Introduction to Cryptology

Lecture 7

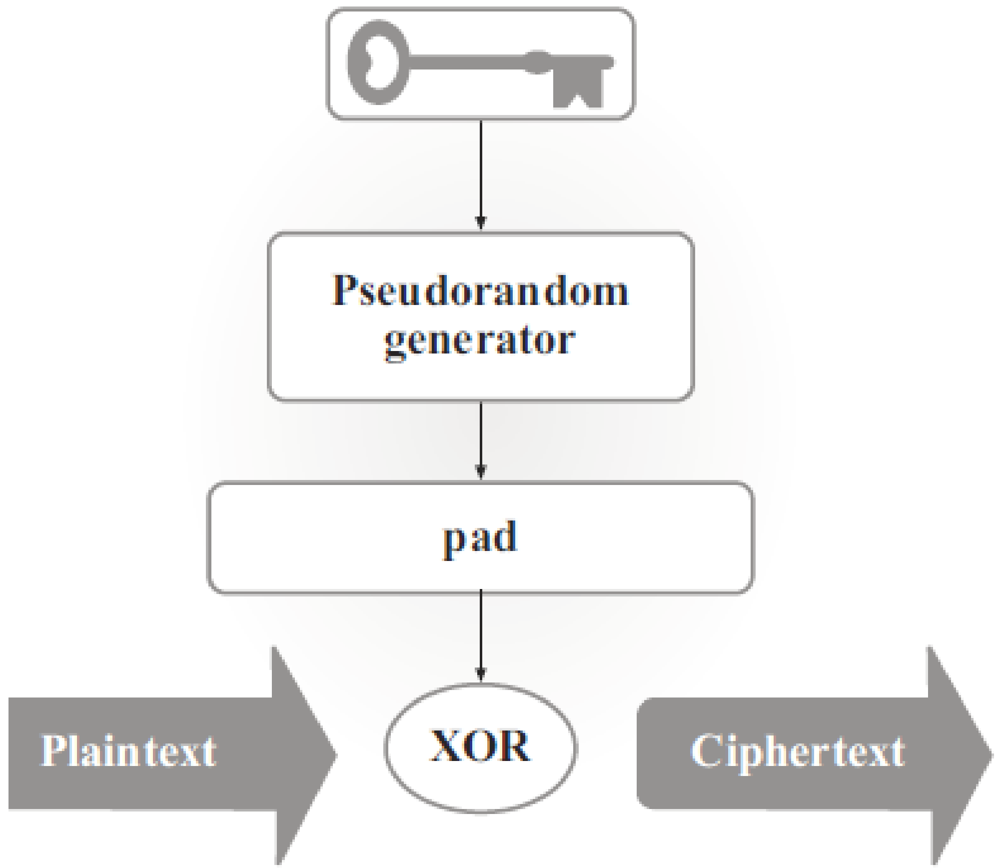
Announcements

- HW3 due Tuesday, 2/23

Agenda

- Last time:
  - Defining computationally secure SKE (Sec. 3.2)
  - Defining PRG (Sec. 3.3)
  - Constructing computationally secure SKE (Sec. 3.3)
- This time:
  - Security proof for construction (Sec. 3.3)
  - Exercise on PRG
  - Discussion on Stream Ciphers

A Secure Fixed-Length Encryption Scheme



The Encryption Scheme

Let G be a pseudorandom generator with expansion factor ℓ. Define a private-key encryption scheme for messages of length ℓ 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 $m \in \{0,1\}^{\ell(n)}$, output the ciphertext
$$c := G(k) \oplus m.$$
- Dec: on input a key $k \in \{0,1\}^n$ and a ciphertext $c \in \{0,1\}^{\ell(n)}$, output the plaintext message
$$m := G(k) \oplus c.$$

Recall: Indistinguishability in the presence of an eavesdropper

Consider a private-key encryption scheme $\Pi = (Gen, Enc, Dec)$, any adversary A, and any value n for the security parameter.

The eavesdropping indistinguishability experiment ${PrivK^{eav}}_{A,\Pi}(n)$:

1. The adversary A is given input 1^n, and outputs a pair of messages m_0, m_1 of the same length.
2. A key k is generated by running $Gen(1^n)$, and a random bit $b \leftarrow \{0,1\}$ is chosen. A challenge ciphertext $c \leftarrow Enc_k(m_b)$ is computed and given to A.
3. Adversary A outputs a bit b'.
4. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. If ${PrivK^{eav}}_{A,\Pi}(n) = 1$, we say that A succeeded.

Recall: Indistinguishability in the presence of an eavesdropper

Definition: A private key encryption scheme $\Pi = (Gen, Enc, Dec)$ has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries A there exists a negligible function $negl$ such that

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

Where the prob. Is taken over the random coins used by A, as well as the random coins used in the experiment.

Security Analysis

Theorem: If G is a pseudorandom generator, then the Construction above is a fixed-length private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper.

Security Analysis

- Proof by reduction method.

Security Analysis

Proof: 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 PRG.

Distinguisher D:

D is given as input a string $w \in \{0,1\}^{\ell(n)}$.

1. Run $A(1^n)$ to obtain messages $m_0, m_1 \in \{0,1\}^{\ell(n)}$.
2. Choose a uniform bit $b \in \{0,1\}$. Set $c := w \oplus m_b$.
3. 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 w is random string r vs. w is a pseudorandom string $G(s)$.

- When w is random, D outputs 1 with probability exactly ½. Why?
- When w is pseudorandom, D outputs 1 with probability $\Pr\left[PrivK^{eav}{}_{A,\Pi}(n) = 1\right] = \frac{1}{2} + \rho(n)$, where ρ is non-negligible.

Security Analysis

D's distinguishing probability is:

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

This is a contradiction to the security of the PRG, since ρ is non-negligible.

Stream Cipher

Sender

State s_i after sending the i-th message:

$$s_0 \coloneqq k$$
$$s_{i+1} \coloneqq G(s_i)_2, \ldots, G(s_i)_{n+1}$$
$$pad_{i+1} \coloneqq G(s_i)_1$$

$$c_{i+1} \coloneqq m_{i+1} \oplus pad_{i+1} \longrightarrow$$

Receiver

State s_i after receiving the i-th message:

$$s_0 \coloneqq k$$
$$s_{i+1} \coloneqq G(s_i)_2, \ldots, G(s_i)_{n+1}$$
$$pad_{i+1} \coloneqq G(s_i)_1$$

$$m_{i+1} \coloneqq c_{i+1} \oplus pad_{i+1}$$