Problem Set 6

Due November 19th, 2019, 11:59pm

Problem 1 [50 points] Let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let

$$D \;=\; \{\, M \in \{0,1\}^* \;:\; 0 < |M| < n2^n \text{ and } |M| \bmod n = 0 \,\}\ .$$

Let $\mathcal{T}\colon \{0,1\}^k \times D \to \{0,1\}^n$ be defined as follows:

Alg $\underline{\mathcal{T}_K(M)}$
$M[1]\ldots M[m] \leftarrow M$; $M[m+1] \leftarrow \langle m\rangle$; $C[0] \leftarrow 0^n$
For $i = 1,\ldots,m+1$ do $C[i] \leftarrow E_K(C[i-1] \oplus M[i])$
$T \leftarrow C[m+1]$; Return T

Above, $M[1]\ldots M[m] \leftarrow M$ means we break M into n-bit blocks, and $\langle m\rangle$ indicates the binary representation of m.

Show that $\mathcal{T}$ is an insecure message-authentication code by presenting a $\mathcal{O}(n)$-time adversary A making at most 2 queries to its **Tag** oracle and achieving $\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{T}}(A) = 1$.

Problem 2 [50 points] Let $\mathcal{SE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ be any symmetric encryption scheme for which $\mathcal{E}'$ encrypts messages of length mn to ciphertexts of length $(m+1)n$, for any $1 \le m < n$. Let $\mathcal{T}'\colon \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^n$ be any MAC.

Then, let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme and $\mathcal{T}\colon \{0,1\}^{2k} \times \{0,1\}^* \to \{0,1\}^{n+k}$ a MAC, with algorithms described below.

The schemes $\mathcal{SE}$ and $\mathcal{T}$.

Alg $\underline{\mathcal{K}}$

$K \xleftarrow{\$} \{0,1\}^{2k}$; Return K

Alg $\underline{\mathcal{E}(K, M)}$

$K_1 \| K_2 \leftarrow K$
$C' \xleftarrow{\$} \mathcal{E}'(K_1, M)$
Return $K_2 \| C'$

Alg $\underline{\mathcal{D}(K, C)}$

$K_1 \| K_2 \leftarrow K$; $K' \| C' \leftarrow C$
$M \leftarrow \mathcal{D}'(K_1, C')$
Return M

Alg $\underline{\mathcal{T}(K, M)}$

$K_1 \| K_2 \leftarrow K$; $T \leftarrow \mathcal{T}'(K_2, M)$
Return $K_1 \| T$

The scheme $\mathcal{AE}$.

Alg $\underline{\mathcal{K}_a}$

$K \xleftarrow{\$} \{0,1\}^{2k}$; Return $K \| K$

Alg $\underline{\mathcal{E}_a(K, M)}$

$K_1 \| K_2 \leftarrow K$
$C \xleftarrow{\$} \mathcal{E}(K_1, M)$
$T \leftarrow \mathcal{T}(K_2, C)$
Return $C \| T$

Alg $\underline{\mathcal{D}_a(K, C \| T)}$

$K_1 \| K_2 \leftarrow K$
$M \leftarrow \mathcal{D}(K_2, C)$
$T' \leftarrow \mathcal{T}(K_2, C)$
If $(T' \neq T)$ then return $\perp$ else return M

Finally, let $\mathcal{AE} = (\mathcal{K}_a, \mathcal{E}_a, \mathcal{D}_a)$ be the AE scheme which combines $\mathcal{SE}$ and $\mathcal{T}$ in a Encrypt-then-MAC generic composition, but using the same key for both encryption and tag generation. These algorithms are described in full detail above. Note that $\mathcal{E}_a$ and $\mathcal{D}_a$ take a key of length $4k$, $\mathcal{E}$ and $\mathcal{D}$ take a key of length $2k$, and $\mathcal{E}'$ and $\mathcal{D}'$ take a key of length k. Here, t_E is the time taken to perform one $\mathcal{AE}$ encryption.

a. Show that $\mathcal{AE}$ is not IND-CPA secure by presenting an $\mathcal{O}(t_E + \ell + k)$ time adversary A_1 making one query with $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A_1) = 1$.

b. Show that $\mathcal{AE}$ is not INT-CTXT secure by presenting an $\mathcal{O}(t_E + \ell + k)$ time adversary A_2 making one query with $\mathbf{Adv}^{\text{int-ctxt}}_{\mathcal{AE}}(A_2) = 1$.

This problem shows that Encrypt-then-MAC is not secure if you use the same key for both primitives. Notice that this is true even if $\mathcal{SE}$ and $\mathcal{T}$ are secure. Think about how you would show that $\mathcal{SE}$ is IND-CPA secure (assuming $\mathcal{SE}'$ is IND-CPA secure) and how you would show that $\mathcal{T}$ is UF-CMA secure (assuming $\mathcal{T}'$ is UF-CMA secure). This will be the topic of an upcoming extra credit question.
