Cryptography

Lecture 9

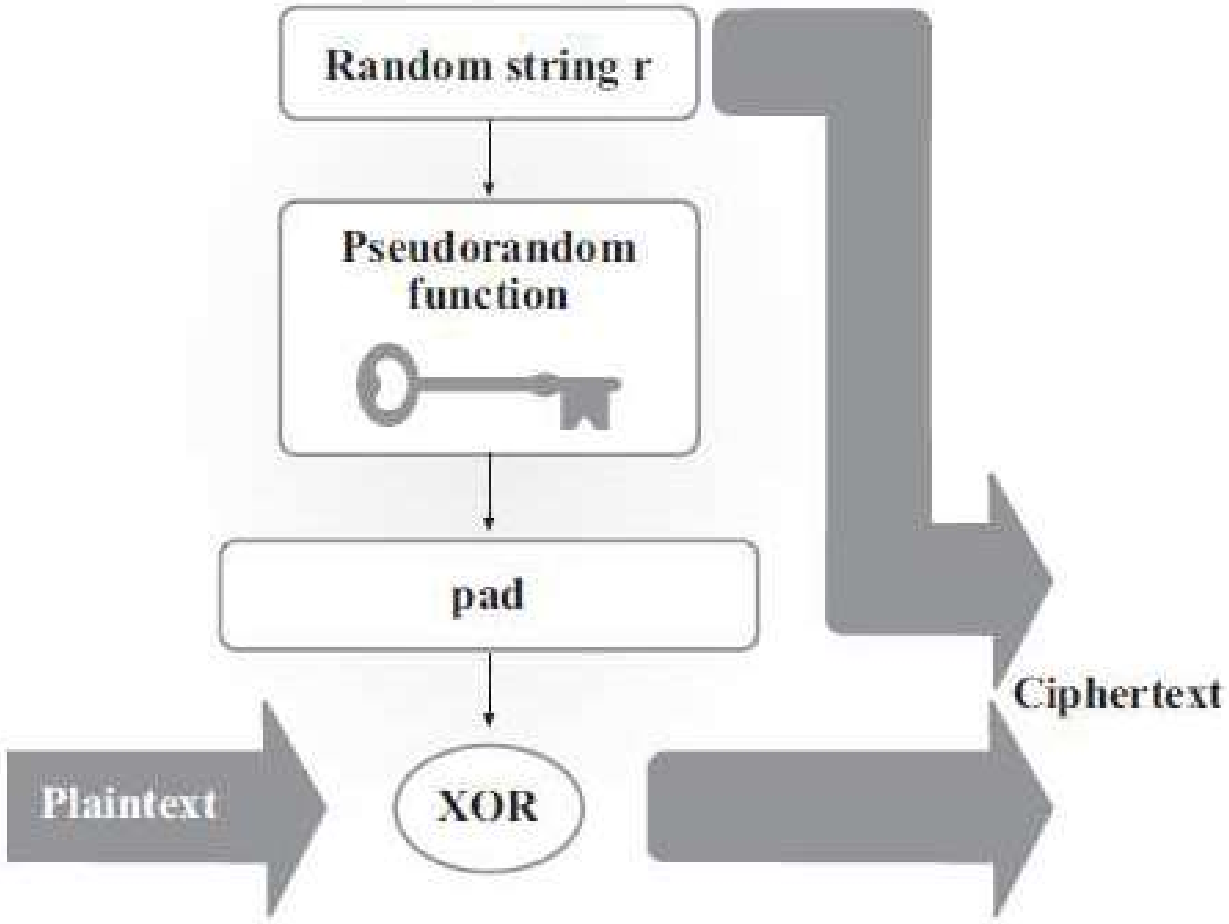
Announcements

- HW4 due today
- HW4 up on course webpage, due 3/4

Agenda

- Last time:
  - Stream Ciphers
  - CPA Security (K/L 3.4)
  - Pseudorandom Functions (PRF) (K/L 3.5)
- This time:
  - CPA-secure encryption from PRF (K/L 3.5)
  - PRP (Block Ciphers) (K/L 3.5)
  - Modes of operation (K/L 3.6)

Construction of CPA-Secure Encryption from PRF



Formal Description of Construction

Let F be a pseudorandom function. Define a private-key encryption scheme for messages of length n as follows:

- Gen: on input 1^n, choose $k \leftarrow \{0,1\}^n$ uniformly at random and output it as the key.
- Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, choose $r \leftarrow \{0,1\}^n$uniformly at random and output the ciphertext
$$c \coloneqq \langle r, F_k(r) \oplus m \rangle.$$
- Dec: on input a key $k \in \{0,1\}^n$ and a ciphertext $c = \langle r, s \rangle$, output the plaintext message
$$m \coloneqq F_k(r) \oplus s.$$

Security Analysis

Theorem: If F is a pseudorandom function, then the Construction above is a CPA-secure private-key encryption scheme for messages of length n.

Recall: CPA-Security

The CPA Indistinguishability Experiment ${PrivK^{cpa}}_{A,\Pi}(n)$:

1. A key k is generated by running $Gen(1^n)$.
2. The adversary A is given input 1^n and oracle access to $Enc_k(\cdot)$, and outputs a pair of messages m_0, m_1 of the same length.
3. A random bit $b \leftarrow \{0,1\}$ is chosen, and then a challenge ciphertext $c \leftarrow Enc_k(m_b)$ is computed and given to A.
4. The adversary A continues to have oracle access to $Enc_k(\cdot)$, and outputs a bit b'.
5. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

Recall: CPA-Security

Definition: A private-key encryption scheme $\Pi = (Gen, Enc, Dec)$ has indistinguishable encryptions under a chosen-plaintext attack if for all ppt adversaries A there exists a negligible function $negl$ such that

$$\Pr\left[PrivK^{cpa}{}_{A,\Pi}(n) = 1\right] \le \frac{1}{2} + negl(n),$$

where the probability is taken over the random coins used by A, as well as the random coins used in the experiment.

Security Analysis

Let A be a ppt adversary trying to break the security of the construction. We construct a distinguisher D that uses A as a subroutine to break the security of the PRF.

Distinguisher D:

D gets oracle access to oracle O, which is either F_k, where F is pseudorandom or f which is truly random.

1. Instantiate $A^{Enc_k(\cdot)}(1^n)$.
2. When A queries its oracle, with message m, choose r at random, query $O(r)$ to obtain z and output c $:= \langle r, z \oplus m \rangle$.
3. Eventually, A outputs $m_0, m_1 \in \{0,1\}^n$.
4. Choose a uniform bit $b \in \{0,1\}$. Choose r at random, query $O(r)$ to obtain z and output c $:= \langle r, z \oplus m \rangle$.
5. Give c to A and obtain output b'. Output 1 if $b' = b$, and output 0 otherwise.

Security Analysis

Consider the probability D outputs 1 in the case that O is truly random function f vs. O is a pseudorandom function F_k.

- When O is pseudorandom, D outputs 1 with probability $\Pr\left[PrivK^{cpa}{}_{A,\Pi}(n) = 1\right] = \frac{1}{2} + \rho(n)$, where ρ is non-negligible.
- When O is random, D outputs 1 with probability at most $\frac{1}{2} + \frac{q(n)}{2^n}$, where $q(n)$ is the number of oracle queries made by A. Why?

Security Analysis

D's distinguishing probability is:

$$\left|\frac{1}{2}+\frac{q(n)}{2^n}-\left(\frac{1}{2}+\rho(n)\right)\right|=\rho(n)\ -\ \frac{q(n)}{2^n}.$$

Since, $\frac{q(n)}{2^n}$ is negligible and $\rho(n)$ is non-negligible, $\rho(n)\ -\ \frac{q(n)}{2^n}$ is non-negligible.

This is a contradiction to the security of the PRF.

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 $F\colon \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ 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 $negl$ such that:

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

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—Block Cipher

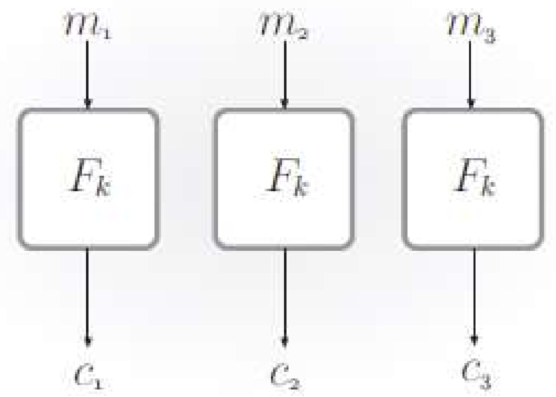


FIGURE 3.5: Electronic Code Book (ECB) mode.

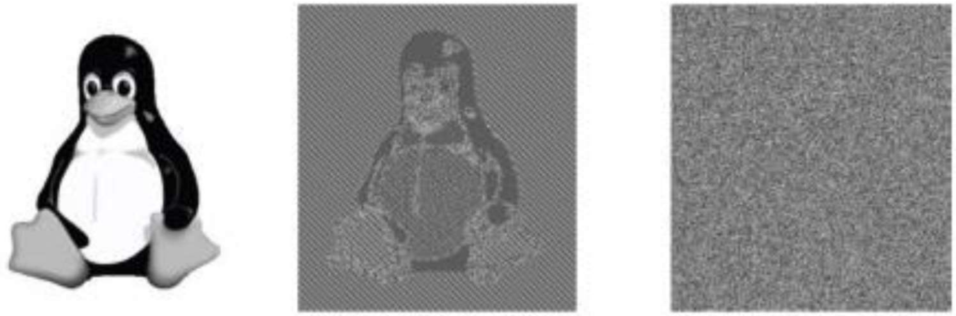


FIGURE 3.6: An illustration of the dangers of using ECB mode. The middle figure is an encryption of the image on the left using ECB mode; the figure on the right is an encryption of the same image using a secure mode.

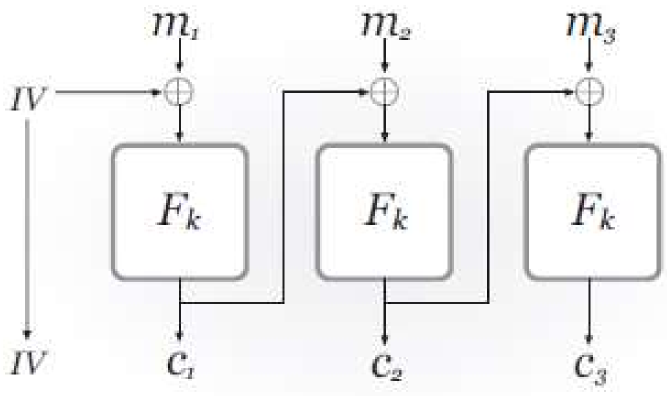


FIGURE 3.7: Cipher Block Chaining (CBC) mode.

Modes of Operation—Block Cipher

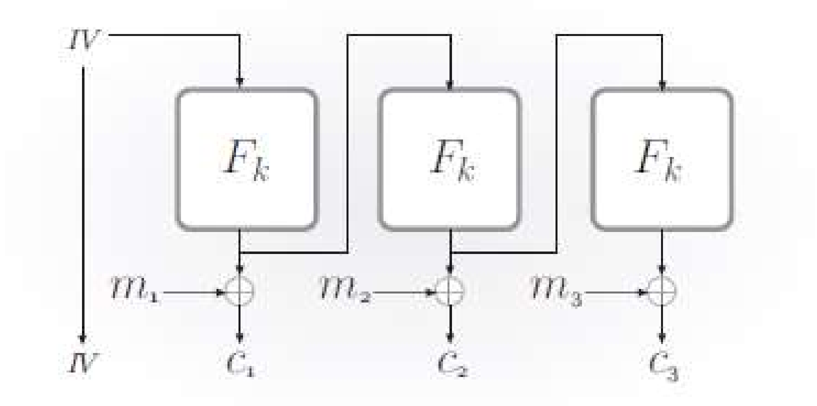


FIGURE 3.9: Output Feedback (OFB) mode.

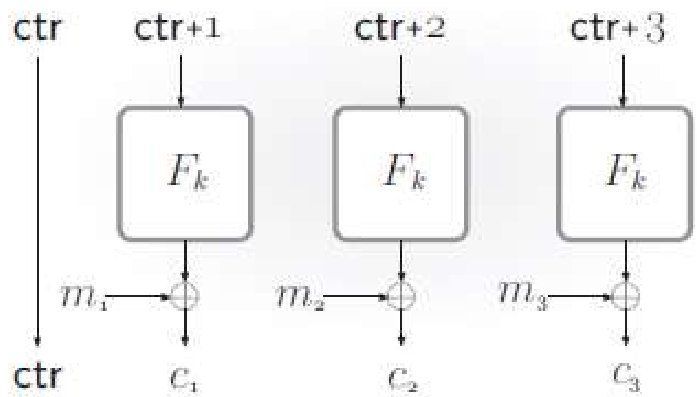


FIGURE 3.10: Counter (CTR) mode.