Introduction to Cryptology

Lecture 14

Announcements

- HW 6 due on Thurs. 4/2.
- HW 5 solutions and grades up on Canvas.

Agenda

- Last time:
  - Constructing a fixed-length MAC (4.3)
  - Domain extension with CBC-MAC (4.4)

- This time:
  - Authenticated Encryption (4.5)
  - New topic: Collision Resistant Hash Functions (CRHF)
    - Definitions (5.1)
    - Domain extension: The Merkle-Damgard Transform (5.2)

Authenticated Encryption

The unforgeable encryption experiment $EncForge_{A,\Pi}(n)$:

1. Run $Gen(1^n)$ to obtain key k.
2. The adversary A is given input 1^n and access to an encryption oracle $Enc_k(\cdot)$. The adversary outputs a ciphertext c.
3. Let $m \coloneqq Dec_k(c)$, and let Q denote the set of all queries that A asked its encryption oracle. The output of the experiment is 1 if and only if (1) $m \neq \perp$ and (2) $m \notin Q$.

Authenticated Encryption

Definition: A private-key encryption scheme Π is unforgeable if for all ppt adversaries A, there is a negligible funcion neg such that:

$$\Pr\left[EncForge_{A,\Pi}(n) = 1\right] \leq neg(n).$$

Definition: A private-key encryption scheme is an authenticated encryption scheme if it is CCA-secure and unforgeable.

Generic Constructions

Encrypt-and-authenticate

Encryption and message authentication are computed independently in parallel.

$$c \leftarrow Enc_{k_E}(m) \qquad t \leftarrow Mac_{k_M}(m)$$

$$\langle c, t \rangle$$

Is this secure? NO!

Authenticate-then-encrypt

Here a MAC tag t is first computed, and then the message and tag are encrypted together.

$$t \leftarrow Mac_{k_M}(m) \qquad c \leftarrow Enc_{k_E}(m||t)$$

c is sent

Is this secure? NO! Encryption scheme may not be CCA-secure.

Encrypt-then-authenticate

The message m is first encrypted and then a MAC tag is computed over the result

$$c \leftarrow Enc_{k_E}(m) \quad t \leftarrow Mac_{k_M}(c)$$

$$\langle c, t \rangle$$

Is this secure? YES! As long as the MAC is strongly secure.

Secure Authenticated Encryption Scheme

Let $\Pi_E = (Enc, Dec)$ be a CPA-secure private key encryption scheme. Let $\Pi_M = (Mac, Vrfy)$ be a strongly secure MAC. In each case key generation is done by choosing a uniform n-bit key. Define (Gen', Enc', Dec') as follows:

- Gen': on input 1^n, choose independent, uniform $k_E, k_M \in \{0,1\}^n$ and output the key (k_E, k_M).
- Enc': on input a key (k_E, k_M) and a plaintext message m, compute$c \leftarrow Enc_{k_E}(m), t \leftarrow Mac_{k_M}(c)$. Output $\langle c, t \rangle$.
- Dec': on input a key (k_E, k_M) and a ciphertext $\langle c, t \rangle$, first check whether $Vrfy_{k_M}(c, t) = 1$. If yes, output $Dec_{k_E}(c)$; if no, then output $\perp$.

Secure Authenticated Encryption Scheme

Theorem: Let Π_E be a CPA-secure private-key encryption scheme and let Π_M be a strongly secure message authentication code. Then the construction is an authenticated encryption scheme.