Kapitulli 5

Enkriptimi simetrik

Detyra për ushtrime

1. Le të jetë $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ një skemë simetrike enkriptimi hapësira e mesazheve të së cilës është $\{0,1\}^n$. Vërtetoni se në qoftë se $\mathcal{SE}$ është IND-CPA e sigurt, atëherë $\mathcal{SE}$ është PRF e sigurt.

2. Le të jetë $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ një skemë simetrike enkriptimi hapësira e mesazheve të së cilës është $\{0,1\}^n$. Supozoni se $\mathcal{B}$ është një kundërshtar i cili kthen mesazhin (plaintext-recovery). Vërtetoni se ekziston një ind-cpa kundërshtar $\mathcal{A}$ me kompleksiteti kohor dhe numër pyetësorësh përafërsisht sikur të $\mathcal{B}$ i tillë që

$$\mathsf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A}) \geqslant \mathsf{Adv}^{\mathrm{pr-cpa}}_{\mathcal{SE}}(\mathcal{B}) - \frac{1}{2^n}.$$

3. Le të jetë $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ një skemë simetrike enkriptimi. Formalizoni nocionin e KR (key-recovery) sigurisë kundrejt kthimit të çelësit për skemat simetrike të enkriptimit. Vërtetoni se IND-CPA siguria implikon KR-sigurinë.

4. Le të jenë $\mathcal{SE}_1 = (\mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$ dhe $\mathcal{SE}_2 = (\mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$ dy skema simetrike enkriptimi për të cilat dihet se së paku njëra është IND-CPA e sigurt. Problemi është se nuk e dijnë se cila është IND-CPA e sigurt e cila mund të mos jetë. Konstruktoni një skemë simetrike enkriptimi $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ e cila është IND-CPA e sigurt përderisa njëra nga $\mathcal{SE}_1$ ose $\mathcal{SE}_2$ është IND-CPA e sigurt.

   Udhëzim: Generoni dy mesazhe nga mesazhi origjinal ashtu që njohja e cilësdo nga pjesët nuk zbulon asnjë informatë mbi mesazhin, por njohja e të dyjave jep mesazhin origjinal.

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

$\mathcal{E}_K(M)$

$R \xleftarrow{\$} \{0,1\}^{128}$
$C[0] \leftarrow R$
for $i = 1, \ldots, n$ **do**
  $W[i] \leftarrow (R + i) \bmod 2^{128}$
  $C[i] \leftarrow \mathrm{AES}_K(M[i] \oplus W[i])$
$C \leftarrow C[0] \parallel C[1] \parallel \cdots \parallel C[n]$
return C

Vërtetoni se $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ është një skemë IND-CPA e pasigurt duke dhënë një kundërshtar praktik $\mathcal{A}$ të tillë që $\mathsf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A})$ të jetë e lartë. Llogaritni vlerën e përparisë së arritur dhe numrin e orakul pyetësorëve që shfrytëzon kundërshtari.

Zgjidhje: Kundërshtari $\mathcal{A}$ shfrytëzon dobësinë e $\mathcal{E}$: blok shifruesi AES shifron bloqe të njëjta në shifra të njëjta.

Le të jetë $m \in \{0, \ldots, n\}$ numri i bitëve 1 me të cilat përfundon stringu i bitëve $W \leftarrow (R + 1) \bmod 2^{128}$. Atëherë, meqë biti i $m + 1$-të i W është 0,

$$W \bmod 2^{m+1} = W \bmod 2^m = 2^m - 1.$$

Vërejmë se

$$\begin{aligned}((R + 1) + (m + 1)) \bmod 2^m &= (2^m - 1 + m + 1) \bmod 2^m \\ &= (2^m + m) \bmod 2^m = m\end{aligned}$$

dhe

$$\begin{aligned}((R + 1) + (m + 1)) \bmod 2^{m+1} &= (2^m - 1 + m + 1) \bmod 2^{m+1} \\ &= (2^m + m) \bmod 2^{m+1} \geqslant 2^m\end{aligned}$$

që d.m.th. se biti i $m + 1$-të i $((R + 1) + (m + 1)) \bmod 2^{128}$ është 1 dhe m bitët e fundit të tij janë m. Kështu, për

$$\begin{aligned}M[1] &\leftarrow 0 \\ M[m + 2] &\leftarrow 2^m + (2^m - 1 - m) = 2^{m+1} - (m + 1) \quad (m = 0, \ldots, n)\end{aligned}$$

kemi

$$W \oplus M[1] = ((R + 1) + (m + 1)) \bmod 2^{128} \oplus M[m + 2].$$

Kundërshtari $\mathcal{A}$ bën një orakul pyetësor të gjatësisë $n+2$ bloqe 128 bitëshe me mesazhin M në botën e majtë dhe $0 \parallel 0 \parallel \cdots \parallel 0 = 0^{128(n+2)}$ në botën e djathtë. Një algoritëm me kompleksitet $\mathcal{O}(n)$ që implementon $\mathcal{A}$ është

$\mathcal{A}$

$M[1] \leftarrow 0$
$M[2] \leftarrow 1$
for $i = 2, \ldots, n$ **do**
  $M[i+2] \leftarrow 2M[i] + i - 1$
$C \leftarrow \mathrm{LR}(M, 0 \parallel 0 \parallel \cdots \parallel 0)$
$R \leftarrow C[0]$
$W \leftarrow (R+1) \bmod 2^{128}$
Parso $s \parallel 0 \parallel 1^m \leftarrow 0 \parallel W$ // $m \in \{0, \ldots, n\}$ 1-she në fund të W
if $C[1] = C[m+2]$ **then** $d \leftarrow 0$
else $d \leftarrow 1$
return d

Përparsia që arrin kundërshtari është

$$\begin{aligned}\mathsf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A}) &= \Pr\left[\mathrm{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1\right] - \Pr\left[\mathrm{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1\right] \\ &= 1 - 0 = 1.\end{aligned}$$