi?

4. Chei slabe şi perechi de chei semi-slabe

Se consideră următoarele chei:

01 01 01 01 01 01 01 01
01 E0 01 E0 01 F1 01 F1
10 10 10 10 10 10 10 10
E0 01 E0 01 F1 01 F1 01

(a) O cheie k este considerată *slabă* dacă este satisfăcută proprietatea $e_k(e_k(m)) = m$, pentru orice mesaj m. Care din cheile de mai sus este o cheie slabă?

(b) O pereche de chei (k_1, k_2) este considerată *semi-slabă* dacă este satisfăcută proprietatea $e_{k_1}(e_{k_2}(m)) = m$, pentru orice mesaj m. Care din perechile de chei de mai sus poate fi considerata semi-slabă?

5. Meet-In-The-Middle Attack (MitM)

`https://en.wikipedia.org/wiki/Meet-in-the-middle_attack`

Se dă textul clar **des**. Se ştie că acesta a fost supus unei operații de dublă cifrare cu DES în mod ECB, folosind două chei de forma **X0 00 00 00 00 00 00 00**, unde **X** poate fi orice cifra hexazecimală. În urma acestei operații s-a obţinut textul cifrat **B1 24 5E 56 79 75 51 A2**.

Folosind un atac de tip MitM determinaţi cele 2 chei.