Outline

Encrypting many messages

MACs

Message Authentication Code
• Participation credit begins today.

• You get a point each time you ask an interesting question or answer a question that I ask or answer a question well on piazza.

• If you get 5 or more points, you get 100% participation credit.

• Scribe volunteer? Claire
Encrypting large messages
Many-time Encryption, Soln 1: PRF

Let \( F: K \times R \rightarrow M \) be a secure PRF.

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

Is \( \text{Enc} \) semantically secure under CPA?

To encrypt \( m \), output
\[
ct = (r, \text{PRF}(k, r) \oplus m).
\]
Adaptive Games:

\[ m_0 \neq m_i \Rightarrow (m_0, m_i)_2 \neq (m_0, m_i)_2 \]

many - msg

---

H.W. Prove that \((E, D)\) where

\[ E(k, m) = (r, \text{PRF}(k, r) \oplus m) \]

\[ D(k, (c_1, c_2)) = \text{PRF}(k, c_1) \oplus c_2 \]

is adaptive many-time secure.
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**: nonce is **random**  
  [File Encryption]
CBC (Cipher Block Chaining) mode

Let \((E,D)\) be a PRP. \(E_{\text{CBC}}(k,m): \) choose \textcolor{red}{\textbf{random}} Initialization Vector and do:

\[
\begin{align*}
m & = m[0] \| m[1] \| m[2] \| m[3] \ldots, \\
\text{Initialization value} & \approx 128 \text{ bits}, \\
\text{m[0]} @ IV & \approx 128 \text{ bits}, \\
\end{align*}
\]

\begin{itemize}
  \item E(k,) \hspace{1cm} E(k,) \hspace{1cm} E(k,) \hspace{1cm} E(k,)
  \end{itemize}

\[
\begin{align*}
\text{ciphertext} & \approx 128 \text{ bits}, \\
\text{Enc is not parallelizable}, \\
\end{align*}
\]
Decryption Circuit

In symbols: \( c[0] = E(k, IV \oplus m[0]) \Rightarrow m[0] = D(k, c[0]) \oplus IV \)
CPA Security of CBC

• **CBC Theorem:** For small enough $L > 0$,
  If $E$ is a secure PRP over $(K,X)$ then $E_{CBC}$ is CPA-secure over $(K, X^L, X^{L+1})$.

  (adaptive, many-time)

• In particular, security error in CBC = $(2 \times \text{sec. error in PRP}) + (q^2L^2/|X|)$

• What if IV was predictable? Is it still CPA-secure?

Bug in SSL/TLS 1.0: IV for record #i is last CT block of record #(i-1)
What happens if adversary can predict IV

Adaptive, many-msg games

ch

K = K

Game

\text{Enc}(K, m_0^{(1)})

\text{Enc}(K, m_0^{(2)})

m_0^{(1)}

m_0^{(2)}

m_{i}^{(1)}

m_{i}^{(2)}

Adv

\text{Enc}(k, m_{i}^{(1)})

\text{Enc}(k, m_{i}^{(2)})

m_{i}^{(1)}

m_{i}^{(2)}

m_{i}^{(2)}
What happens if adversary can predict IV

CBC - mode

Adaptive, many - msg games

Game,

\[ \text{ch} \]

\[ k \leftarrow K \]

\[ m_0 \leftarrow IV_1 \uparrow \]

\[ m_1 \leftarrow E(k, IV_1) \]

\[ m_0 \leftarrow IV_1 \oplus IV_2 \]

\[ m_1 \leftarrow E(k, IV_2) \]

Same? 

Game,

\[ 0, 0 \]

\[ IV_1, E(k, IV_1) \]

\[ m_0^{(2)} \]

\[ m_1^{(2)} \]

\[ m_0^{(2)} \leftarrow IV_1 \oplus IV_2 \]

\[ m_1^{(2)} \leftarrow E(k, IV_2) \]
CBC (Cipher Block Chaining) mode: Version 2

- Cipher block chaining with **unique** nonce: \( \text{key} = (k,k_1) \)

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

(1) Can use PRF instead of PRP and (2) is parallelizable.
Message Integrity: MACs
Goal: Integrity (not secrecy)
Shared key setting

MAC = (S, V) is a pair of algorithms that satisfy:

1. **CORRECTNESS.** \( V(k, m, tag) = 1 \) when \( tag = S(k, m) \)
MAC = (S,V) is a pair of algorithms that satisfy:

2. **SECURITY.** Attacker unable to compute \((m’, \text{tag’})\) different from \((m, \text{tag})\) such that \(V (k, m, \text{tag’}) = 1\)
Shared key setting: security of MACs

Security, more generally:

• Attacker can demand tags \((t_1, t_2, \ldots, t_n)\) for messages \((m_1, m_2, \ldots, m_n)\)

• Attacker wins if it outputs \((m', \text{tag}')\) not in \{\((m_1, t_1), (m_2, t_2), \ldots, (m_n, t_n)\)\} such that \(V(k, m', \text{tag}') = 1\)
How do you build a secure MAC?

- Say *k* is a PRF key

\[ \text{tag} = S(k, m) \]

\[ V(k, m, \text{tag}) = \text{acc/rej} \]
How do you build a secure MAC?

• Say *k* is a PRF key

• $S(k, m) = PRF(k, m)$

• $V(k, m, \text{tag}) = 1 \; \text{if and only if} \; \text{tag} = PRF(k, m)$

• Correctness?
How do you build a secure MAC?

• $S(k, m) = PRF(k, m)$
• $V(k, m, \text{tag}) = 1$ \textit{if and only if} \text{tag} = PRF(k, m)

• Security?
Examples

• AES: MAC for 64-bit messages

• What about larger messages?

• For larger messages, we use:
  • CBC-MAC
  • HMAC
Encrypted CBC-MAC

\[
\begin{align*}
F(k, \cdot) & \quad \quad F(k, \cdot) & \quad \quad F(k, \cdot) & \quad \quad F(k, \cdot) \\
\oplus & \quad \quad \oplus & \quad \quad \oplus & \quad \quad \oplus \\
\tag & \quad \quad \text{tag}
\end{align*}
\]
What happens if we remove encryption step?

Obtain tag for m, then get \( t = F(k, m) \)

Output forgery \((m', t')\) where \( m' = (m | |(t \oplus m)) \) and \( t' = t \).
What if message length is not a multiple of block size?

![Diagram showing the XOR operation between four blocks of a message and the final output block.]
First idea?
Need invertible padding!

For security, padding must be invertible!

\[ m_0 \neq m_1 \Rightarrow \text{pad}(m_0) \neq \text{pad}(m_1) \]

Pad with “1000...00”. Add new dummy block if needed.

- The “1” indicates beginning of pad.
Need invertible padding!

For security, padding must be invertible!

\[ m_0 \neq m_1 \implies \text{pad}(m_0) \neq \text{pad}(m_1) \]

Pad with “1000…00”. Add new dummy block if needed.

- The “1” indicates beginning of pad.