Lecture 14
Block Ciphers: Modes of Operations

Zhiqiang Lin
Zhiqiang.lin@utdallas.edu
The University of Texas at Dallas

March 21st, 2016
Processing with Block Ciphers

• Most ciphers work on blocks of fixed (small) size
• How to encrypt long messages?

• Modes of operation
  – ECB (Electronic Code Book)
  – CBC (Cipher Block Chaining)
  – OFB (Output Feedback)
  – CFB (Cipher Feedback)
  – CTR (Counter)
Issues for Block Modes
Issues for Block Modes

• Information leakage
  – Does it reveal info about the plaintext blocks?
Issues for Block Modes

• **Information leakage**
  – Does it reveal info about the plaintext blocks?

• **Ciphertext manipulation**
  – Can an attacker *modify/rearrange* ciphertext block(s) in a way that will produce a *predictable/desired change* in the decrypted plaintext block(s)?

  – Note: assume the *structure* of the plaintext is known, e.g., first block is employee #1 salary, second block is employee #2 salary, etc.
Issues... (Cont’d)
Issues... (Cont’d)

• **Parallel/Sequential**
  – Can blocks of plaintext (ciphertext) be encrypted (decrypted) in parallel?
Issues... (Cont’d)

• **Parallel/Sequential**
  – Can blocks of plaintext (ciphertext) be encrypted (decrypted) in parallel?

• **Error propagation**
  – If there is an error in a plaintext (ciphertext) block, will there be an encryption (decryption) error in more than one ciphertext (plaintext) block?
Agenda

• ECB (Electronic Code Book)
• CBC (Cipher Block Chaining)
• OFB (Output Feedback)
• CFB (Cipher Feedback)
• CTR (Counter)
Electronic Code Book (ECB)
Electronic Code Book (ECB)

Plaintext $\Rightarrow$  $M_1$  $M_2$  $M_3$  $M_4$

64 64 64 46 + padding
Electronic Code Book (ECB)

Plaintext $\Rightarrow M_1$ $\Rightarrow M_2$ $\Rightarrow M_3$ $\Rightarrow M_4$

$\begin{array}{cccc}
\text{64} & \text{64} & \text{64} & \text{46 + padding} \\
\text{E} & \text{E} & \text{E} & \text{E} \\
\end{array}$
Electronic Code Book (ECB)

Plaintext ⇒ $M_1$ $M_2$ $M_3$ $M_4$

Key

$E$ $E$ $E$ $E$

64 64 64 46 + padding

⇒
Electronic Code Book (ECB)

Plaintext $\Rightarrow$ M₁ $\Rightarrow$ M₂ $\Rightarrow$ M₃ $\Rightarrow$ M₄

Key

Ciphertext $\Rightarrow$ C₁ $\Rightarrow$ C₂ $\Rightarrow$ C₃ $\Rightarrow$ C₄

64

64

64

64

46 + padding
Electronic Code Book (ECB)

- The easiest mode of operation; each block is independently encrypted
ECB Decryption

Key

M_1 \rightarrow D \rightarrow M_2 \rightarrow D \rightarrow M_3 \rightarrow D \rightarrow M_4

C_1 \rightarrow 64 \rightarrow D \rightarrow 64 \rightarrow C_2 \rightarrow 64 \rightarrow D \rightarrow 64 \rightarrow C_3 \rightarrow 64 \rightarrow D \rightarrow 64 \rightarrow C_4

46 + padding
Each block is independently decrypted
Electronic Code Book (ECB) Mode

PT: $\begin{array}{cccccc} m_1 & m_2 & m_3 & m_4 & m_5 & \cdots & m_n \end{array}$

E($k, m_i$) $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$

CT: $\begin{array}{cccccc} c_1 & c_2 & c_3 & c_4 & c_5 & \cdots & c_n \end{array}$
Electronic Code Book (ECB) Mode

PT: $m_1 \quad m_2 \quad m_3 \quad m_4 \quad m_5 \quad \cdots \quad m_n$

$E(k, m_i)$ ↓ ↓ ↓ ↓ ↓

CT: $c_1 \quad c_2 \quad c_3 \quad c_4 \quad c_5 \quad \cdots \quad c_n$

Problem:
Electronic Code Book (ECB) Mode

Problem:

\[ m_1 = m_2 \rightarrow c_1 = c_2 \]
What can possibly go wrong?

Plaintext  Ciphertext

Images from Wikipedia
What can possibly go wrong?

Plaintext

Ciphertext

Images from Wikipedia
In pictures

An example plaintext

Encrypted with AES in ECB mode

(courtesy B. Preneel)
ECB Properties

Key -> D -> M_1 -> C_1
D -> M_2 -> C_2
D -> M_3 -> C_3
D -> M_4 -> C_4 (46 + padding)
ECB Properties

• Does information leak?
ECB Properties

• Does information leak?
• Can ciphertext be manipulated profitably?
ECB Properties

- Does information leak?
- Can ciphertext be manipulated profitably?
ECB Properties

- Does information leak?
- Can ciphertext be manipulated profitably?
- Parallel processing possible?
ECB Properties

- Does information leak?
- Can ciphertext be manipulated profitably?
- Parallel processing possible?
- Do ciphertext errors propagate?
Recap: ECB

Blockcipher

Encrypt one block of n-bit length plaintext into one block of n-bits of cipher text (For AES128, n = 128)
Recap: ECB

Blockcipher

Encrypt one block of n-bit length plaintext into one block of n-bits of cipher text (For AES128, n = 128)

Electronic Code Book (ECB) Mode
Block Cipher Modes (ECB)

Plaintext
Block Cipher Modes (ECB)

Plaintext

AES128/ECB
Agenda

- ECB (Electronic Code Book)
- CBC (Cipher Block Chaining)
- OFB (Output Feedback)
- CFB (Cipher Feedback)
- CTR (Counter)
Cipher Block Chaining (CBC)

$M_1$ 64

$M_2$ 64

$M_3$ 64

$M_4$ 46 + padding
Cipher Block Chaining (CBC)

Key

\[E \quad \oplus \quad 64 \quad \oplus \quad 64 \quad \oplus \quad 64 \quad \oplus \quad 46 + \text{padding}\]
Cipher Block Chaining (CBC)

M₁ → E → C₁

M₂ → E → C₂

M₃ → E → C₃

M₄ → E → C₄

Key

64

46 + padding

M₁

M₂

M₃

M₄
Cipher Block Chaining (CBC)

M₁  64  E  64  C₁
M₂  64  E  64  C₂
M₃  64  E  64  C₃
M₄  46 + padding  E  64  C₄

Initialization Vector
Key
Cipher Block Chaining (CBC)

- Chaining dependency: each ciphertext block depends on all preceding plaintext blocks
Initialization Vectors

• **Initialization Vector (IV)**
  – Used along with the key
  – For a given plaintext, changing either the key, or the IV, will produce a different ciphertext

• IV generation and sharing
  – Random; may transmit with the ciphertext
  – Incremental; predictable by receivers
CBC Decryption

Initialization Vector

Key

M_1

M_2

M_3

M_4

46 + padding

C_1

C_2

C_3

C_4
CBC Decryption

- How many ciphertext blocks does each plaintext block depend on?
CBC Properties

• Does information leak?
  – Identical plaintext blocks will produce different ciphertext blocks

• Can ciphertext be manipulated profitably?
  – ???

• Parallel processing possible?
  – no (encryption), yes (decryption)

• Do ciphertext errors propagate?
  – yes (encryption), a little (decryption)
Recap: CBC

Blockcipher

Encrypt one block of n-bit length plaintext into one block of n-bits of cipher text (For AES128, n = 128)
Recap: CBC

Blockcipher

Encrypt one block of n-bit length plaintext into one block of n-bits of cipher text (For AES128, n = 128)
Recap: CBC

Blockcipher

Encrypt one block of n-bit length plaintext into one block of n-bits of cipher text (For AES128, n = 128)
Recap: CBC

Blockcipher

Encrypt one block of n-bit length plaintext into one block of n-bits of cipher text (For AES128, n = 128)
Block Cipher Modes (CBC)

Plaintext
Block Cipher Modes (CBC)

Plaintext  AES128/CBC
Agenda

• ECB (Electronic Code Book)
• CBC (Cipher Block Chaining)
• OFB (Output Feedback)
• CFB (Cipher Feedback)
• CTR (Counter)
Output Feedback Mode (OFB)
Output Feedback Mode (OFB)
Output Feedback Mode (OFB)
Output Feedback Mode (OFB)

Pseudo-Random Number Generator

$M_1 \oplus M_2 \oplus M_3 \oplus M_4$

$C_1, C_2, C_3, C_4$

one-time pad
Output Feedback Mode (OFB)

Initialization Vector

Key

M₁ 64

E

M₂ 64

E

M₃ 64

E

M₄ 46 + padding

E

one-time pad

M₁ 64

C₁

M₂ 64

C₂

M₃ 64

C₃

M₄ 64

C₄
OFB Decryption

Key

IV

64

E

C

M

64

64

64

64

64

64

64

64

46 + padding

one-time pad
OFB Decryption

No block decryption required!
OFB Properties

• Does information leak?
  – identical plaintext blocks produce different ciphertext blocks

• Can ciphertext be manipulated profitably?
  – ???

• Parallel processing possible?
  – no (generating pad), yes (XORing with blocks)

• Do ciphertext errors propagate?
  – ???
OFB ... (Cont’d)

• OFB Advantages
  – Allow pre-computing of pseudo-random stream (One-Time Pad); XOR can be implemented very efficiently
  – Allow in-time encrypt/decrypt due to bit-wise computation (versus the fixed blocks)
• If you know one plaintext/ciphertext pair, can easily derive the one-time pad that was used
  – i.e., should not reuse a one-time pad!
  – Conclusion: IV must be different every time
• Another issue
  – If a bad guy knows the plaintext and ciphertext, can he send arbitrary (valid) messages?
Agenda

• ECB (Electronic Code Book)
• CBC (Cipher Block Chaining)
• OFB (Output Feedback)
• CFB (Cipher Feedback)
• CTR (Counter)
Cipher Feedback Mode (CFB)
Cipher Feedback Mode (CFB)

Key

IV

E

64

M_1

64

64

M_2

64

64

M_3

64

64

M_4

64

46 + padding

64

64

64

64
Cipher Feedback Mode (CFB)

Ciphertext block $C_j$ depends on all preceding plaintext blocks.
CFB Decryption

• No block decryption required!
CFB Properties

• Does information leak?
  – Identical plaintext blocks produce different ciphertext blocks

• Can ciphertext be manipulated profitably?
  – ???

• Parallel processing possible?
  – no (encryption), yes (decryption)

• Do ciphertext errors propagate?
  – ???
Agenda

- ECB (Electronic Code Book)
- CBC (Cipher Block Chaining)
- OFB (Output Feedback)
- CFB (Cipher Feedback)
- CTR (Counter)
Counter mode

\[
\begin{array}{cccccc}
\oplus & m[0] & m[1] & m[2] & \cdots & m[L] \\
F(k,0) & F(k,1) & F(k,2) & \cdots & F(k,L) \\
\end{array}
\]
CTR Mode Properties

• Does information leak?
  – Identical plaintext block produce different ciphertext blocks

• Can ciphertext be manipulated profitably
  – ???

• Parallel processing possible
  – Yes (both generating pad and XORing)

• Do ciphertext errors propagate?
  – ???

• Allow decryption the ciphertext at any location
  – Ideal for random access to ciphertext
Summary

• ECB (Electronic Code Book)
• CBC (Cipher Block Chaining)
• OFB (Output Feedback)
• CFB (Cipher Feedback)
• CTR (Counter)