Block Ciphers

Modes of Operation for Encryption and Authentication
Definition

- A block cipher $E_{\pi}(\cdot)$ is a (parametrized) deterministic function mapping $n$-bit plaintext blocks to $n$-bit ciphertext blocks. The value $n$ is called the blocklength.
  - It is essentially a simple substitution cipher with character set $= \{0, 1\}^n$. 

From J. Savard’s website
The Key to the Cipher

• The parameter **key** is a $k$-bit binary string.
  – It may be that the set of all keys, the **keyspace** $K$, is a proper subset of all $k$-bit binary strings. In that case, we say that the **effective key size**, or **security parameter**, provided by the cipher is $\log_2|K|$

• The keyed block cipher $E_k(\cdot)$ is a bijection, and has a unique inverse: the decryption function $D_k(\cdot)$.
  – Alternative notation: $K\{\cdot\}$ and $K^{-1}\{\cdot\}$
Modes of Operation

- Clearly, the block cipher can be used exactly as a substitution cipher, i.e., by encrypting each block of plaintext independently using the same key. This is called the **Electronic Codebook Mode**, or **ECB**:

\[
\begin{align*}
M_0 & \quad M_1 & \quad M_2 & \ldots & \quad M_i \\
C_0 & \quad C_1 & \quad C_2 & \ldots & \quad C_i \\
K\{\} & \quad K\{\} & \quad K\{\} & K\{\} \\
\end{align*}
\]
ECB (continued)

- Decryption also works block by block (inverse substitution):

![Diagram showing encryption (E) and decryption (D) processes with inputs \(M_i\), outputs \(C_i\) and \(M_i\), and key inputs and outputs]
Cipher Block Chaining (CBC)

• An initial vector (IV) is \textit{xored} into the first block before encryption:
  \[ C_0 = E_k(IV \oplus M_0) \]

• Subsequent blocks are first \textit{xored} with the previous cipherblock before encrypting:
  \[ C_{i+1} = E_k(C_i \oplus M_{i+1}) \]

• The encrypted message is transmitted as
  \[ IV, C_0, ..., C_l \]
CBC (continued)

- Decryption of $C_i$ uses $C_{i-1}$ (where $C_0 = IV$):
  \[ M_i = D_k(C_i \oplus C_{i-1}) \]

Diagram:
- $M_i$ enters $E$ with $k$.
- $E$ outputs $C_{i-1}$ to $C_{i-1} \leftarrow C_i$ and $C_i$ to $D$.
- $D$ outputs $C_{i-1}$.
- $M_i$ is XORed with $C_{i-1}$.
- $C_i$ is XORed with $C_{i-1}$.
Block Ciphers as Stream Ciphers

• Two modes of operation of a block cipher implement a stream cipher:
  – **Cipher Feedback Mode (CFB)**, a **Ciphertext-auto-key** stream cipher (**CTAK**)
  – **Output Feedback Mode (OFB)**, a **Key-auto-key** stream cipher (**KAK**)
  – In both cases encryption is obtained by xoring a keystream with the plaintext.
    • CFB: Keystream depends on previous ciphertext
    • OFB: Keystream depends on previous keystream
The keystream (output of encryption) is xored into plaintext to obtain ciphertext. The ciphertext is the input for next chained encryption: \( C_i = M_i \oplus E(C_{i-1}) \).
The keystream - output of $E(\cdot)$ - is xored into the plaintext to obtain ciphertext. The keystream is also the input for next chained encryption:

- $C_i = M_i \oplus O_i; \quad O_i = E(O_{i-1})$

\[ \begin{align*}
(O_0=IV) \quad O_{i-1} & \quad O_{i-1} \leftrightarrow O_i \\
E \quad k & \quad E \quad k \\
M_i \oplus & \quad C_i \oplus \quad M_i
\end{align*} \]
Security Issues

• ECB is the least secure mode
  – Does not diffuse plaintext information over more than one block. Use is limited.

• IV issues in other modes
  – IV need not be secret; but:
    • IV for CBC needs to be integrity-protected (for instance, by ECB encryption)
    • IV for CFB should be generated in strong pseudo-random way.
    • Never re-use a (Key, IV) pair!