Thus, for PRP/PRF in "counter mode" gives us a stream cipher (one-time encryption scheme) typically, the IV is divided into a nonce (value that does not repeat) and a counter: IV = nonce + counter

How do we reuse it? Choose a random starting point (called an initialization vector) "randomized counter mode"

<table>
<thead>
<tr>
<th>( m_1 )</th>
<th>( m_2 )</th>
<th>( m_3 )</th>
<th>( m_4 )</th>
</tr>
</thead>
</table>

divide message into blocks (based on block size of PRF)

\[
\begin{array}{c|c|c|c}
IV & F(k, IV) & F(k, IV_2) & F(k, IV_3) \\
\end{array}
\]

observe: ciphertext is longer than the message (required for CPA security)

Theorem: Let \( F: \mathbb{K} \times \mathbb{X} \rightarrow \mathbb{Y} \) be a secure PRF and let \( T_{lctr} \) denote the randomized counter mode encryption scheme from above for \( l \)-block messages \( (M = \mathbb{X}^l) \). Then, for all efficient CPA adversaries \( A \), there exists an efficient PRF adversary \( B \) such that

\[
\text{CPAAdv}[A, T_{lctr}] \leq \frac{4Q^2l}{\mathbb{X}^l} + 2 \cdot \text{PRFAdv}[B, F]
\]

\( Q \): number of encryption queries

\( l \): number of blocks in message

Intuition:

1. If there are no collisions (i.e., PRF never evaluated on the same block), then it is as if everything is encrypted under a fresh one-time pad.

2. Collision event: \( (X, X+1, \ldots, X+l-1) \) overlaps with \( (X', X'+1, \ldots, X'+l-1) \) when \( X, X' \in \mathbb{X} \)

\[
\mathbb{P}[X = X'] \leq \frac{2l}{\mathbb{X}^l}
\]

\( \mathbb{P} \): probability that \( X' \) lies in this interval is \( \leq \frac{2l}{\mathbb{X}^l} \)

There are \( \leq Q^2 \) possible pairs \((X, X')\), so by a union bound,

\[
\Pr[\text{collision}] \leq \frac{2lQ^2}{\mathbb{X}^l}
\]

3. Remaining factor of 2 in advantage due to intermediate distribution (hybrid argument):

\[
\begin{align*}
\text{Encrypt } m_0 \text{ with PRF} & \Rightarrow \text{PRFAdv}[B, F] + \frac{4Q^2}{\mathbb{X}^l} \\
\text{Encrypt } m_0 \text{ with fresh one-time pad} & \Rightarrow 0 \\
\text{Encrypt } m, \text{ with fresh one-time pad} & \Rightarrow 0 \\
\text{Encrypt } m_1 \text{ with PRF} & \Rightarrow \text{PRFAdv}[B, F] + \frac{2lQ^2}{\mathbb{X}^l}
\end{align*}
\]

Interpretation: If \( \mathbb{X}^l = 2^{64} \) (e.g., AES), and messages are 1 MB long \((2^{16} \text{ blocks})\) and we want the distinguishing advantage to be below \( 2^{-32} \), then we can use the same key to encrypt

\[
Q \leq \sqrt{\frac{4Q^2l}{\mathbb{X}^l}} = \sqrt{\frac{2^{16}}{2^{64}}} = \sqrt{2^{18}} = 2^{9} \approx 1 \text{ trillion messages!}
\]
Nonce-based counter mode: divide IV into two pieces: IV = nonce || counter

\[ \text{value that does not repeat} \]

common choices: 64-bit nonce, 64-bit counter \} only nonce needs to be sent!
96-bit nonce, 32-bit counter \} (slightly smaller ciphertexts)

Only requirement for security is that IV does not repeat:
- Option 1: Choose randomly (either IV or nonce)
- Option 2: If sender and recipient have shared state (e.g., packet counter), can just use a counter, in which case, IV/nonce does not have to be sent

Counter mode is parallelizable, simple-to-implement, just requires PRF — preferred mode of using block ciphers

Other block cipher modes of operation:

Cipher-block chaining (CBC): common mode in the past (e.g., TLS 1.0, still widely used today)

\[ m_1 \xrightarrow{F(k,:)} c_1 \quad m_2 \xrightarrow{F(k,:)} c_2 \quad m_3 \xrightarrow{F(k,:)} c_3 \]

\[ \text{Encryption} \quad \text{IV} \quad \text{ciphertext} \quad \text{counter} \]

\[ c_1 \xrightarrow{F^{-1}(k,:)} m_1 \quad c_2 \xrightarrow{F^{-1}(k,:)} m_2 \quad c_3 \xrightarrow{F^{-1}(k,:)} m_3 \]

\[ \text{Decryption} \]

Theorem: Let \( F: \mathbb{K} \times \mathbb{X} \rightarrow \mathbb{Y} \) be a secure PRF and let T\text{CBC} denote the CBC encryption scheme for \( l \)-block messages (\( M = \mathbb{X}^l \)). Then, for all efficient CPA adversaries \( A \), there exists an efficient PRF adversary \( B \) such that

\[ \text{CPAAdv}[A, T\text{CBC}] \leq \frac{2^l}{1X1} + 2 \cdot \text{PRFAdv}[B, F] \]

\( Q \): number of encryption queries
\( l \): number of blocks in message

Intuition: Similar to analysis of randomized counter mode:

1. Ciphertext is indistinguishable from random string if PRP is evaluated on distinct inputs
2. When encrypting, PRP is invoked on \( l \) random blocks: so after \( Q \) queries, we have \( Ql \) random blocks.
   \[ \Rightarrow \text{Collision probability} \leq \frac{2^l}{1X1} \]
   \[ \text{this is larger than collision prob} \] for randomized counter mode by a factor of \( \frac{Q}{l} \) [overlap of \( Q \) random intervals vs. \( Ql \) random points]
3. Factor of 2 arises for same reason as before

Interpretation: CBC mode provides weaker security compared to counter mode:

Concretely, for same parameters as before (1 MB messages, \( 2^{-12} \) distinguishing advantage):

\[ Q \leq \sqrt{1X1 \cdot 2^{32}} = \sqrt{2^{32} = 2^{16} = 2^{31.5} \text{ (n 1 billion messages)}} \]

\[ \Rightarrow 2^{25} \sim 180x \text{ smaller than using counter mode} \]
Padding in CBC mode: each ciphertext block is computed by feeding a message block into the PRP

\[ \Rightarrow \text{message must be an even multiple of the block size} \]

\[ \Rightarrow \text{when used in practice, need to pad messages} \]

Can we pad with zeroes? Cannot decrypt! What if original message ended with a bunch of zeroes?

Requirement: padding must be invertible.

CBC padding in TLS 1.0: if k bytes of padding is needed, then append k bytes to the end, with each byte set to k-1 (for AES-CBC)

\[ \text{if } 0 \text{ bytes of padding is needed, then append a block of 16 bytes, with each byte equal to } 15 \]

\[ \text{and a dummy block needed to ensure padding is invertible} \]

\[ \Rightarrow \text{called PKCS#5/PKCS#7 (public-key cryptography standards)} \]

Need to pad in CBC encryption can be exploited in “padding oracle” attacks

Padding in CBC can be avoided using Idea called “cipher text stealing” (as long as messages are more than 1 block)

Comparing CTR mode to CBC mode:

CTR mode

1. no padding needed (shorter ciphertexts)

2. parallelizable

3. only requires PRF (no need to invert)

4. tighter security

5. IVs have to be non-repeating (and spaced far apart)

CBC mode

1. padding needed

2. sequential

3. requires PRF

4. less tight security

5. requires unpredictable IVs

\[ \text{easy to implement: } \begin{cases} \text{IV: nonce} \oplus \text{counter} \oplus \text{k} \end{cases} \]

\[ \Rightarrow \text{only needs to be non-repeating (can be predictable)} \]

Bottom-line: use randomized or nonce-based counter mode whenever possible: simpler, easier, and better than CBC!

A tempting and bad way to use a block cipher: ECB mode (electronic codebook)

\[ \begin{array}{ccc}
  m_1 & \rightarrow & F(k_1) \\
  \downarrow & & \downarrow \\
  m_2 & \rightarrow & F(k_1) \\
  \downarrow & & \downarrow \\
  m_3 & \rightarrow & F(k_1) \\
  \downarrow & & \downarrow \\
  C_1 & \rightarrow & C_2 \\
  \downarrow & & \downarrow \\
  C_2 & \rightarrow & C_3 \\
  \end{array} \]

\[ \Rightarrow \text{Scheme is deterministic! Cannot be CPA secure!} \]

\[ \Rightarrow \text{Not even semantically secure! } (m_0, m_0) \text{ vs. } (m_0, m_1) \text{ were } m \oplus m_0 \]

\[ \Rightarrow \text{Cipher text blocks output are same} \]

\[ \Rightarrow \text{Cipher text blocks output are different} \]

Encryption: Simply apply block cipher to each block of the message

Decryption: Simply invert each block of the ciphertext

\[ \text{NEVER USE ECB MODE FOR ENCRYPTION!} \]