Kapitulli 3

Blok shifruesit

Detyra për ushtrime

1. Tregoni se për çdo $K \in \{0,1\}^{56}$ dhe për pdo $x \in \{0,1\}^{64}$

$$DES_K(x) = \overline{DES_{\overline{K}}(\overline{x})}.$$

(ku $\overline{x}$ shënon komplementin bit pët bit të x). Kjo quhet *vetia e komplementimit të çelësit* e DES.

Udhëzim: Analizoni algoritmin $DES_{\overline{K}}(\overline{M})$. Meqë algoritmi për $KeySchedule(K)$ performon vetëm kundrejt pozitave të bitëve brenda K,

$$KeySchedule(\overline{K}) = \overline{KeySchedule(K)}.$$

Meqë $\overline{R} \oplus \overline{J} = R \oplus J$,

$$f(\overline{J}, \overline{R}) = f(J, R).$$

Tani, në secilin raund të algoritmit të DES

$$f(\overline{K_i}, \overline{R_{i-1}}) \oplus \overline{L_{i-1}} = f(K_i, R_{i-1}) \oplus \overline{L_{i-1}} = \overline{f(K_i, R_{i-1}) \oplus L_{i-1}}.$$

Prandaj,

$$DES_{\overline{K}}(\overline{M}) = \overline{DES_K(M)}.$$

2. Shpjegoni si të përdoret vetia e komplementimit të çelësit e DES, nga detyra paraprake, për të gjetur çelësin e targetuar me kompleksitet 2^{55}.

Udhëzim: Përdorni sulmin e mesazhit të zgjedhur me dy mesazhe të zgjedhura me kujdes.

3. Sa është numri i permutacioneve të ndryshme nga 128 bit në 128 bit (d.m.th. nga $\{0,1\}^{128}$ në $\{0,1\}^{128}$)? Sa funksione ka nga 128 bit në 128 bit?

Udhëzim: Shih Maxima skriptin `cryptography-exc-03.wxm`

4. Duke përdorur formulën e Stirling-ut

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n,$$

vlerësoni probabilitetin që një funksion i rastësishëm nga 128 bit në 128 bit (d.m.th. $f : \{0,1\}^{128} \to \{0,1\}^{128}$) është permutacion.

Udhëzim: Shih Maxima skriptin `cryptography-exc-03.wxm`

5. Gjeni një çelës K të tillë që për çdo $x \in \{0,1\}^{64}$ të vlejë $DES_K(x) = DES_K^{-1}(x)$. Një çelës i tillë quhet *çelës i dobët* i DES.

Udhëzim: Gjeni një çelës për të cilin raundet e algoritmave DES dhe DES^{-1} janë identike.

6. Në qoftë se K është një çelës i dobët i DES (shih detyrën paraprake), vërtetoni se edhe $\overline{K}$ është poashtu çelës i dobët i DES.

Udhëzim: Shih detyrën 1.

7. Cili nga algoritmat: për enkriptim apo për dekriptim është më i shpejtë për

   (a) DES;

   (b) AES?

8. Le të jetë $\mathcal{K}$ një algoritëm për gjenerim çelësi që kthen $K \xleftarrow{\$} \{0,1\}^{128}$. Le të jetë $\mathcal{E}$ algritmi vijues i enkriptimit, i mbështetur në blok shifruesin AES.

---

function $\mathcal{E}_K(M)$
  $R \xleftarrow{\$} \{0,1\}^{128}$
  $C_0 \leftarrow R$
  for $i = 1, \ldots, n$ **do**
    $W_i \leftarrow (R + i) \bmod 2^{128}$
    $C_i \leftarrow AES_K(M_i \oplus W_i)$
  end for
  $C \leftarrow C_0 \parallel C_1 \parallel \cdots \parallel C_n$
  return C
end function

Më sipër $W_i \leftarrow (R+i) \bmod 2^{128}$ ka kuptimin se R e konsiderojmë si numër të plotë, e mbledhim me i, marrim resultatin module 2^{128}, e konsiderojmë këtë si string 128 bitësh, dhe ia ndajmë për vlerë W_i. Hapësira e mesazheve janë të gjithë stringjet me gjatësi shumëfish 128 bitësh, M_i është bloku i i-të (128 bitësh) i mesazhit M dhe n është numri i bloqeve. Shkruani algoritmin $\mathcal{D}$ të dekriptimit të tillë që $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ të jetë një skemë simetrike enkriptimi. A është kjo një skemë e sigurtë?

9. Familja e funksioneve $F : \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$ është përkufizuar me

$$\begin{aligned} y_1 &\leftarrow AES_{x_1}(K_1), \\ y_2 &\leftarrow AES_{K_1}(x_2 \oplus K_2), \\ F_{K_1 \| K_2}(x_1 \parallel x_2) &\leftarrow y_1 \parallel y_2 \end{aligned}$$

për K_1, K_2, x_1, x_2 128 bitësh. Prezantoni një sulm praktik për kthim çelësi të mesazhit të njohur mbi F. Çfarë numri q çiftesh hyrje dalje dhe çfarë kompleksiteti t ka sulmi juaj? Çfarë kompleksiteti do të kishte sulmi i kërkimit të të gjithë çelësave?