Noțiuni de securitate

- 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 funcția de criptare definită astfel:

$$Enc'_{k}(m_{1}||m_{2}) = (Enc_{k}(m_{1}), Enc_{k}(m_{2}))$$

Arătați că sistemul nu este CCA-sigur.

3. Arătați 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.

$$\begin{aligned} Mac'(k,m) &= Mac(k,m) \\ Vrfy'(k,m,t) &= \left\{ \begin{array}{ll} Vrfy(k,m,t), & \text{dacă } m \neq 0^n \\ 1, & \text{altfel} \end{array} \right. \end{aligned}$$

- 5. Fie F PRF. Se definește MAC pentru mesajele de lungime 2n-2 astfel: pentru intrarea $m_0||m_1||(m_0|=|m_1|=n-1)$ și $k\in\{0,1\}^n$, $t=F_k(0||m_0)||F_k(1||m_1)$. Funcția de verificare a validității este definită în mod natural. Este MAC astfel definit sigur?
- 6. Arătați că CBC-MAC nu este sigur dacă se folosește pentru autentificarea mesajelor de lungimi diferite.

Funcții hash

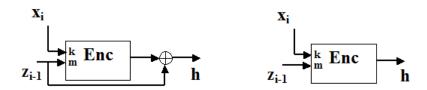
- 7. Se consideră $Enc_k(m)$ un sistem de criptare bloc sigur. Se defineşte o funcție hash H astfel:
 - i. m se concatenează cu 0-uri până la un multiplu de lungimea blocului;
 - ii. Se sparge secvența obținută anterior în n blocuri, i.e. $m_0||m_1||...||m_{n-1}$;
 - iii. Se aplică:
 - 1: $c \leftarrow Enc_{m_0}(m_0)$ 2: **for** i = 1 **to** n-1 **do** 3: $d \leftarrow Enc_{m_0}(m_i)$ 4: $c \leftarrow c \oplus d$

5: end for

6:
$$H(m) \leftarrow c$$

Este H rezistentă la coliziuni? Argumentați.

8. Se mai obține h rezistentă la coliziuni dacă nu se folosește \oplus în construcția Davies - Meyer, i.e. se folosește construcția din dreapta în locul celei din stânga?



S-box

9. Poate fi un S-box ales aleator? Considerați un S-box aleator, inversabil, cu 4 biți la intrare, 4 biți la ieșire și analizați posibilitatea de apariție a efectului de avalanșă.