# Introduction to Cryptology

Lecture 9

# Announcements

- HW4 up on course webpage, due Tuesday, 3/1

# Agenda

- Last time:
  - CPA Security (Sec. 3.4)
  - Pseudorandom Functions (PRF) (Sec. 3.5)
  - Constructing CPA-secure encryption from PRF (Sec. 3.5)
- This time:
  - Proof of security for the construction (3.5)
  - Class exercise on PRFs

# 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.

# 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

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

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

# CPA-security for multiple encryptions

Theorem: Any private-key encryption scheme that has indistinguishable encryptions under a chosen-plaintext attack also has indistinguishable multiple encryptions under a chosen-plaintext attack.

# CPA-secure Encryption Must Be Probabilisitic

Theorem: If $\Pi = (Gen, Enc, Dec)$ is an encryption scheme in which $Enc$ is a deterministic function of the key and the message, then $\Pi$ cannot be CPA-secure.

Why not?

# Constructing CPA-Secure Encryption Scheme

# Pseudorandom Function

Definition: A keyed function $F: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ is a two-input function, where the first input is called the key and denoted $k$.

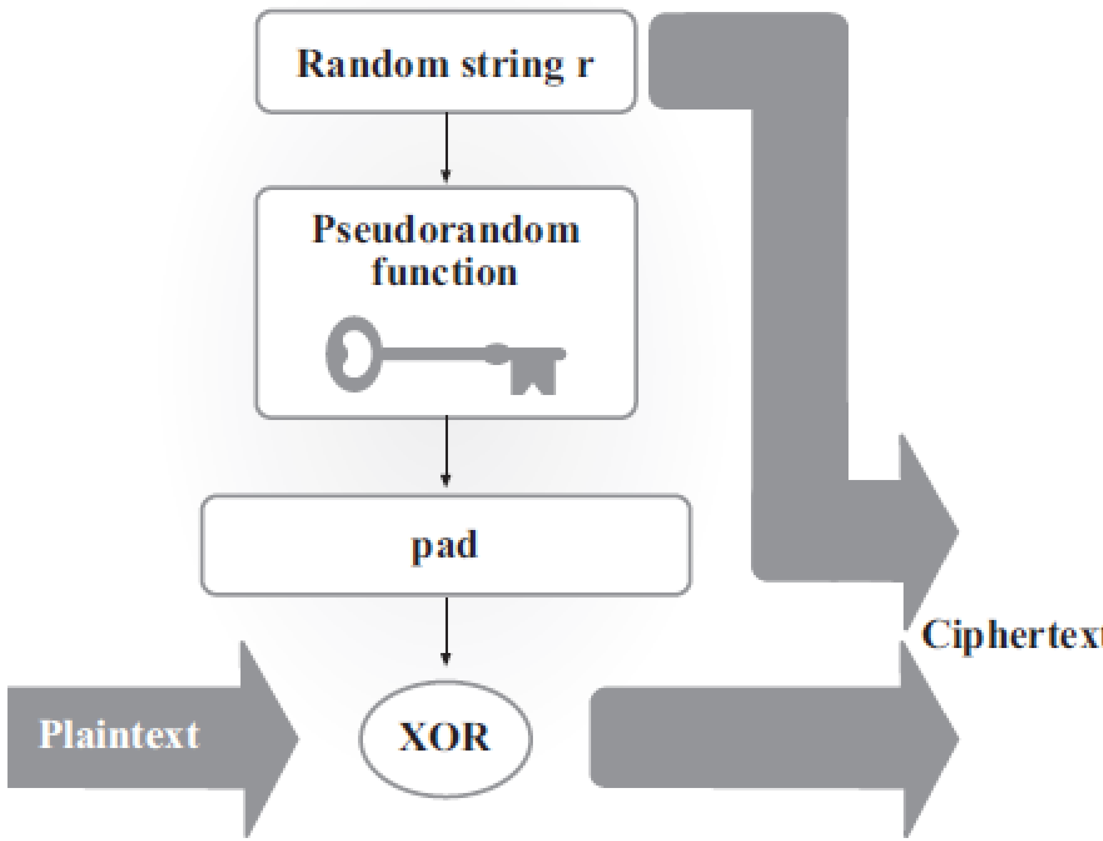
# Pseudorandom Function

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

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

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

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

# 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

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

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 $\rho$ 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.