Moduri de operare

1. Scrieţi formulele de decriptare pentru modurile de operare ECB, CBC, OBF, CTR. Care pot fi paralelizate?

2. O tranzacţie bancară foloseşte modul de operare ECB cu structura indicată mai jos, unde Banca A, respectiv Contul CA indică proveniența banilor, iar Banca B, respectiv contul CB indică destinaţia banilor care se transferă. Ce strategie poate să adopte Oscar pentru a transmite banii în contul personal?

1	2	3	4	5
Banca A	Contul CA	Banca B	Contul CB	Suma transferată (EUR)

3. 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.

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

S-box

5. Poate fi un S-box ales aleator? Consideraţi un S-box aleator cu 4 biţi la intrare şi calculaţi posibilitatea de apariţie a efectului de avalanşă.

6. Consideraţi DES care utilizează S-box-uri liniare. Atunci întreg sistemul de criptare poate fi considerat liniar, i.e. $DES_k(m) = A \cdot (m, k)^T = c$, unde A este matricea care defineşte sistemul. Indicaţi o vulnerabilitate.

DES. AES

7. Un program de criptare foloseşte DES cu chei pe 56 de biţi. Cheia este generată pe baza unei parole de 8 caractere codate ASCII extended (coduri posibile: 0-255): $8 \cdot 8 = 64$ biţi, dintre care 8 nu se iau în calcul, conform criptării obişnuite DES (mai exact, lsb din fiecare caracter este ignorat). Se presupune că un calculator obişnuit poate să testeze 10^6 chei pe secundă.

   (a) Care este spaţiul cheilor dacă toate caracterele sunt alese aleator? Cât timp necesită o căutare exhaustivă?

   (b) Care este spaţiul cheilor dacă se consideră doar caracterele ASCII obişnuite (coduri posibile: 0-127)? Cât timp necesită o căutare exhaustivă?

   (c) Care este spaţiul cheilor dacă parola foloseşte numai litere mari? Cât timp necesită o căutare exhaustivă?

8. Se consideră intrarea într-o rundă AES:

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

şi cheia de rundă

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

Care este ieşirea din rundă?

MAC

9. 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 CPA-sigur?

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

Funcţii Hash. Construcţia Davies-Meyer

11. 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?