Noţiuni de securiate

1. Se consideră varianta criptării în modul de operare CBC în care emiţătorul incrementează IV cu 1 de fiecare dată când criptează un mesaj (în loc să aleagă IV aleator). Arătaţi că schema nu este CPA-sigură.

2. Fie (Enc, Dec) un sistem de criptare simetric. Se consideră sistemul de criptare (Enc', Dec') pentru mesaje de dimensiune dublă cu funcţia de criptare definită astfel:

$$Enc'_k(m_1||m_2) = (Enc_k(m_1), Enc_k(m_2))$$

   Arătaţi că sistemul nu este CCA-sigur.

3. Arătaţi că modul CBC nu este CCA-sigur.

Message Authentication Code (MAC)

4. Fie (Mac, Vrfy) un MAC sigur definit peste (K,M,T) unde $M = \{0,1\}^n$ şi $T = \{0,1\}^{128}$. Este MAC-ul de mai jos sigur? Argumentaţi răspunsul.

$$Mac'(k,m) = Mac(k,m)$$
$$Vrfy'(k,m,t) = \begin{cases} Vrfy(k,m,t), & \text{dacă } m \neq 0^n \\ 1, & \text{altfel} \end{cases}$$

5. Fie F PRF. Se defineşte MAC pentru mesajele de lungime $2n-2$ astfel: pentru intrarea $m_0||m_1$ ($|m_0| = |m_1| = n-1$) şi $k \in \{0,1\}^n$, $t = F_k(0||m_0)||F_k(1||m_1)$. Funcţia de verificare a validităţii este definită în mod natural. Este MAC astfel definit sigur?

6. Arătaţi că CBC-MAC nu este sigur dacă se foloseşte pentru autentificarea mesajelor de lungimi diferite.

Funcţii hash

7. Se consideră $Enc_k(m)$ un sistem de criptare bloc sigur. Se defineşte o funcţie hash H astfel:

   i. m se concatenează cu 0-uri până la un multiplu de lungimea blocului;

   ii. Se sparge secvenţa obţinută anterior în n blocuri, i.e. $m_0||m_1||...||m_{n-1}$;

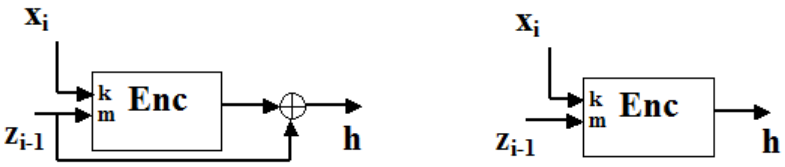
   iii. Se aplică:

```
1: c ← Enc_{m_0}(m_0)
2: for i = 1 to n-1 do
3:     d ← Enc_{m_0}(m_i)
4:     c ← c ⊕ d
5: end for
```

6: $H(m) \leftarrow c$

Este H rezistentă la coliziuni? Argumentaţi.

8. Se mai obţine h rezistentă la coliziuni dacă nu se foloseşte $\oplus$ în construcţia Davies - Meyer, i.e. se foloseşte construcţia din dreapta în locul celei din stânga?



S-box

9. Poate fi un S-box ales aleator? Consideraţi un S-box aleator, inversabil, cu 4 biţi la intrare, 4 biţi la ieşire şi analizaţi posibilitatea de apariţie a efectului de avalanşă.