5.2.4 Design Considerations and Security

- After 2 rounds full diffusion is achieved, i.e., if one byte of input is changed, all bytes of the output are changed.

- S-Box is constructed as $x \mapsto x^{-1}$ in $\mathbb{F}_2^8$. Advantages:
  - Simple, algebraic, highly non-linear.
  - Resists differential and linear cryptanalysis.
  - No suspension of impossible built-in.

- ShiftRows to resist the attack: truncated differential and Square attack.

- MixColumns causes diffusion among the bytes.

- Key Schedule to avoid advantage from knowing parts of the key.

- Presently no better attacks than exhaustive reach known against AES-128. (Not entirely true $2^{126.1}$)

- Fault attacks are known if the number of rounds is less than 7.

- Attacks against AES-192 and AES-256 of complexity $2^{119}$ are known (see Schneier). A Related-Key cryptanalysis is used.

- Even more refining this attack on AES-256 leads to a complexity of $2^{99.5}$. 

5.3 Other Block Ciphers

- IDEA - International Data Encryption Alg.
  Designed by Massey et al., 1990
  IDEA was part of PGP (pretty good privacy)
  Block length of 64 bits, key length 128 bits
  IDEA is secure, best known attack is exhaustive search
  Patented in Europe (1991), USA (1993), but for
  non-commercial applications, it is free

- RC5 (Rivest et al., '94)
- Blowfish (Schneier, '93)
- Serpent (Anderson, Biham, Knudsen, 1998)
Input:

ENCRYPTED?

Encrypted with ECB:

ENCRYPTED?

Encrypted with CBC:
5.4 Modes of operation

Let $E_k$ denote a blockcipher operating on blocks of fixed length using key $k$. 5 modes of operation were standardized in Dec. 1980

5.4.1 ECB (Electronic codebook mode)

Directors of $E_k$.

Given: Plaintext blocks: $M_1, M_2, M_3, ...$

Encryption: $C_i = E_k (M_i)$

Decryption: $M_i = E_k^{-1} (C_i)$

\[
\begin{align*}
M_1 & \leftrightarrow [E_k] \leftrightarrow C_1 \\
M_i & \leftrightarrow [E_k] \leftrightarrow C_i
\end{align*}
\]

5.4.2 CBC (Cipher block chaining mode)

Given: Plaintext blocks: $M_1, M_2, M_3, ...$

Key: $K$

Non-secret Initial Vector: $C_0$

Encryption: $C_i = E_k (M_i \oplus C_{i-1}) \quad i = 1, 2, ...

Decryption: $M_i = E_k^{-1} (C_i) \oplus C_{i-1}$

\[
\begin{align*}
C_0 \quad \rightarrow \oplus \rightarrow [E_k] \rightarrow C_1 \quad \rightarrow \oplus \rightarrow [E_k] \rightarrow C_2 \rightarrow \ldots
\end{align*}
\]
5.4.4 CFB (Cipher feedback mode)

Given: (*)

Encryption: \( C_i = E_K (C_{i-1}) \oplus M_i \)

Decryption: \( M_i = C_i \oplus E_K (C_{i-1}) \)

\[
\begin{array}{ccc}
E_K & \oplus & C_i \\
\downarrow & & \downarrow \\
M_i & & \downarrow \\
\end{array}
\]

5.4.3 OFB (Output feedback mode)

Given: (\#) \( z_0 = C_0 \)

Encryption: \( C_i = E_K (2^i \cdot z_{i-1}) \), \( C_i = M_i \oplus z_i \)

Decryption: \( C_i = E_K (2^i \cdot z_{i-1}) \), \( \tilde{M_i} = C_i \oplus z_i \)

A key stream is generated and XORed with the message

\[
\begin{array}{ccc}
E_K & \oplus & \tilde{C_i} \\
\downarrow & & \downarrow \\
\tilde{M_i} & & \downarrow \\
\end{array}
\]

5.4.5 CTR (Counter mode)

Given: (\#) \( z_0 = C_0 \) (interpreted as some integer)

Encryption: \( z_i = z_{i-1} + 1 \), \( C_i = E_K (z_i) \oplus M_i \)

Decryption: \( z_i = z_{i-1} + 1 \), \( M_i = E_K (z_i) \oplus C_i \)

\[
\begin{array}{ccc}
E_K & +1 & \rightarrow \\
\downarrow & & \downarrow \\
M_i & +1 & \rightarrow \\
\end{array}
\]
In ECB, CFB, or CTR: Changing one plaintext block does not affect the ciphertext blocks.

**Example:** MAC - Message authentication code

In CFB and CTR modes, changing any plaintext block affects all subsequent ciphertext blocks. Appropriate for generating a MAC.

- Append $C_n$ to the message $(M_1, \ldots, M_n)$
  - If $C_n$ is tampered with, the message is no longer valid.

- The authorized receiver, knowing $K$, can easily verify $C_n$.
  - Hence, the integrity or authenticity of $(M_1, \ldots, M_n)$.

**Example:** Storing passwords

Direct plaintext storing of passwords is insecure. Hence,

- Users type $(\text{name}, \text{password})$
- System generates a key $K = K(\text{name}, \text{password})$ and stores $(\text{name}, \text{BC}(K(\text{password})))$
- When logging in, system compares $(\text{name}, \text{BC}(K(\text{password})))$ with the stored value.
  - Knowledge of $(\text{name}, \text{BC}(K(\text{password})))$ is useless for an intruder.