Introduction to Cryptology

Lecture 11
Announcements

• HW5 is up on course webpage, deadline extended to 3/12
• Grades and solutions for HW3, HW4 are up on Canvas.
• Midterm is on Thursday, 3/12
  – Review problems and solutions and list of topics for exam are up on the course webpage
Agenda

• Last time:
  – Construction of CPA-secure SKE from PRF (3.5)

• This time:
  – Block ciphers, Stream ciphers and modes of operation (3.6)
  – CCA security (3.7)
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.

**FIGURE 3.4:** Synchronized mode vs. unsynchronized mode.
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.