MTAT.07.003 Cryptology II
Spring 2008 / Homework 5

1. Let $\mathcal{F} \subseteq \{f : \mathcal{M} \to \mathcal{M}\}$ be a pseudorandom function family. Then we can use the CBC-MAC construction to stretch the input domain:

$$f^{(k)}(m_1, \ldots, m_k) = f(f(\cdots f(f(m_1) + m_2) + \cdots + m_{k-1}) + m_k) \ ,$$

provided that $(\mathcal{M}, +)$ is a commutative group. Prove the following facts about CBC-MAC construction.

   (a) If f is (t, q, ε)-pseudorandom function, then $f^{(k)} : \mathcal{M}^k \to \mathcal{M}$ is also pseudorandom function. Find the corresponding security guarantees.
   Hint: Write down the corresponding security game and simplify the evaluation of $f^{(k)}$ until all intermediate values are chosen uniformly from $\mathcal{M}$. Compute the probability of collisions.

   (b) Let $f^{(*)} : \mathcal{M}^* \to \mathcal{M}$ be a natural extension for variable input lengths, i.e., $f^{(*)}(m_1, \ldots, m_k) = f^{(k)}(m_1, \ldots, m_k)$ for any $k \in \mathbb{N}$. Prove that $f^{(*)}$ is not a pseudorandom function. Give a corresponding distinguisher that makes only 3 oracle calls.

   (c) Can we use CBC-MAC as an message authentication code?

2. A keyed hash function $h : \mathcal{M} \times \mathcal{K} \to \mathcal{T}$ is ε_1-almost universal if

$$\Pr\left[k \xleftarrow{u} \mathcal{K} : h(m_0, k) = h(m_1, k) \wedge m_0 \neq m_1\right] \leq \varepsilon_1$$

for all $m_0 \neq m_1$.

   (a) Prove that hybrid-MAC construction

$$\mathsf{mac}_{f,h}(m, k_1, k_2) = f(h(m, k_1), k_2)$$

   is secure message authentication code if f is (t, q, ε_2)-pseudorandom permutation and h is ε_1-almost universal. What are the corresponding security guarantees?
   Hints: Write down the corresponding game. Unroll the for cycle. Replace f with random function. Replace t_i with randomly chosen element of $\mathcal{T}$. Compute the differences in the game chain.

   (b) The hybrid hybrid CBC-MAC construction is following

$$\mathsf{mac}(m, f_1, f_2) = f_2\left(f_1^{(*)}(m)\right) \quad \text{for} \quad f_1 \in \mathcal{F}_1, f_2 \in \mathcal{F}_2 \ ,$$

   where $\mathcal{F}_1$ and $\mathcal{F}_2$ be a pseudorandom permutations. Show that the hybrid CBC-MAC construction is secure message authentication code even for variable input lengths. What is the role of f_2?

3. Although authentication codes provide security against impersonation and substitution attacks, they do not guarantee security against reflection and interleaving attacks.

(a) Show that message authentication protocol where $\mathcal{P}_1$ sends m and the corresponding authentication tag $t \leftarrow \mathsf{mac}(m, k)$ to $\mathcal{P}_2$ is not secure if we want to send several messages.

(b) Construct a protocol for authenticated communication that preserves message order and handles bidirectional message transfer. Establish the corresponding security guarantees.

(c) Construct a similar protocol without internal state. Use random nonces $r_i \leftarrow \mathcal{R}$ to guarantee that messages arrive in correct order.

(d) What are the advantages and disadvantages of stateful and stateless protocols for authenticated communication?

4. The polynomial message authentication code is secure only if we do not reuse the authentication key. Construct a modified stateful authentication code that allows us to use the same key for many messages. You can use the AES block cipher as a (t, ε)-pseudorandom permutation:

   (a) use the AES cipher to build hybrid-MAC;

   (b) use the AES cipher to stretch the initial key.

   Give the corresponding security proofs.

5. Let $h : \mathcal{M}^* \times \mathcal{K}_1 \to \mathcal{M}_2$ and $f : \mathcal{M}_2 \times \mathcal{K}_2 \to \mathcal{T}$ be keyed hash functions such that h is (t, q_1, ε_1)-weakly collision resistant and f is (t, q_2, ε_2)-secure message authentication code. Show that the NMAC construction

$$\textsc{Nmac}_{f,h}(m, k_1, k_2) = f(h(m, k_1), k_2)$$

   is secure message authentication code.

   Clarification: A keyed hash function h is (t, q, ε)-weakly collision resistant if any t-time adversary $\mathcal{A}$ that makes at most q oracle queries finds a collision with probability

$$\mathsf{Adv}_h^{\mathsf{w\text{-}cr}}(\mathcal{A}) = \Pr\left[\mathcal{G}^{\mathcal{A}} = 1\right] \le \varepsilon \ ,$$

   where the security game is defined as follows

$$\begin{array}{l}
\mathcal{G}^{\mathcal{A}} \\
\left[\begin{array}{l}
k \xleftarrow[u]{} \mathcal{K} \\
\text{For } i \in \{1, \ldots, q\} \text{ do} \\
\left[\text{Given } m_i \leftarrow \mathcal{A} \text{ send } t_i \leftarrow h(m_i, k) \text{ back to } \mathcal{A}.\right. \\
(m_0, m_1) \leftarrow \mathcal{A} \\
\mathsf{return}\ [m_0 \neq m_1] \wedge [h(m_0, k) = h(m_1, k)]
\end{array}\right.
\end{array}$$

   Hint: What happens if no collisions $f(m_1, k_1) = f(m_2, k_1)$ are revealed during the security game?

The NMAC construction is often instantiated with a single cryptographic hash function $h : \{0,1\}^* \to \{0,1\}^{256}$ by defining $f(m, k_1) = h(k_1 \| \mathsf{42} \| m)$ and $g(m, k_2) = h(k_2 \| \mathsf{13} \| m)$. Is this construction secure?

6. Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a IND-CPA secure symmetric encryption scheme and let $\mathsf{mac}(\cdot,\cdot)$ be a secure message authentication code. Show that following protection methods assure IND-CCA2 security:

   (a) first encrypt and then authenticate

   $\mathsf{Auth\text{-}Enc}(m)$

   $$\left[\begin{array}{l} c_1 \leftarrow \mathsf{Enc}_{\mathsf{sk}}(m) \\ c_2 \leftarrow \mathsf{mac}(c_1, k) \\ \text{return } (c_1, c_2) \end{array}\right.$$

   $\mathsf{Auth\text{-}Dec}(c_1, c_2)$

   $$\left[\begin{array}{l} \text{if } c_2 \neq \mathsf{mac}(c_1, k) \text{ then return } \perp \\ \text{else return } \mathsf{Dec}_{\mathsf{sk}}(c_1) \end{array}\right.$$

   (b) first authenticate and then encrypt

   $\mathsf{Auth\text{-}Enc}(m)$

   $$\left[\begin{array}{l} t \leftarrow \mathsf{mac}(m, k) \\ \text{return } \mathsf{Enc}_{\mathsf{sk}}(m, t) \end{array}\right.$$

   $\mathsf{Auth\text{-}Dec}(c)$

   $$\left[\begin{array}{l} (m, t) \leftarrow \mathsf{Dec}_{\mathsf{sk}}(c) \\ \text{if } t \neq \mathsf{mac}(m, k) \text{ then return } \perp \\ \text{else return } m \end{array}\right.$$

   (c) What are the advantages and drawbacks of both approaches? Why the construction does not generalise to public key cryptosystems?