Modes of operation of secret-key block ciphers

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

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
- Keystream
- Plaintext $m_i$ → $k_i$ → Keystream $k_i$ → Ciphertext $c_i$

Receiver

- Key
- Initialization vector
- Pseudorandom Key Generator
- Keystream
- Ciphertext $c_i$ → $k_i$ → Keystream $k_i$ → Plaintext $m_i$

**Electronic Codebook Mode - ECB**

$$M_1 \rightarrow E \rightarrow C_1 \rightarrow K \leftarrow m_1$$

$$M_2 \rightarrow E \rightarrow C_2 \rightarrow K \leftarrow m_2$$

$$M_3 \rightarrow E \rightarrow C_3 \rightarrow K \leftarrow m_3$$

$$\vdots$$

$$M_{N-1} \rightarrow E \rightarrow C_{N-1} \rightarrow K \leftarrow m_{N-1}$$

$$M_N \rightarrow E \rightarrow C_N \rightarrow K \leftarrow m_N$$

$$C_i = E(M_i) \text{ for } i=1..N$$
### Counter Mode - CTR Encryption

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

### Counter Mode - CTR 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

**Encryption**

\[ C_i = M_i \oplus K_i \]

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

**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**

- **IN**
  - L-j bits
  - j bits
- **E**
  - OUT
  - j bits
  - L-j bits
- **shift**
- **K**
- **IV**
- **c_i**
- **m_i**

**Cipher Feedback Mode - CFB Encryption**

- **E**
- **M_i** → **C_i**
- **C_i = M_i ⊕ K_i**
- **K_i = E(C_{i-1})** for i=1..N, 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

\[ \text{shift} \]
\[ \text{IN} \]
\[ \text{E} \]
\[ \text{OUT} \]
\[ m_i \]

\[ \text{shift} \]
\[ \text{IN} \]
\[ \text{E} \]
\[ \text{OUT} \]
\[ m_i \]
Cipher Block Chaining Mode - CBC

Encryption

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

\[ \begin{align*}
M_1 & \quad M_2 & \quad M_3 & \quad \ldots & \quad M_{N-1} & \quad M_N \\
\quad \downarrow & \quad \downarrow & \quad \downarrow & \quad \cdots & \quad \downarrow & \quad \downarrow \\
\quad E & \quad E & \quad E & \quad \cdots & \quad E & \quad E \\
\quad C_1 & \quad C_2 & \quad C_3 & \quad \cdots & \quad C_{N-1} & \quad C_N \\
\end{align*} \]

Decryption

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

\[ \begin{align*}
C_1 & \quad C_2 & \quad C_3 & \quad \ldots & \quad C_{N-1} & \quad C_N \\
\quad \downarrow & \quad \downarrow & \quad \downarrow & \quad \cdots & \quad \downarrow & \quad \downarrow \\
\quad D & \quad D & \quad D & \quad \cdots & \quad D & \quad D \\
\quad M_1 & \quad M_2 & \quad M_3 & \quad \cdots & \quad M_{N-1} & \quad M_N \\
\end{align*} \]
Modes of operation: CBC

Encryption

\[ \text{IV} \rightarrow E \rightarrow C_1 \]
\[ \vdots \]
\[ \text{IV} \rightarrow E \rightarrow C_N \]

Decryption

\[ \text{IV} \rightarrow D \rightarrow M_1 \]
\[ \vdots \]
\[ \text{IV} \rightarrow D \rightarrow M_N \]

CBC: Implementation Issues: Encryption

Packet 1

\[ \text{IV} = \text{random string} \]
\[ \text{IV} \rightarrow E \rightarrow C_1 \]
\[ \vdots \]
\[ \text{IV} \rightarrow E \rightarrow C_N \]

Packet 2

\[ \text{IV} = C_1 \]
\[ \text{IV} \rightarrow E \rightarrow C_2 \]
\[ \vdots \]
\[ \text{IV} \rightarrow E \rightarrow C_N \]
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_{\text{ECB}})</td>
<td>(=s_{\text{ECB}})</td>
<td>(=j/L \cdot s_{\text{ECB}})</td>
<td>(=j/L \cdot s_{\text{ECB}})</td>
<td>(=s_{\text{ECB}})</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
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=L)</td>
<td>1 plaintext blocks, 2 ciphertext blocks (for j=L)</td>
<td>1 plaintext blocks, 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>L+j bits</td>
<td>L+j bits</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>L bits</td>
<td>Current and all 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>

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>2D-Encryption Mode</td>
<td>A. A. Belal, M. A. Abdel-Gawad</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alexandria University, Egypt</td>
</tr>
<tr>
<td>ABC</td>
<td>Accumulated Block Chaining</td>
<td>L. Knudsen</td>
</tr>
<tr>
<td></td>
<td></td>
<td>U. of Bergen Norway</td>
</tr>
<tr>
<td>CTR</td>
<td>Counter Mode</td>
<td>H. Lipmaa, P. Rogaway, D. Wagner</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Finland, Estonia, USA, Thailand</td>
</tr>
<tr>
<td>IACBC</td>
<td>Integrity Aware CBC</td>
<td>C. Jutla</td>
</tr>
<tr>
<td>IAPM</td>
<td>Integrity Aware Parallalizable Mode</td>
<td>C. Jutla</td>
</tr>
<tr>
<td></td>
<td></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>Infinite Garble Extension</td>
<td>V. D. Gligor, P. Donescu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VDG, Inc., USA</td>
</tr>
<tr>
<td>KFB</td>
<td>Key Feedback Mode</td>
<td>J. Håstad, M. Naslund</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NADA, Ericsson Sweden</td>
</tr>
<tr>
<td>OCB</td>
<td>Offset Codebook</td>
<td>P. Rogaway</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UCSD, USA, Thailand</td>
</tr>
<tr>
<td>PCFB</td>
<td>Propagating Cipher Feedback</td>
<td>H. Hellström</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StreamSec, Sweden</td>
</tr>
<tr>
<td>XCBC</td>
<td>eXtended CBC Encryption</td>
<td>V. D. Gligor, P. Donescu</td>
</tr>
<tr>
<td></td>
<td></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
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

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

IV → E → K₀ → M₀ → C₀

IV+1 → E → K₁ → M₁ → C₁

IV+2 → E → K₂ → M₂ → C₂

... → E → ... → E → ...

IV+N-1 → E → Kₙ₋₁ → Mₙ₋₁ → Cₙ₋₁

IV+N → E → Kₙ → Mₙ → Cₙ

**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><strong>Proof of security</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Parallel processing</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>decryption only</td>
<td>—</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Preprocessing</strong></td>
<td>—</td>
<td>—</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Integrity and authentication</strong></td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Resistance to implementation errors</strong></td>
<td>✓</td>
<td>✓</td>
<td>—</td>
<td>✓</td>
</tr>
</tbody>
</table>
## Encryption with authentication

<table>
<thead>
<tr>
<th>Abbreviation</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

IV \(0\) → \(E\) → \(Z_1\) → \(Z_2\) → ... → \(Z_{N-1}\) → \(Z_N\) → \(M_N\) → Control sum

\[ Z_i = f(L, R) \]