MTAT.07.003 Cryptology II
Spring 2009 / Exercise session VI

Formal Security Definition

Recall that a keyed hash function $h : \mathcal{M} \times \mathcal{K} \to \mathcal{T}$ is a (t, q, ε)-*secure message authentication code* if any t-time adversary $\mathcal{A}$:

$$\mathsf{Adv}_h^{\mathsf{mac}}(\mathcal{A}) = \Pr\left[\mathcal{G}^{\mathcal{A}} = 1\right] \leq \varepsilon \enspace ,$$

where the security game is following

$$\begin{array}{l}\mathcal{G}^{\mathcal{A}}\\ \left[\begin{array}{l} k \xleftarrow[u]{} \mathcal{K}\\ \text{For } i \in \{1, \ldots, q\} \text{ do}\\ \left[\ \text{Given } m_i \leftarrow \mathcal{A} \text{ send } t_i \leftarrow h(m_i, k) \text{ back to } \mathcal{A}\right.\\ (m, t) \leftarrow \mathcal{A}\\ \textbf{return } [t \stackrel{?}{=} h(m, k)] \wedge [(m, t) \notin \{(m_1, t_1), \ldots, (m_q, t_q)\}]\end{array}\right.\end{array}$$

Applications of Message Authetication Codes

1. Although a good message authentication code $h : \mathcal{M} \times \mathcal{K} \to \mathcal{T}$ protects against impersonation and substitution attacks, it does 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 $t \leftarrow h(m, k)$ 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.

   (c) Construct a similar protocol without an 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?

2. Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a IND-CPA secure symmetric encryption scheme and let h be a secure message authentication code with the appropriate message and key domains. Show that the following protection methods assure IND-CCA2 security:

(a) first encrypt and then authenticate

$$\begin{array}{ll}\mathsf{Auth\text{-}Enc}_{\mathsf{sk},k}(m) & \mathsf{Auth\text{-}Dec}_{\mathsf{sk},k}(c_1,c_2)\\ \left[\begin{array}{l} c_1 \leftarrow \mathsf{Enc}_{\mathsf{sk}}(m)\\ c_2 \leftarrow h(c_1,k)\\ \mathbf{return}\ (c_1,c_2)\end{array}\right. & \left[\begin{array}{l}\mathsf{if}\ c_2 \neq h(c_1,k)\ \mathsf{then}\ \mathbf{return}\ \perp\\ \mathsf{else}\ \mathbf{return}\ \mathsf{Dec}_{\mathsf{sk}}(c_1)\end{array}\right.\end{array}$$

(b) first authenticate and then encrypt

$$\begin{array}{ll}\mathsf{Auth\text{-}Enc}_{\mathsf{sk},k}(m) & \mathsf{Auth\text{-}Dec}_{\mathsf{sk},k}(c)\\ \left[\begin{array}{l} t \leftarrow h(m,k)\\ \mathbf{return}\ \mathsf{Enc}_{\mathsf{sk}}(m,t)\end{array}\right. & \left[\begin{array}{l}(m,t) \leftarrow \mathsf{Dec}_{\mathsf{sk}}(c)\\ \mathsf{if}\ t \neq h(m,k)\ \mathsf{then}\ \mathbf{return}\ \perp\\ \mathsf{else}\ \mathbf{return}\ m\end{array}\right.\end{array}$$

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

Common Message Authentication Codes

3. A keyed hash function $h : \mathcal{M} \times \mathcal{K} \to \mathcal{T}$ 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

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

where the security game is defined as follows

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

(a) 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.

(b) Analyse the NMAC construction under the assumption that that h is (t, q_1, ε_1)-weakly collision resistant and $\mathcal{F} = \{f_k\}$ where $f_k(x) = f(x, k)$ is (t, q_2, ε_2)-pseudorandom function family.

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

Hint: Write down the corresponding security game. What happens if the adversary provides a message m that creates a collision $h(m, k) = h(m_i, k)$ as an answer? How probable this event can be?

4. A keyed hash function $h : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{T}$ is ε_1-almost universal if for all distinct message pairs $m_0 \neq m_1$ the collision probability is bounded

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

Prove that hybrid-MAC construction

$$\text{HYB-MAC}_{f,h}(m, k_1, k_2) = f(h(m, k_1), k_2)$$

is secure message authentication code if $\mathcal{F} = \{f_{k_2}\}_{k_2 \in \mathcal{K}_2}$ is (t, q, ε_2)-pseudorandom function family and $h : \mathcal{M} \times \mathcal{K}_2 \rightarrow \mathcal{T}$ is ε_1-almost universal. What are the corresponding security guarantees?

Hints: Write down the corresponding security game. Unroll the for cycle. Replace f with a random function. Replace t_i with randomly chosen element of $\mathcal{T}$ when possible. Most importantly, treat the cases when f is evaluated several times at the same argument correctly. What is the main difference in the security analysis compared to the previous exercise?

5. 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.

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

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

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?

7. The hybrid hybrid CBC-MAC construction is following

$$\textsc{Hyb-Cbc-Mac}(m, f_1, f_2) = f_2\big(f_1^{(*)}(m)\big) \quad \text{for} \quad f_1 \in \mathcal{F}_1, f_2 \in \mathcal{F}_2 \ ,$$

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