Modes of operation of secret-key block ciphers

**Block vs. stream ciphers**

- **Block cipher**
  - $M_1, M_2, \ldots, M_N$
  - $C_1, C_2, \ldots, C_N$
  - $C_i = f_K(M_i)$
  - Every block of ciphertext is a function of only one corresponding block of plaintext

- **Stream cipher**
  - $m_1, m_2, \ldots, m_N$
  - $c_1, c_2, \ldots, c_N$
  - $c_i = f_k(m_i, m_{i-1}, \ldots, m_2, m_1)$
  - Every block of ciphertext is a function of the current and all proceeding blocks of plaintext

**Typical stream cipher**

- **Sender**
  - Key
  - Initialization vector
  - Pseudorandom Key Generator
  - $k_i$
  - Keystream
  - $m_i$ plaintext
  - $c_i$ ciphertext

- **Receiver**
  - Key
  - Initialization vector
  - Pseudorandom Key Generator
  - $k_i$
  - Keystream
  - $c_i$ ciphertext
  - $m_i$ plaintext
**Electronic Codebook Mode - ECB**

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

**Counter Mode - CTR**

- **Encryption**
  \[ C_i = M_i \oplus K_i \]
  \[ K_i = E(IV+i-1) \quad \text{for } i=1..N \]

- **Decryption**
  \[ M_i = C_i \oplus K_i \]
  \[ K_i = E(IV+i-1) \quad \text{for } i=1..N \]
J-bit Counter Mode - CTR

\[ c_i = m_i \oplus k_i \]
\[ k_i = E(IV+i-1)[1..j] \quad \text{for } i=1..N \]

Output Feedback Mode - OFB

\[ C_i = M_i \oplus K_i \]
\[ K_i = E(K_{i-1}) \quad \text{for } i=1..N, \text{ and } K_0 = IV \]
Output Feedback Mode - OFB

Decryption

\[ M_i = C_i \oplus K_i \]

\[ K_i = E(K_{i-1}) \quad \text{for } i=1..N, \text{ and } K_0 = IV \]

J-bit Output Feedback Mode - OFB

Cipher Feedback Mode - CFB

Encryption

\[ C_i = M_i \oplus K_i \]

\[ K_i = E(C_{i-1}) \quad \text{for } i=1..N, \text{ and } C_0 = IV \]
Cipher Feedback Mode - CFB

Decryption

\[ C_i = M_i \oplus K_i \]
\[ K_i = E(C_{i-1}) \quad \text{for } i = 1..N, \text{ and } C_0 = IV \]

J-bit Cipher Feedback Mode - CFB

\[ \text{shift} \]

\[ K \]

\[ E \]

\[ \text{IN} \]

\[ \text{OUT} \]

\[ \text{shift} \]

\[ K \]

\[ E \]

\[ \text{IN} \]

\[ \text{OUT} \]

Cipher Block Chaining Mode - CBC

Encryption

\[ C_i = E(M_i \oplus C_{i-1}) \quad \text{for } i = 1..N, \ C_0 = IV \]
Cipher Block Chaining Mode - CBC
Decryption

\[ M_i = D(C_i) \oplus C_{i-1} \text{ for } i=1..N \quad C_0=IV \]

Modes of operation: CBC

Encrypted

\[ E \quad IV \quad \cdots \quad E \quad M_N \]

Decrypted

\[ D \quad IV \quad \cdots \quad D \quad M_N \]

CBC: Implementation Issues: Encryption

Packet 1

\[ P_1 \quad P_1_2 \quad P_1_3 \quad \cdots \quad P_1_N \]

\[ IV1 = \text{random string} \quad C_{1} \quad C_{1_2} \quad C_{1_3} \quad \cdots \quad C_{1_N} \]

Packet 2

\[ P_2 \quad P_2_2 \quad P_2_3 \quad \cdots \quad P_2_N \]

\[ IV2=C_{1_N} \quad C_{2} \quad C_{2_2} \quad C_{2_3} \quad \cdots \quad C_{2_N} \]
Interleaved operating modes

\[ C_i = E(M_i \oplus IV_i) \quad \text{for } i = 1 \text{ to } N, \]
\[ C_i = E(M_i \oplus C_{i-N}) \quad \text{for } i > N \]

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>Security</td>
<td>weak</td>
<td>strong</td>
<td>strong</td>
<td>strong</td>
<td>strong</td>
</tr>
<tr>
<td>Basic speed</td>
<td>$s_{ECB}$</td>
<td>$s_{ECB}$</td>
<td>$s_{ECB}$</td>
<td>$s_{ECB}$</td>
<td>$s_{ECB}$</td>
</tr>
<tr>
<td>Capability</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></td>
<td>Encryption only</td>
<td>Encryption only</td>
<td>Encryption only</td>
<td>Encryption and decryption</td>
<td></td>
</tr>
<tr>
<td>Cipher operations</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Preprocessing</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>R only</td>
<td>R only</td>
</tr>
</tbody>
</table>

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, 1 ciphertext block</td>
<td>2 plaintext blocks, 2 ciphertext blocks</td>
<td>2 plaintext blocks, 2 ciphertext blocks (for ( j \neq L ))</td>
<td>1 plaintext block, 2 ciphertext blocks (for ( j \neq L ))</td>
<td>1 plaintext block, 2 ciphertext blocks</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>( Lj ) bits</td>
<td>( Lj ) bits</td>
</tr>
<tr>
<td>Deletion of ( j ) bits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### Operating Modes Contest

4 Old Modes
(CBC, CFB, OFB, ECB)

April 2001

10 New Candidates
from Egypt, Estonia, Norway, Sweden, Thailand, USA

Summer 2001

5 Standard Modes

2002

New Standard Modes

---

#### Modes submitted to the contest (1)

<table>
<thead>
<tr>
<th>Full name</th>
<th>Authors</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>2DEM</td>
<td>A. A. Belal, M. A. Abdel-Gawad</td>
<td>Alexandria University, Egypt</td>
</tr>
<tr>
<td>ABC</td>
<td>L. Knudsen</td>
<td>U. of Bergen, Norway</td>
</tr>
<tr>
<td>CTR</td>
<td>H. Lipmaa, P. Rogaway, D. Wagner</td>
<td>Finland, Estonia, USA, Thailand</td>
</tr>
<tr>
<td>IACBC</td>
<td>C. Jutla</td>
<td>IBM, USA</td>
</tr>
<tr>
<td>IAPM</td>
<td>C. Jutla</td>
<td>IBM, USA</td>
</tr>
</tbody>
</table>

---

#### Modes submitted to the contest (2)

<table>
<thead>
<tr>
<th>Full name</th>
<th>Authors</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGE</td>
<td>V. D. Gilgor, P. Donescu</td>
<td>VDG, Inc., USA</td>
</tr>
<tr>
<td>KFB</td>
<td>J. Håstad, M. Naslund</td>
<td>NADA, Ericsson, Sweden</td>
</tr>
<tr>
<td>OCB</td>
<td>P. Rogaway</td>
<td>UCSD, USA, Thailand</td>
</tr>
<tr>
<td>PCFB</td>
<td>H. Hellström</td>
<td>StreamSec, Sweden</td>
</tr>
<tr>
<td>XCBC</td>
<td>V. D. Gilgor, P. Donescu</td>
<td>VDG, Inc., USA</td>
</tr>
</tbody>
</table>

---
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

• 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
Modes of operation: Current standard - CBC

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

Counter mode

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

Properties of existing and new cipher modes

<table>
<thead>
<tr>
<th></th>
<th>CBC</th>
<th>CFB</th>
<th>OFB</th>
<th>New standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proof of security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Parallel processing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preprocessing</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Integrity and</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>authentication</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Resistance to</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>implementation errors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Encryption with authentication

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Full name</th>
<th>Authors</th>
<th>Institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IACBC</td>
<td>Integrity Aware CBC</td>
<td>C. Jutla</td>
<td>IBM (patent)</td>
<td></td>
</tr>
<tr>
<td>IAPM</td>
<td>Integrity Aware Parallalizable Mode</td>
<td>C. Jutla</td>
<td>IBM (patent)</td>
<td></td>
</tr>
<tr>
<td>XCBC-XOR</td>
<td>eXtended CBC Encryption</td>
<td>V. D. Gligor, P. Donescu</td>
<td>VDG, Inc., (patent)</td>
<td></td>
</tr>
<tr>
<td>XECB-XOR</td>
<td>eXtended ECB Encryption</td>
<td>V. D. Gligor, P. Donescu</td>
<td>VDG, Inc., (patent)</td>
<td></td>
</tr>
<tr>
<td>OCB</td>
<td>Offset Codebook</td>
<td>P. Rogaway</td>
<td>UCSD, USA, Thailand</td>
<td></td>
</tr>
</tbody>
</table>

### OCB

\[
\begin{align*}
\text{IV} & \xrightarrow{E} M_1 \\ L & \xrightarrow{E} Z_1 \\ R & \xrightarrow{E} C_1 \\ E & \xrightarrow{E} M_2 \\ & \quad \vdots \quad \quad \quad \vdots \\ & \quad \xrightarrow{E} M_{N-1} \\ & \quad \xrightarrow{E} M_N \\
\end{align*}
\]

Control sum

\[
\begin{align*}
Z_i &= f(L, R) \\
\end{align*}
\]