{ CSCI 6331 · 4331 | Lecture 3 }

Cryptography

Hoeteck Wee · hoeteck@gwu.edu

http://tinyurl.com/cryptogw/

Announcements

- Evaluation:

  10% In-Class/Piazza, 20% Final Presentation / Project

  30% Homework, 40% Final (Apr 25)

Today

- Single Message Security
- Block Ciphers
- Security for Multiple Encryptions

Eavesdropping Security for Single Message

1. (message selection) $\mathcal{A}(1^n)$ outputs m_0, m_1 of same length.
2. (key generation) generate key k
3. (challenge bit) random bit $b \leftarrow \{0, 1\}$.
4. (challenge ciphertext) $c \leftarrow \mathrm{Enc}(m_b)$ given to $\mathcal{A}$
5. $\mathcal{A}$ outputs b' and wins if $b' = b$

Q. What is $\mathcal{A}$'s winning probability if it outputs random bit b'?

Q. What is $\mathcal{A}$'s winning probability if it chooses $m_0 = m_1$?

NB. $\mathcal{A}$ chooses m_0, m_1 (chosen plaintext) and knows m_0, m_1.

Eavesdropping Security for Single Message

1. (message selection) $\mathcal{A}(1^n)$ outputs m_0, m_1 of same length.
2. (key generation) generate key k
3. (challenge bit) random bit $b \leftarrow \{0, 1\}$.
4. (challenge ciphertext) $c \leftarrow \mathrm{Enc}(m_b)$ given to $\mathcal{A}$
5. $\mathcal{A}$ outputs b' and wins if $b' = b$

definition. $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is (t, ϵ)-single-message indistinguishable if for all adversaries $\mathcal{A}$ running in time t, winning probability bounded by $1/2 + \epsilon$

$\Longrightarrow$ e.g. ciphertext "hides" first bit of plaintext

last lecture. single-message indistinguishability by using PRG as one-time pad.

Q. typically, PRG has fixed-length output. How to encrypt longer messages?

Pseudorandom Functions (PRF)

Pseudorandom Functions (PRF) defined over $(\mathrm{K}, \mathrm{X}, \mathrm{Y})$:

$$\mathrm{F} : \mathrm{K} \times \mathrm{X} \to \mathrm{Y} \quad (\text{ key } \times \text{ input } \to \text{ output })$$

- "efficient" algorithm to evaluate $\mathrm{F}(\mathrm{k}, \mathrm{x})$

example. AES : $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$

intuition. gives us many one-time pads, $\mathrm{F}(\mathrm{k}, 0), \mathrm{F}(\mathrm{k}, 1), \mathrm{F}(\mathrm{k}, 2), \mathrm{F}(\mathrm{k}, 3), \ldots$

1. (challenge bit) random bit $\mathrm{b} \leftarrow \{0,1\}$.
2. (challenge function) if $\mathrm{b} = 1$, f is truly random function from X to Y;

   if $\mathrm{b} = 0$, f is $\mathrm{F}(\mathrm{k}, \cdot)$ for a random k
3. $\mathcal{A}$ gets $\mathrm{f}(0), \mathrm{f}(1), \mathrm{f}(2), \ldots$
4. $\mathcal{A}$ outputs b' and wins if $\mathrm{b}' = \mathrm{b}$

definition. $\mathrm{F} : \mathrm{K} \times \mathrm{X} \to \mathrm{Y}$ is (t, ϵ)-secure PRF if for all adversaries $\mathcal{A}$ running in time t, winning probability bounded by $1/2 + \epsilon$

Pseudorandom Functions (PRF)

Pseudorandom Functions (PRF) defined over (K, X, Y):

$$F : K \times X \to Y \quad (\text{ key} \times \text{input} \to \text{output })$$

- "efficient" algorithm to evaluate $F(k, x)$

example. AES : $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$

intuition. gives us many one-time pads, $F(k,0), F(k,1), F(k,2), F(k,3), \ldots$

Deterministic Counter Mode. using PRF $F : K \times \{0,1\}^{128} \to \{0,1\}^{128}$.

- break message m into 128-bit blocks $(m_0, m_1, m_2, m_3, m_4, \ldots)$
- $\mathrm{Enc}_k(m)$ outputs $(m_0 \oplus F(k,0), m_1 \oplus F(k,1), m_2 \oplus F(k,2), \ldots)$
- $\mathrm{Dec}_k(c_0, c_1, \ldots)$ outputs $(c_0 \oplus F(k,0), c_1 \oplus F(k,1), \ldots)$

Pseudorandom Permutations (PRP) aka Block Ciphers

Pseudorandom Functions (PRF) defined over $(\mathrm{K}, \mathrm{X}, \mathrm{Y})$:

$$\mathrm{F} : \mathrm{K} \times \mathrm{X} \to \mathrm{Y} \quad (\text{ key } \times \text{ input } \to \text{ output })$$

- "efficient" algorithm to evaluate $\mathrm{F}(\mathrm{k}, \mathrm{x})$

Pseudorandom Permutations (PRP) defined over (K, X):

$$\mathrm{E} : \mathrm{K} \times \mathrm{X} \to \mathrm{X} \quad (\text{ input = output = } \mathrm{X})$$

- "efficient" algorithm to evaluate $\mathrm{E}(\mathrm{k}, \mathrm{x})$
- function $\mathrm{E}(\mathrm{k}, \cdot)$ is one-to-one
- "efficient" inversion algorithm $\mathrm{D}(\mathrm{k}, \mathrm{x})$

example. AES : $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$;

DES : $\{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$

note. functionally, a PRP is also a PRF where $\mathrm{X} = \mathrm{Y}$ and is efficiently invertible

Pseudorandom Permutations (PRP) aka Block Ciphers

Pseudorandom Permutations (PRP) defined over (K, X):

$\mathrm{E} : \mathrm{K} \times \mathrm{X} \to \mathrm{X}$ (input = output = X)

1. (challenge bit) random bit $\mathrm{b} \leftarrow \{0, 1\}$.
2. (challenge function) if $\mathrm{b} = 1$, f is truly random permutation from X to X;

   if $\mathrm{b} = 0$, f is $\mathrm{E}(\mathrm{k}, \cdot)$ for a random k
3. $\mathcal{A}$ gets $\mathrm{f}(0), \mathrm{f}(1), \mathrm{f}(2), \ldots$
4. $\mathcal{A}$ outputs b' and wins if $\mathrm{b}' = \mathrm{b}$

definition. $\mathrm{F} : \mathrm{K} \times \mathrm{X} \to \mathrm{X}$ is (t, ϵ)-secure PRP if for all adversaries $\mathcal{A}$ running in time t, winning probability bounded by $1/2 + \epsilon$

AES Assumption. AES : $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ is a $(2^{80}, 2^{-40})$-secure PRP

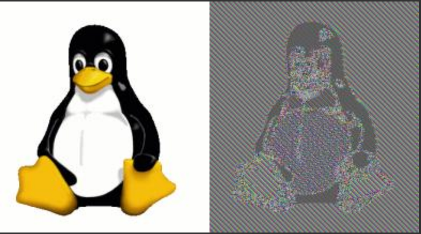
theorem. any secure PRP is also a secure PRF.

Electronic Code Book (ECB)

Electronic Code Book (ECB) Mode. using PRP $E : K \times \{0,1\}^{128} \to \{0,1\}^{128}$.

- break message m into 128-bit blocks $(m_0, m_1, m_2, m_3, m_4, \ldots)$
- $\mathrm{Enc}_k(m)$ outputs $(E(k, m_0), E(k, m_1), E(k, m_2), \ldots)$

problem. if two message blocks are equal, then ciphertext blocks are equal.



solution. Don't use ECB!

One-Time vs Many-Time Key

so far.. One key per message

- example application: encrypted email, new key for every message

next... One key for multiple messages

- example applications: file systems (same AES key, many files); IPsec (same AES key, many packets)
- alternative viewpoint: many-time / reuseable key
- "multiple messages" different from "one message, multiple blocks"

  Q. how to define security?

  Q. how to build such schemes from block ciphers?

Eavesdropping Security for Multiple Messages

1. (message selection) $\mathcal{A}(1^n)$ outputs $(m_0^1, \ldots, m_0^t), (m_1^1, \ldots, m_1^t)$
2. (key generation) generate key k
3. (challenge bit) random bit $b \leftarrow \{0, 1\}$.
4. (challenge ciphertext) $c^i \leftarrow \mathrm{Enc}(m_b^i), i = 1, 2, \ldots, t$ given to $\mathcal{A}$
5. $\mathcal{A}$ outputs b' and wins if $b' = b$

definition. $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is (t, ϵ)-multiple-message indistinguishable if for all adversaries $\mathcal{A}$ running in time t, winning probability bounded by $1/2 + \epsilon$

example: shift cipher. messages are characters, $k \in 0, 1, \ldots, 25$.

$\mathcal{A}$ outputs ('A', 'B'), ('C', 'D') and suppose $k = 3$.

what is (c^1, c^2) if $b = 0$? and $b = 1$?

Eavesdropping Security for Multiple Messages

lemma. if Enc is deterministic, not two-message indistinguishable

proof. if two messages are equal, then ciphertexts are equal

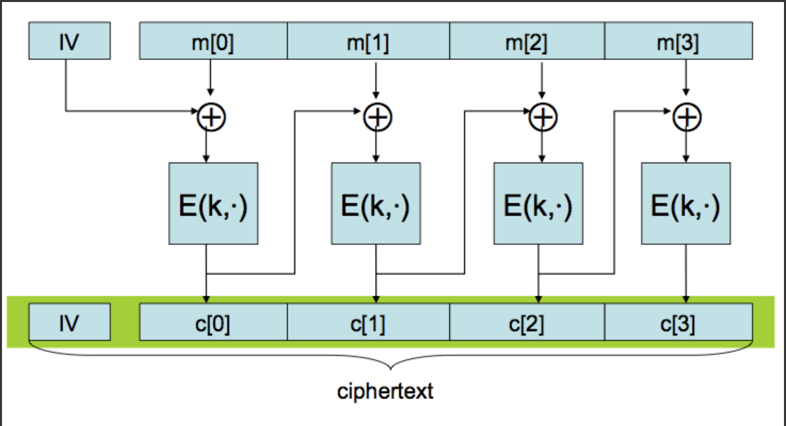
corollary. given the same plaintext message twice, encryption algorithm must produce different outputs

method. encryptor picks a random nonce (aka IV), changes from message to message

Cipher Block Chaining (CBC) Mode

CBC Mode. using PRP $E : K \times \{0,1\}^{128} \to \{0,1\}^{128}$.

- break message m into 128-bit blocks $(m_0, m_1, m_2, m_3, m_4, \ldots)$



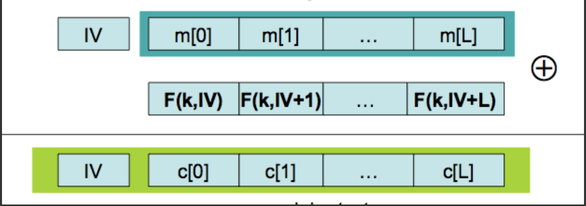
Random Counter Mode

Random Counter Mode. using PRF $F : K \times \{0,1\}^{128} \to \{0,1\}^{128}$.

- break message m into 128-bit blocks $(m_0, m_1, m_2, m_3, m_4, \ldots)$
- $\mathrm{Enc}_k(m)$:

  pick a random IV;

  output $(IV, m_0 \oplus F(k, IV), m_1 \oplus F(k, IV+1), m_2 \oplus F(k, IV+2), \ldots)$



- $\mathrm{Dec}_k(IV, c_0, c_1, \ldots)$ outputs $(c_0 \oplus F(k, IV), c_1 \oplus F(k, IV+1), \ldots)$
- parallelizable (unlike CBC)