Using block ciphers

Review: PRPs and PRFs
Block ciphers: crypto work horse

Canonical examples:
1. 3DES: $n=64$ bits, $k=168$ bits
2. AES: $n=128$ bits, $k=128, 192, 256$ bits
Abstractly: PRPs and PRFs

• Pseudo Random Function (PRF) defined over (K,X,Y):
  
  \[ F: K \times X \rightarrow Y \]

  such that exists “efficient” algorithm to evaluate \( F(k,x) \)

• Pseudo Random Permutation (PRP) defined over (K,X):
  
  \[ E: K \times X \rightarrow X \]

  such that:
  
  1. Exists “efficient” deterministic algorithm to evaluate \( E(k,x) \)
  2. The function \( E(k, \cdot) \) is one-to-one
  3. Exists “efficient” inversion algorithm \( D(k,x) \)
Secure PRFs

• Let $F: \mathbb{K} \times X \rightarrow Y$ be a PRF

\[
Funs[X,Y]: \text{ the set of all functions from } X \text{ to } Y
\]

\[
S_F = \{ F(k, \cdot) \text{ s.t. } k \in \mathbb{K} \} \subseteq Funs[X,Y]
\]

• Intuition: a PRF is **secure** if a random function in $Funs[X,Y]$ is indistinguishable from a random function in $S_F$

Size $|\mathbb{K}|$

Size $|Y|^{|X|}$
Secure PRF: definition

- For $b=0,1$ define experiment $\text{EXP}(b)$ as:
  
  $b$

  $b=0$: $k \leftarrow K$, $f \leftarrow F(k, \cdot)$

  $b=1$: $f \leftarrow \text{Funs}[X,Y]$

  $x_1 \in X$, $x_2$, ..., $x_q$

  $f(x_1)$, $f(x_2)$, ..., $f(x_q)$

- Def: $F$ is a secure PRF if for all “efficient” $A$:

  $$\text{Adv}_{\text{PRF}}[A,F] := \left| \Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1] \right|$$

  is “negligible.”
Secure PRP (secure block cipher)

• For \( b=0,1 \) define experiment \( \text{EXP}(b) \) as:

\[
\begin{align*}
\text{Chal.} & : \quad b=0: \quad k \leftarrow K, \quad f \leftarrow E(k, \cdot) \\
& \quad b=1: \quad f \leftarrow \text{Perms}[X] \\
\text{Adv. A} & : \quad x_1 \in X, x_2, \ldots, x_q \\
& \quad f(x_1), f(x_2), \ldots, f(x_q) \\
& \quad b' \in \{0,1\}
\end{align*}
\]

• Def: \( E \) is a secure PRP if for all “efficient” \( A \):

\[
\text{Adv}_{\text{PRP}}[A,E] = \left| \Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1] \right|
\]

is “negligible.”
Let $X = \{0,1\}$. Perms[$X$] contains two functions

Consider the following PRP:
key space $K=\{0,1\}$, input space $X = \{0,1\}$, PRP defined as:

$E(k,x) = x \oplus k$

Is this a secure PRP?

- Yes
- No
- It depends
Example secure PRPs

- **PRPs believed to be secure:** 3DES, AES, ...

  AES-128: $K \times X \rightarrow X$  where  $K = X = \{0,1\}^{128}$

- An example concrete assumption about AES:

  All $2^{80}$-time algs. $A$ have  $\text{Adv}_{\text{PRP}}[A, AES] < 2^{-40}$
Consider the 1-bit PRP from the previous question:  \( E(k,x) = x \oplus k \)

Is it a secure PRF?

Note that \( \text{Funs}[X,X] \) contains four functions

- Yes
- No
- It depends

Attacker A:
(1) query \( f(\cdot) \) at \( x=0 \) and \( x=1 \)
(2) if \( f(0) = f(1) \) output “1”, else “0”

\[ \text{Adv}_{\text{PRF}}[A,E] = |0-\frac{1}{2}| = \frac{1}{2} \]
PRF Switching Lemma

Any secure PRP is also a secure PRF, if $|X|$ is sufficiently large.

**Lemma:** Let $E$ be a PRP over $(K,X)$

Then for any $q$-query adversary $A$:

$$\left| \text{Adv}_{\text{PRF}}[A,E] - \text{Adv}_{\text{PRP}}[A,E] \right| < \frac{q^2}{2|X|}$$

$\Rightarrow$ Suppose $|X|$ is large so that $q^2 / 2|X|$ is “negligible”

Then $\text{Adv}_{\text{PRP}}[A,E]$ “negligible” $\Rightarrow$ $\text{Adv}_{\text{PRF}}[A,E]$ “negligible”
Final note

• Suggestion:
  – don’t think about the inner-workings of AES and 3DES.

• We assume both are secure PRPs and will see how to use them
End of Segment
Using block ciphers

Modes of operation: one time key

example: encrypted email, new key for every message.
Using PRPs and PRFs

**Goal:** build “secure” encryption from a secure PRP (e.g. AES).

This segment: **one-time keys**

1. Adversary’s power:
   
   Adv sees only one ciphertext (one-time key)

2. Adversary’s goal:
   
   Learn info about PT from CT (semantic security)

Next segment: **many-time keys** (a.k.a chosen-plaintext security)
Incorrect use of a PRP

Electronic Code Book (ECB):

PT:  

\[
\begin{array}{c}
\vdots \\
\text{m}_1 \\
\vdots \\
\text{m}_2 \\
\vdots \\
\text{m} \\
\vdots \\
\end{array}
\]

CT:  

\[
\begin{array}{c}
\vdots \\
\text{c}_1 \\
\vdots \\
\text{c}_2 \\
\vdots \\
\end{array}
\]

Problem:

\[\text{if } \text{m}_1=\text{m}_2 \text{ then } \text{c}_1=\text{c}_2\]
In pictures

An example plaintext

Encrypted with AES in ECB mode

(courtesy B. Preneel)
Semantic Security (one-time key)

**EXP(0):**
- Chal. \( k \leftarrow K \)
- \( m_0, m_1 \in M : \ |m_0| = |m_1| \)
- \( c \leftarrow E(k, m_0) \)
- Adv. A

**EXP(1):**
- Chal. \( k \leftarrow K \)
- \( m_0, m_1 \in M : \ |m_0| = |m_1| \)
- \( c \leftarrow E(k, m_1) \)
- Adv. A

one time key \( \Rightarrow \) adversary sees only one ciphertext

\[
\text{Adv}_{\text{SS}}[A,\text{OTP}] = \left| \Pr[\text{EXP(0)}=1] - \Pr[\text{EXP(1)}=1] \right| \quad \text{should be "neg."}
\]
ECB is not Semantically Secure

ECB is not semantically secure for messages that contain more than one block.

\[
\begin{align*}
    b &\in \{0,1\} \\
    \text{Chal.} \\
    k &\leftarrow K \\
    \text{Two blocks} \\
    m_0 &= \text{“Hello World”} \\
    m_1 &= \text{“Hello Hello”} \\
    (c_1, c_2) &\leftarrow E(k, m_b) \\
    \text{Adv. A} \\
    \text{If } c_1 = c_2 \text{ output 0, else output 1}
\end{align*}
\]

Then \( \text{Adv}_{SS} [A, \text{ECB}] = \)
Secure Construction I

Deterministic counter mode from a PRF $F : \mathbb{K} \times \{0,1\}^* \rightarrow \{0,1\}^*$

- $E_{\text{DETCTR}} (k, m) = \oplus_{i=0}^{L} m_i \oplus F(k,i)$

⇒ Stream cipher built from a PRF (e.g. AES, 3DES)
Det. counter-mode security

**Theorem:** For any $L>0$,

If $F$ is a secure PRF over $(K,X,X)$ then $E_{DETCTR}$ is sem. sec. cipher over $(K,X^L,X^L)$.

In particular, for any eff. adversary $A$ attacking $E_{DETCTR}$ there exists a n eff. PRF adversary $B$ s.t.:

$$\text{Adv}_{SS}[A, E_{DETCTR}] = 2 \cdot \text{Adv}_{PRF}[B, F]$$

$\text{Adv}_{PRF}[B, F]$ is negligible (since $F$ is a secure PRF)
Hence, $\text{Adv}_{SS}[A, E_{DETCTR}]$ must be negligible.
Proof
End of Segment
Example applications:

1. File systems: Same AES key used to encrypt many files.
2. IPsec: Same AES key used to encrypt many packets.
Semantic Security for many-time key

Key used more than once ⇒ adv. sees many CTs with same key

**Adversary’s power:** chosen-plaintext attack (CPA)
- Can obtain the encryption of arbitrary messages of his choice
  (conservative modeling of real life)

**Adversary’s goal:** Break semantic security
Semantic Security for many-time key

$E = (E,D)$ a cipher defined over $(K,M,C)$. For $b=0,1$ define $\text{EXP}(b)$ as:

\begin{align*}
\text{Chal.} & \quad k \leftarrow K \\
\text{Adv.} & \quad m_{1,0}, m_{1,1} \in M : |m_{1,0}| = |m_{1,1}| \\
& \quad c_1 \leftarrow E(k, m_{1,b})
\end{align*}
Semantic Security for many-time key

$E = (E,D)$ a cipher defined over $(K, M, C)$. For $b=0,1$ define $\text{EXP}(b)$ as:

Chal.

$k \leftarrow K$

$m_{2,0}, m_{2,1} \in M : |m_{2,0}| = |m_{2,1}|$

Adv.

c_2 \leftarrow E(k, m_{2,b})$
Semantic Security for many-time key  (CPA security)

\[ E = (E, D) \] a cipher defined over \((K, M, C)\). For \(b=0,1\) define \(\text{EXP}(b)\) as:

\[ \text{Def: } E \text{ is sem. sec. under CPA if for all “efficient” A:} \]

\[ \text{Adv}_{\text{CPA}} [A, E] = \left| \Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1] \right| \text{ is “negligible.”} \]
Ciphers insecure under CPA

Suppose $E(k,m)$ always outputs same ciphertext for msg $m$. Then:

So what? an attacker can learn that two encrypted files are the same, two encrypted packets are the same, etc.

- Leads to significant attacks when message space $M$ is small
Ciphers insecure under CPA

Suppose \( E(k,m) \) always outputs same ciphertext for msg \( m \). Then:

If secret key is to be used multiple times \( \implies \)

given the same plaintext message twice, encryption must produce different outputs.
Solution 1: randomized encryption

- $E(k, m)$ is a randomized algorithm:

\[ \Rightarrow \text{encrypting same msg twice gives different ciphertexts (w.h.p)} \]

\[ \Rightarrow \text{ciphertext must be longer than plaintext} \]

Roughly speaking: $\text{CT-size} = \text{PT-size} + \# \text{random bits}$
Let $F: K \times R \rightarrow M$ be a secure PRF.

For $m \in M$ define $E(k,m) = \left[ r \xleftarrow{\$} R, \text{ output } (r, F(k,r) \oplus m) \right]$

Is $E$ semantically secure under CPA?

- Yes, whenever $F$ is a secure PRF
- No, there is always a CPA attack on this system
- Yes, but only if $R$ is large enough so $r$ never repeats (w.h.p)
- It depends on what $F$ is used
Solution 2: nonce-based Encryption

- nonce \( n \): a value that changes from msg to msg.
  \((k,n)\) pair never used more than once

- **method 1**: nonce is a **counter** (e.g. packet counter)
  – used when encryptor keeps state from msg to msg
  – if decryptor has same state, need not send nonce with CT

- **method 2**: encryptor chooses a **random nonce**, \( n \leftarrow \mathcal{N} \)
CPA security for nonce-based encryption

System should be secure when nonces are chosen adversarially.

Def: nonce-based $E$ is sem. sec. under CPA if for all "efficient" $A$:

$$\text{Adv}_{nCPA} [A, E] = \left| \Pr[\text{EXP}(0) = 1] - \Pr[\text{EXP}(1) = 1] \right|$$

is "negligible."

All nonces $\{n_1, \ldots, n_q\}$ must be distinct.
Let $F: K \times R \rightarrow M$ be a secure PRF. Let $r = 0$ initially.

For $m \in M$ define $E(k,m) = [r++, \text{ output } (r, F(k,r) \oplus m)]$

Is $E$ CPA secure nonce-based encryption?

- Yes, whenever $F$ is a secure PRF
- No, there is always a nonce-based CPA attack on this system
- Yes, but only if $R$ is large enough so $r$ never repeats
- It depends on what $F$ is used
End of Segment
Using block ciphers

Modes of operation: many time key (CBC)

Example applications:

1. File systems: Same AES key used to encrypt many files.
2. IPsec: Same AES key used to encrypt many packets.
Construction 1: CBC with random IV

Let \((E,D)\) be a PRP. 

\[
E: \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n
\]

\[E_{\text{CBC}}(k,m): \text{ choose random } IV \in X \text{ and do: }\]

\[
IV \oplus m[0] \oplus E(k,\cdot) \oplus m[1] \oplus E(k,\cdot) \oplus m[2] \oplus E(k,\cdot) \oplus m[3] \oplus E(k,\cdot)
\]

\[
IV \oplus c[0] \oplus c[1] \oplus c[2] \oplus c[3]
\]

\[\text{ciphertext}\]
Decryption circuit

In symbols: \( c[0] = E(k, IV \oplus m[0]) \) \Rightarrow m[0] = 

\[ \begin{align*}
IV & \quad c[0] & \quad c[1] & \quad c[2] & \quad c[3] \\
\downarrow & \quad \downarrow & \quad \downarrow & \quad \downarrow & \quad \downarrow \\
D(k, \cdot) & \quad D(k, \cdot) & \quad D(k, \cdot) & \quad D(k, \cdot) \\
\downarrow & \quad \downarrow & \quad \downarrow & \quad \downarrow \\
m[0] & \quad m[1] & \quad m[2] & \quad m[3]
\end{align*} \]
CBC: CPA Analysis

CBC Theorem: For any $L>0$,

If $E$ is a secure PRP over $(K,X)$ then $E_{CBC}$ is a sem. sec. under CPA over $(K, X^L, X^{L+1})$.

In particular, for a $q$-query adversary $A$ attacking $E_{CBC}$ there exists a PRP adversary $B$ s.t.:

$$\text{Adv}_{\text{CPA}}[A, E_{CBC}] \leq 2 \cdot \text{Adv}_{\text{PRP}}[B, E] + 2q^2L^2 / |X|$$

Note: CBC is only secure as long as $q^2L^2 \ll |X|$
An example

\[
\text{Adv}_{\text{CPA}} [A, E_{\text{CBC}}] \leq 2 \cdot \text{PRP Adv}[B, E] + 2 q^2 L^2 / |X|
\]

\(q = \# \text{ messages encrypted with } k\), \(L = \text{ length of max message}\)

Suppose we want \(\text{Adv}_{\text{CPA}} [A, E_{\text{CBC}}] \leq 1/2^{32}\) \iff \(q^2 L^2 / |X| < 1/2^{32}\)

- AES: \(|X| = 2^{128}\) \Rightarrow \(q L < 2^{48}\)
  
  So, after \(2^{48}\) AES blocks, must change key

- 3DES: \(|X| = 2^{64}\) \Rightarrow \(q L < 2^{16}\)
Warning: an attack on CBC with rand. IV

CBC where attacker can predict the IV is not CPA-secure !!

Suppose given \( c \leftarrow E_{CBC}(k,m) \) can predict IV for next message

Chal.

\( k \leftarrow K \)

\[ c_1 \leftarrow [ IV_1, E(k, 0 \oplus IV_1) ] \]

\( 0 \in X \)

Adv.

predict IV

\[ m_0 = IV \oplus IV_1, \quad m_1 \neq m_0 \]

\[ c \leftarrow [ IV, E(k, m_1 \oplus IV) ] \]

output 0 if \( c[1] = c_1[1] \)

Bug in SSL/TLS 1.0: IV for record \#i is last CT block of record \#(i-1)
Construction 1’: nonce-based CBC

- Cipher block chaining with **unique** nonce: key = (k, k₁)
  - unique nonce means: (key, n) pair is used for only one message

\[
\begin{align*}
\text{nonce} & \rightarrow E(k₁, \cdot) \rightarrow m[0] \\
& \rightarrow E(k, \cdot) \rightarrow m[1] \\
& \rightarrow E(k, \cdot) \rightarrow m[2] \\
& \rightarrow E(k, \cdot) \rightarrow m[3] \\
& \rightarrow \oplus \rightarrow c[0] \\
& \rightarrow \oplus \rightarrow c[1] \\
& \rightarrow \oplus \rightarrow c[2] \\
& \rightarrow \oplus \rightarrow c[3] \\
\end{align*}
\]
void AES_cbc_encrypt(
    const unsigned char *in,
    unsigned char *out,
    size_t length,
    const AES_KEY *key,
    unsigned char *ivec,          ← user supplies IV
    AES_ENCRYPT or AES_DECRYPT);

When nonce is non random need to encrypt it before use.
A CBC technicality: padding

TLS: for \( n > 0 \), \( n \) byte pad is removed during decryption

if no pad needed, add a dummy block
End of Segment
Using block ciphers

Modes of operation: many time key (CTR)

Example applications:

1. File systems: Same AES key used to encrypt many files.
2. IPsec: Same AES key used to encrypt many packets.
Construction 2: rand ctr-mode

Let $F: K \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a secure PRF.

$E(k,m)$: choose a random $IV \in \{0,1\}^n$ and do:

\[
\begin{align*}
\text{msg} & \quad \begin{array}{cccc}
IV & m[0] & m[1] & \ldots & m[L] \\
\end{array} \\
\hline
F(k,IV) & F(k,IV+1) & \ldots & F(k,IV+L) \\
\hline
\text{ciphertext} & \begin{array}{cccc}
IV & c[0] & c[1] & \ldots & c[L] \\
\end{array}
\end{align*}
\]

note: parallelizable (unlike CBC)
## Construction 2’: nonce ctr-mode

To ensure $F(k,x)$ is never used more than once, choose $IV$ as:

$IV$: 

<table>
<thead>
<tr>
<th>nonce</th>
<th>counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>64 bits</td>
<td>64 bits</td>
</tr>
</tbody>
</table>

$IV$ starts at 0 for every msg.
rand ctr-mode (rand. IV): CPA analysis

- **Counter-mode Theorem:** For any $L>0$,
  
  If $F$ is a secure PRF over $(K,X,X)$ then
  
  $E_{CTR}$ is a sem. sec. under CPA over $(K,X^L,X^{L+1})$.

  In particular, for a $q$-query adversary $A$ attacking $E_{CTR}$
  there exists a PRF adversary $B$ s.t.:
  
  $$\text{Adv}_{\text{CPA}}[A, E_{CTR}] \leq 2 \cdot \text{Adv}_{\text{PRF}}[B, F] + 2 \cdot \frac{q^2 L}{|X|}$$

  **Note:** ctr-mode only secure as long as $q^2 L << |X|$. Better than CBC!
An example

\[ \text{Adv}_{\text{CPA}} [A, E_{\text{CTR}}] \leq 2 \cdot \text{Adv}_{\text{PRF}} [B, E] + 2 q^2 L / |X| \]

\( q = \# \) messages encrypted with \( k \), \( L = \) length of max message

Suppose we want \( \text{Adv}_{\text{CPA}} [A, E_{\text{CTR}}] \leq 1/2^{32} \iff q^2 L / |X| < 1/2^{32} \)

- **AES:** \( |X| = 2^{128} \implies q L^{1/2} < 2^{48} \)

So, after \( 2^{32} \) CTs each of len \( 2^{32} \), must change key

(total of \( 2^{64} \) AES blocks)
## Comparison: ctr vs. CBC

<table>
<thead>
<tr>
<th></th>
<th>CBC</th>
<th>ctr mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>uses</td>
<td>PRP</td>
<td>PRF</td>
</tr>
<tr>
<td>parallel processing</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Security of rand. enc.</td>
<td>$q^2 L^2 \ll</td>
<td>X</td>
</tr>
<tr>
<td>dummy padding block</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>1 byte msgs (nonce-based)</td>
<td>16x expansion</td>
<td>no expansion</td>
</tr>
</tbody>
</table>

(for CBC, dummy padding block can be solved using ciphertext stealing)
Summary

- PRPs and PRFs: a useful abstraction of block ciphers.

- We examined two security notions: (security against eavesdropping)
  1. Semantic security against one-time CPA.
  2. Semantic security against many-time CPA.

Note: neither mode ensures data integrity.

- Stated security results summarized in the following table:

<table>
<thead>
<tr>
<th>Goal</th>
<th>Power</th>
<th>one-time key</th>
<th>Many-time key (CPA)</th>
<th>CPA and integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sem. Sec.</td>
<td>steam-ciphers</td>
<td>steam-ciphers det. ctr-mode</td>
<td>rand CBC</td>
<td>later</td>
</tr>
<tr>
<td></td>
<td>det. ctr-mode</td>
<td>rand ctr-mode</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Further reading


• Nonce-Based Symmetric Encryption, P. Rogaway, FSE 2004
End of Segment