1. Abstract block ciphers: PRPs and PRFs,
2. Security models for encryption,
3. Analysis of CBC and counter mode
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” algorithm to evaluate \( E(k,x) \)
  2. The function \( E( k, \cdot ) \) is one-to-one
  3. Exists “efficient” inversion algorithm \( D(k,x) \)
Running example

- **Example PRPs:** 3DES, AES, ...

  - **AES-128:** \( K \times X \rightarrow X \) where \( K = X = \{0,1\}^{128} \)
  
  - **DES:** \( K \times X \rightarrow X \) where \( X = \{0,1\}^{64}, K = \{0,1\}^{56} \)
  
  - **3DES:** \( K \times X \rightarrow X \) where \( X = \{0,1\}^{64}, K = \{0,1\}^{168} \)

- Functionally, any PRP is also a PRF.
  - A PRP is a PRF where \( X=Y \) and is efficiently invertible
  - A PRP is sometimes called a **block cipher**
Secure PRFs

- Let $F: K \times X \rightarrow Y$ be a PRF
  
  \[
  \begin{align*}
  \text{Funs}[X,Y]: & \quad \text{the set of all functions from } X \text{ to } Y \\
  S_F = & \{ F(k, \cdot) \text{ s.t. } k \in K \} \subseteq \text{Funs}[X,Y]
  \end{align*}
  \]

- **Intuition**: a PRF is **secure** if a random function in $\text{Funs}[X,Y]$ is indistinguishable from a random function in $S_F$
Secure PRFs

- Let \( F: K \times X \rightarrow Y \) be a PRF

\[
\begin{align*}
\text{Funs}[X,Y]: & \quad \text{the set of all functions from } X \text{ to } Y \\
S_F = \{ F(k,\cdot) \text{ s.t. } k \in K \} & \subseteq \text{Funs}[X,Y]
\end{align*}
\]

- **Intuition:** a PRF is **secure** if a random function in \( \text{Funs}[X,Y] \) is indistinguishable from a random function in \( S_F \)
Secure PRF: definition

- For \( b=0,1 \) define experiment \( EXP(b) \) as:

  \[ \text{Def: } F \text{ is a secure PRF if for all “efficient” } A: \]

  \[
  Adv_{PRF}[A,F] = \left| \Pr[EXP(0)=1] - \Pr[EXP(1)=1] \right|
  \]

  is “negligible.”
Secure PRP

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

\[
\text{Def: } E \text{ is a secure PRP if for all "efficient" } A: \\
\text{Adv}_{PRP}[A,E] = \left| \Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1] \right|
\]
is “negligible.”
Example secure PRPs

• **Example secure PRPs:** 3DES, AES, ...

  \( AES_{256} : K \times X \rightarrow X \) where \( X = \{0,1\}^{128} \)

  \( K = \{0,1\}^{256} \)

• **AES\textsubscript{256} PRP Assumption** (example):

  All explicit \( 2^{80} \)-time algs A have \( \text{PRP Adv}[A, AES_{256}] < 2^{-40} \)
PRF Switching Lemma

Any secure PRP is also a secure PRF.

**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 $\frac{q^2}{2|X|}$ is “negligible”

Then $\text{Adv}_{\text{PRP}}[A,E]$ “negligible” $\Rightarrow$ $\text{Adv}_{\text{PRF}}[A,E]$ “negligible”
Using PRPs and PRFs

- **Goal**: build “secure” encryption from a PRP.

- Security is always defined using two parameters:

  1. **What “power” does adversary have?**
     - Adv sees only one ciphertext (one-time key)
     - Adv sees many PT/CT pairs (many-time key, CPA)

  2. **What “goal” is adversary trying to achieve?**
     - Fully decrypt a challenge ciphertext.
     - Learn info about PT from CT (semantic security)
Incorrect use of a PRP

Electronic Code Book (ECB):

PT: \[ m_1 \quad m_2 \quad - \quad - \quad - \quad - \quad - \]

CT: \[ c_1 \quad c_2 \quad - \quad - \quad - \quad - \quad - \]

Problem:

– if \( m_1 = m_2 \) then \( c_1 = c_2 \)
In pictures

An example plaintext

Encrypted with AES in ECB mode

(courtesy B. Preneel)
Modes of Operation for One-time Use Key

**Example application:**
- Encrypted email. New key for every message.
Semantic Security for one-time key

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

```
Def: $E$ is sem. sec. for one-time key if for all “efficient” $A$:

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

is “negligible.”
Semantic security (cont.)

Sem. Sec. \(\Rightarrow\) no “efficient” adversary learns info about PT from a **single** CT.

Example: suppose efficient A can deduce LSB of PT from CT. Then \(E = (E,D)\) is not semantically secure.

Then \(\text{Adv}_{\text{SS}}[B, E] = 1\) \(\Rightarrow\) \(E\) is not sem. sec.
Note: ECB is not Sem. Sec.

ECB is not semantically secure for messages that contain two or more blocks.

If \( c_1 = c_2 \) output 0, else output 1

Then \( \text{Adv}_{SS}[A, \text{ECB}] = 1 \)
Secure Constructions

Examples of sem. sec. systems:

1. $\text{Adv}_{\text{SS}}[A, \text{OTP}] = 0$ for all $A$

2. Deterministic counter mode from a PRF $F$:
   - $E_{\text{DETCTR}}(k,m) =$
   - $m[0]$ $m[1]$ $\ldots$ $m[L]$
     $\oplus$
   - $F(k,0)$ $F(k,1)$ $\ldots$ $F(k,L)$
     $\underline{c[0]}$ $c[1]$ $\ldots$ $c[L]$

   - Stream cipher built from 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 adversary \( A \) attacking \( E_{DETCTR} \) there exists a 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)

\[\Rightarrow\] \( \text{Adv}_{SS}[A, E_{DETCTR}] \) must be negligible.
Modes of Operation for Many-time Key

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 (CPA security)

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

- Chal.
  - $k \leftarrow K$
  - for $i=1,\ldots,q$:
    - $m_{i,0}, m_{i,1} \in M : |m_{i,0}| = |m_{i,1}|$
    - $c_i \leftarrow E(k, m_{i,b})$
  - $c = E(k, m)$
  - if adv. wants $c = E(k, m)$ it queries with $m_{j,0} = m_{j,1} = m$

- Adv.
  - $b' \in \{0,1\}$

Def: $E$ is sem. sec. under CPA if for all “efficient” $A$:

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

is “negligible.”
Security for many-time key

Fact: stream ciphers are insecure under CPA.

- More generally: if $E(k,m)$ always produces same ciphertext, then cipher is insecure under CPA.

If secret key is to be used multiple times $\Rightarrow$

given the same plaintext message twice, the encryption alg. must produce different outputs.
**Nonce-based Encryption**

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

- **method 1**: encryptor chooses a random nonce, $n \leftarrow \mathcal{N}$
- **method 2**: 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
Construction 1: CBC with random nonce

Cipher block chaining with a random IV \( (IV = \text{nonce}) \)

\[
\text{IV} \quad m[0] \quad m[1] \quad m[2] \quad m[3]
\]

\[
E(k, \cdot) \quad E(k, \cdot) \quad E(k, \cdot) \quad E(k, \cdot)
\]

\[
\text{IV} \quad c[0] \quad c[1] \quad c[2] \quad c[3]
\]

ciphertext

note: CBC where attacker can predict the IV is not CPA-secure. HW.
CBC: CPA Analysis

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

If $E$ is a secure PRP over $(K,X)$ then $E_{CBC}$ is a semi-secure 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.:

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

**Note:** CBC is only secure as long as $q^2L^2 << |X|$
Construction 1’: CBC with **unique** nonce

Cipher block chaining with **unique** IV \( (IV = \text{nonce}) \)

unique IV means: \( (\text{key}, \text{IV}) \) pair is used for only one message

![Diagram of CBC with unique nonce](image-url)

- \( \text{IV} \)
- \( m[0] \)
- \( m[1] \)
- \( m[2] \)
- \( m[3] \)
- \( \oplus \)
- \( E(k_2, \cdot) \)
- \( E(k_1, \cdot) \)
- \( \oplus \)
- \( \oplus \)
- \( \oplus \)
- \( \text{IV}' \)
- \( \text{ciphertext} \)
- \( \oplus \)
- \( \oplus \)
- \( \oplus \)
- \( \oplus \)

Included only if unknown to decryptor
A CBC technicality: padding

TLS 1.0: for $n > 0$, $n+1$ byte pad is
if no pad needed, add a dummy block

removed during decryption
Construction 2: rand ctr-mode

IV - chosen at random for every message

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

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

IV:
- nonce: 96 bits
- counter: 32 bits

starts at 0 for every msg
rand ctr-mode: CPA analysis

Randomized counter mode: random IV.

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.:

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

Note: ctr-mode only secure as long as $q^2L \ll |X|$  

Better than CBC!
An example

\[
\text{Adv}_{\text{CPA}}[A, E_{\text{CTR}}] \leq 2 \cdot \text{Adv}_{\text{PRF}}[B, E] + 2 \frac{q^2 L}{|X|} \leq \frac{1}{2^{32}}
\]

q = \# messages encrypted with k, \quad L = \text{length of max msg}

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

- AES: \( |X| = 2^{128} \Rightarrow q L^{1/2} < 2^{48} \)
  
  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 &lt;&lt;</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 avoided using *ciphertext stealing*
Summary

PRPs and PRFs: a useful abstraction of block ciphers.

We examined two security notions:

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 CT integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sem. Sec.</td>
<td>steam-ciphers det. ctr-mode</td>
<td>rand CBC rand ctr-mode</td>
<td>later</td>
<td></td>
</tr>
</tbody>
</table>