Introduction to Cryptology

Lecture 10
Announcements

• HW4 due today
• HW5 up on course webpage, due 3/7
• Instructor OH this week:
  – Thursday 3/2, 3-4pm
  – Monday 3/6, 3:30-4:30pm
Agenda

• Last time:
  – CPA-secure encryption from PRF (Sec. 3.5)

• This time:
  – PRP (Block Ciphers) (3.5)
  – Modes of operation (3.6)
  – New topic:
    • Message Authentication Codes (MAC) (4.2)
    • Constructing MAC from PRF (4.3)
Block Ciphers/Pseudorandom Permutations

Definition: Pseudorandom Permutation is exactly the same as a Pseudorandom Function, except for every key $k$, $F_k$ must be a permutation and it must be indistinguishable from a random permutation.
Strong Pseudorandom Permutation

Definition: Let $F: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be an efficient, length-preserving, keyed permutation. We say that $F$ is a strong pseudorandom permutation if for all ppt distinguishers $D$, there exists a negligible function $\text{negl}$ such that:

$$\left| \Pr[D^{F_k(\cdot),F^{-1}_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot),f^{-1}(\cdot)}(1^n) = 1] \right| \leq \text{negl}(n).$$

where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and $f$ is chosen uniformly at random from the set of all permutations mapping $n$-bit strings to $n$-bit strings.
Modes of Operation—Stream Cipher

If sender and receiver are willing to maintain state, can encrypt multiple messages.
Modes of Operation—Block Cipher

**FIGURE 3.5:** Electronic Code Book (ECB) mode.

**FIGURE 3.6:** An illustration of the dangers of using ECB mode. The middle figure is an encryption of the image on the left using ECB mode; the figure on the right is an encryption of the same image using a secure mode.

**FIGURE 3.7:** Cipher Block Chaining (CBC) mode.
Modes of Operation—Block Cipher

**FIGURE 3.9:** Output Feedback (OFB) mode.

**FIGURE 3.10:** Counter (CTR) mode.
Message Integrity

- Secrecy vs. Integrity

- Encryption vs. Message Authentication
Message Authentication Codes

Definition: A message authentication code (MAC) consists of three probabilistic polynomial-time algorithms \((Gen, Mac, Vrfy)\) such that:

1. The key-generation algorithm \(Gen\) takes as input the security parameter \(1^n\) and outputs a key \(k\) with \(|k| \geq n\).

2. The tag-generation algorithm \(Mac\) takes as input a key \(k\) and a message \(m \in \{0,1\}^*\), and outputs a tag \(t\).
   \[
   t \leftarrow Mac_k(m).
   \]

3. The deterministic verification algorithm \(Vrfy\) takes as input a key \(k\), a message \(m\), and a tag \(t\). It outputs a bit \(b\) with \(b = 1\) meaning valid and \(b = 0\) meaning invalid.
   \[
   b \overset{\text{def}}{=} Vrfy_k(m, t).
   \]

It is required that for every \(n\), every key \(k\) output by \(Gen(1^n)\), and every \(m \in \{0,1\}^*\), it holds that \(Vrfy_k(m, Mac_k(m)) = 1\).
Security of MACs

The message authentication experiment $MAC_{\text{forge}}_{A,\Pi}(n)$:

1. A key $k$ is generated by running $Gen(1^n)$.

2. The adversary $A$ is given input $1^n$ and oracle access to $Mac_k(\cdot)$. The adversary eventually outputs $(m, t)$. Let $Q$ denote the set of all queries that $A$ asked its oracle.

3. $A$ succeeds if and only if (1) $Vrfy_k(m, t) = 1$ and (2) $m \notin Q$. In that case, the output of the experiment is defined to be 1.
Security of MACs

Definition: A message authentication code $\Pi = (Gen, Mac, Vrfy)$ is existentially unforgeable under an adaptive chosen message attack if for all probabilistic polynomial-time adversaries $A$, there is a negligible function $neg$ such that:

$$\Pr[\text{MAC\text{-}forge}_{A,\Pi}(n) = 1] \leq neg(n).$$
Strong MACs

The strong message authentication experiment $MAC_{forge}^{A,\Pi}(n)$:

1. A key $k$ is generated by running $Gen(1^n)$.
2. The adversary $A$ is given input $1^n$ and oracle access to $Mac_k(\cdot)$. The adversary eventually outputs $(m, t)$. Let $Q$ denote the set of all pairs $(m, t)$ that $A$ asked its oracle.
3. $A$ succeeds if and only if (1) $Vrfy_k(m, t) = 1$ and (2) $(m, t) \notin Q$. In that case, the output of the experiment is defined to be $1$. 
Strong MACs

Definition: A message authentication code \( \Pi = (\text{Gen}, \text{Mac}, \text{Vrfy}) \) is a strong MAC if for all probabilistic polynomial-time adversaries \( A \), there is a negligible function \( neg \) such that:

\[
\Pr[\text{MACsforge}_{A,\Pi}(n) = 1] \leq neg(n).
\]