Modes of Operation

Block vs. Stream Ciphers

Every block of ciphertext is a function of only one corresponding block of plaintext.

Standard modes of operation of block ciphers

<table>
<thead>
<tr>
<th>Block ciphers</th>
<th>Stream ciphers</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECB mode</td>
<td>Counter mode</td>
</tr>
<tr>
<td></td>
<td>OFB mode</td>
</tr>
<tr>
<td></td>
<td>CFB mode</td>
</tr>
<tr>
<td></td>
<td>CBC mode</td>
</tr>
</tbody>
</table>
ECB (Electronic CodeBook) mode

Electronic CodeBook Mode – ECB

Encryption

\[ C_i = E_k(M_i) \quad \text{for } i=1..N \]

Decryption

\[ M_i = E_k^{-1}(C_i) \quad \text{for } i=1..N \]

Criteria for Comparison of Modes of Operation

- hiding repeating message blocks
- speed
- capability for parallel processing and pipelining during encryption / decryption
- use of block cipher operations (encryption only or both)
- capability for preprocessing during encryption / decryption
- capability for random access for the purpose of reading / writing
- number of plaintext and ciphertext blocks required for exhaustive key search
- error propagation in the message after modifying / deleting one block / byte / bit of the corresponding ciphertext
Counter Mode - CTR Encryption

\[ E_K(IV+i-1) \]

\[ c_i = m_i \oplus k_i \]

\[ k_i = E_K(IV+i-1) \quad \text{for } i=1..N \]

Counter Mode - CTR Decryption

\[ m_i = c_i \oplus k_i \]

\[ k_i = E_K(IV+i-1) \quad \text{for } i=1..N \]

J-bit Counter Mode - CTR

\[ c_i = m_i \oplus k_i \]

\[ k_i = E(IV+i-1)[1..j] \quad \text{for } i=1..N \]
### Block Cipher Modes of Operation

**Basic Features (1)**

<table>
<thead>
<tr>
<th>Mode</th>
<th>ECB</th>
<th>CTR</th>
<th>OFB</th>
<th>CFB</th>
<th>CBC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocking repeating plaintext blocks</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic speed</td>
<td>$t_{ECB}$</td>
<td>$t_{CTR}$</td>
<td>$t_{OFB}$</td>
<td>$t_{CFB}$</td>
<td>$t_{CBC}$</td>
</tr>
<tr>
<td>Capabilities for parallel processing and pipelining</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
</tr>
<tr>
<td>Cipher operations</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
</tr>
<tr>
<td>Preprocessing</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random access</td>
<td>R/W</td>
<td>R/W</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Basic Features (2)**

<table>
<thead>
<tr>
<th>Mode</th>
<th>ECB</th>
<th>CTR</th>
<th>OFB</th>
<th>CFB</th>
<th>CBC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security against the exhaustive key search attack</td>
<td>ECB plaintext block, CFB ciphertext block</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum number of plaintext blocks and ciphertext blocks needed</td>
<td>ECB plaintext block, CFB ciphertext block</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error propagation in the decrypted message</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modification of $j$-bits</td>
<td>ECB plaintext block, CFB ciphertext block</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deletion of $j$-bits</td>
<td>ECB plaintext block, CFB ciphertext block</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### OFB (Output Feedback) Mode

**Encryption**

$c_i = m_i \oplus k_i$

$k_i = E_k(k_{i-1})$ for $i = 1 \ldots N$ and $k_0 = IV$

**Decryption**

$m_i = c_i \oplus k_i$

$k_i = E_k(k_{i-1})$ for $i = 1 \ldots N$ and $k_0 = IV$
**Block Cipher Modes of Operation**

**Basic Features (1)**

<table>
<thead>
<tr>
<th></th>
<th>ECB</th>
<th>CTR</th>
<th>OFB</th>
<th>CFB</th>
<th>CBC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiding repeating plaintext blocks</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Basic speed</td>
<td>$\frac{1}{k_c}$</td>
<td>$\frac{1}{k_c}$</td>
<td>$\frac{1}{k_c}$</td>
<td>$\frac{1}{k_c}$</td>
<td>$\frac{1}{k_c}$</td>
</tr>
<tr>
<td>Capability for parallel processing and pipelining</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Cipher operations</td>
<td>Encryption and decryption</td>
<td>Encryption only</td>
<td>Encryption only</td>
<td>Encryption only</td>
<td></td>
</tr>
<tr>
<td>Preprocessing</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Random access</td>
<td>R/W</td>
<td>R/W</td>
<td></td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Block Cipher Modes of Operation**

**Basic Features (2)**

<table>
<thead>
<tr>
<th></th>
<th>ECB</th>
<th>CTR</th>
<th>OFB</th>
<th>CFB</th>
<th>CBC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security against the exhaustive key search attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum number of the message and ciphertext blocks needed</td>
<td>1 plaintext block, ciphertext block</td>
<td>1 plaintext block, ciphertext block</td>
<td>2 plaintext blocks, ciphertext blocks (for j=L)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error propagation in the decrypted message</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modification of j bits</td>
<td>L bits</td>
<td>j bits</td>
<td>j bits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deletion of j bits</td>
<td>Current and all subsequent</td>
<td>Current and all subsequent</td>
<td>Current and all subsequent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CFB (Cipher Feedback) Mode**

**Encryption**

$c_i = m_i \oplus k_i$

$k_i = E_k(c_{i-1})$ for $i=1..N$ and $c_0 = IV$

**Decryption**

$m_i = c_i \oplus k_i$

$k_i = E_k(c_{i-1})$ for $i=1..N$ and $c_0 = IV$
CBC (Cipher Block Chaining) Mode

\[ c_i = E_K(m_i \oplus c_{i-1}) \quad \text{for } i = 1..N \quad c_0 = \text{IV} \]
**Cipher Block Chaining Mode - CBC Decryption**

\[ m_i = D_K(c_i) \oplus c_{i-1} \text{ for } i = 1 \ldots N \quad c_0 = IV \]

**Block Cipher Modes of Operation**

<table>
<thead>
<tr>
<th>Basic Features (1)</th>
<th>ECB</th>
<th>CTR</th>
<th>OFB</th>
<th>CFB</th>
<th>CBC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiding repeating plaintext blocks</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Basic speed</td>
<td>( \frac{s}{LU} )</td>
<td>( \frac{s}{LU} )</td>
<td>( \frac{s}{LU} )</td>
<td>( \frac{s}{LU} )</td>
<td>( \frac{s}{LU} )</td>
</tr>
<tr>
<td>Capability for parallel processing and pipelining</td>
<td>Encryption and decryption</td>
<td>Encryption and decryption</td>
<td>None</td>
<td>Decryption only</td>
<td>Decryption only</td>
</tr>
<tr>
<td>Cipher operations</td>
<td>Encryption and decryption</td>
<td>Encryption only</td>
<td>Encryption only</td>
<td>Encryption only</td>
<td>Encryption and decryption</td>
</tr>
<tr>
<td>Preprocessing</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Random access</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>R only</td>
<td>R only</td>
</tr>
</tbody>
</table>

**Block Cipher Modes of Operation**

<table>
<thead>
<tr>
<th>Basic Features (2)</th>
<th>ECB</th>
<th>CTR</th>
<th>OFB</th>
<th>CFB</th>
<th>CBC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security against the exhaustive key search attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum number of message and ciphertext blocks needed</td>
<td>1 plaintext block, ciphertext block</td>
<td>1 plaintext block, ciphertext block</td>
<td>2 plaintext blocks, ciphertext blocks (for ( j=L ))</td>
<td>1 plaintext block, ciphertext block (for ( j=L ))</td>
<td>1 plaintext block, ciphertext block</td>
</tr>
<tr>
<td>Error propagation in the decrypted message</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modification of j-bits</td>
<td>L bits</td>
<td>j bits</td>
<td>j bits</td>
<td>L+j bits</td>
<td>L+j bits</td>
</tr>
<tr>
<td>Deletion of j-bits</td>
<td>All and subsequent</td>
<td>All and subsequent</td>
<td>All and subsequent</td>
<td>All and subsequent</td>
<td>All and subsequent</td>
</tr>
<tr>
<td>Integrity</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**New modes of operation**

**Evaluation Criteria for Modes of Operation**

- **Security**
  - resistance to attacks
  - proof of security
  - random properties of the ciphertext

- **Efficiency**
  - number of calls of the block cipher
  - capability for parallel processing
  - memory/area requirements
  - initialization time
  - capability for preprocessing

- **Functionality**
Evaluation criteria (2)

Functionality

- **security services**
  - confidentiality, integrity, authentication
- flexibility
  - variable lengths of blocks and keys
  - different amount of precomputations
  - requirements on the length of the message
- vulnerability to implementation errors
  - requirements on the amount of keys, initialization vectors, random numbers, etc.
- error propagation and the capability for resynchronization
- patent restrictions

---

**CBC**

- $m_0, m_1, m_2, \ldots, m_N$
- $E$, $c_0, c_1, c_2, \ldots, c_N$

**Problems:**
- No parallel processing of blocks from the same packet
- No speed-up by preprocessing
- No integrity or authentication

---

**Counter mode**

- $m_0, m_1, m_2, \ldots, m_N$
- $E$, $c_0, c_1, c_2, \ldots, c_N$

**Features:**
- Potential for parallel processing
- Speed-up by preprocessing
- No integrity or authentication

---

**OCB - Offset Codebook Mode**

- $m_0, m_1, m_2, \ldots, m_N$
- $E$, $c_0, c_1, c_2, \ldots, c_N$

**New modes of block ciphers**

1. **CCM - Counter with CBC-MAC**
   - developed by R. Housley, D. Whiting, N. Ferguson in 2002
   - assures simultaneous confidentiality and authentication
   - not covered by any patent
   - part of the IEEE 802.11i standard for wireless networks

2. **GCM – Galois/Counter Mode**
   - developed by D. McGrew and J. Vega in 2005
   - assures simultaneous confidentiality and authentication
   - not covered by any patent
   - used in the IEEE 802.1AE (MACsec) Ethernet security, ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1 tape storage, and IETF IPSec standards
### Properties of new modes of operation

<table>
<thead>
<tr>
<th></th>
<th>CBC</th>
<th>CFB</th>
<th>OFB</th>
<th>CTR</th>
<th>CCM</th>
<th>GCM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proof of security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Parallel processing</td>
<td>only decryption</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Preprocessing</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Integrity and authentication</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Resistance to implementation errors</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

### Modes of operation of block ciphers

**Timeline**

- **1997**: CBC, CFB, OFB, ECB
- **1998**: CBC, CFB, OFB, CTR
- **1999**: CBC, CFB, OFB, CTR, CBCM
- **2000**: CBC, CFB, OFB, CTR, CBCM
- **2001**: CBC, CFB, OFB, CTR, CBCM
- **2002**: CBC, CFB, OFB, CTR, CBCM
- **2003**: CBC, CFB, OFB, CTR, CBCM
- **2004**: CBC, CFB, OFB, CTR, CBCM
- **2005**: CBC, CFB, OFB, CTR, CBCM
- **2006**: CBC, CFB, OFB, CTR, CBCM
- **2007**: CBC, CFB, OFB, CTR, CBCM
- **2008**: CBC, CFB, OFB, CTR, CBCM

**Contests**: Apr 2001 - 10 modes submitted to the contest (including CTR, CFB, CBC, CBCM, AEAD)

**Attacks**: Aug 2001 - DCM mode developed by NSA, several days after the publication

### Confidentiality & Authentication

**Authenticated Ciphers**

- **Bob**
  - Npub
  - Nsec
  - AD
  - Message
  - K_{AB}
  - Encrypted Secret Message Number
  - Associated Data
  - Secret key of Alice and Bob

- **Alice**
  - Npub
  - Nsec
  - AD
  - Ciphertext
  - Tag
  - K_{AB}
  - Associated Data
  - Secret key of Alice and Bob

- **Confidentiality & Authentication**

  - Npub
  - Nsec
  - AD
  - Message
  - K_{AB}
  - Encryption
  - Decryption

- **Cryptographic Standard Contests**

  - IX.1997: AES
  - X.2000: NESSIE
  - XII.2002: CRYPTREC
  - XI.2004: eSTREAM
  - IV.2008: SPN-3
  - XII.2012: CAESAR

- **1997-2000**
  - 15 block ciphers
  - 1 winner
  - 4 SW winners
  - 4 HW winners
  - 51 hash functions
  - 1 winner
  - 57 authenticated ciphers
  - multiple winners

- **2013-2017**
  - 51 hash functions
  - 1 winner
  - 57 authenticated ciphers
  - multiple winners
  - CAESAR

---

**CAESAR Contest 2013-2017**

**Confidentiality & Authentication**

- **Authenticated Ciphers**
  - Npub
  - Nsec
  - AD
  - Message
  - K_{AB}
  - Encrypted Secret Message Number
  - Associated Data
  - Secret key of Alice and Bob
Contest Timeline

- 2014.03.15: Deadline for first-round submissions
- 2014.04.15: Deadline for first-round software
- 2015.07.07: Announcement of second-round candidates
- 2015.12.15: Deadline for second-round Verilog/VHDL
- 2016.03.15: Announcement of third-round candidates
- 2016.12.15: Announcement of finalists
- 2017.12.15: Announcement of final portfolio