Modern Block Ciphers

A sym. key MBC encrypts an n-bit block of plaintext or decrypt an n-bit block of ciphertext.
Encryption & Decryption use a k-bit key.

Components of MBC: MBC is made of different units namely transposition, substitution and other units.

1. D-Boxes (Diffusion Boxes or P-Boxes):

Types: ① Straight D-Box
② Compression D-Box
③ Expansion D-Box.

① Straight D-Box:

n-bits input, n-bits of output

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \checkmark \qquad [2\ 3\ 1]$$

D-boxes are normally keyless, this means that the permutation in the D-box would be predetermined.

If a D-Box is implemented in hardware then, it is prewired.
If it is implemented in the software, a permutation table shows the rule of mapping

Ex:

$$\boxed{\begin{matrix} 7 & 16 & 9 & 3 \\ 1 & 5 & \boxed{4} & 2 \\ 11 & 13 & 15 & 6 \\ 14 & 8 & 10 & 12 \end{matrix}}$$

⇒ 7th bit of the ciphertext would be the 4th bit of the plaintext.

21 August 2020 11:55

(2) Compression D-Box: This is a D-box with n-bits input and m-bits output where $m < n$.

Ex: 6×4 D-box

$\boxed{5\ 6\ 2\ 1}$

⇒ In a C. D-box some inputs bits are blocked and do not reach to the output.

(3) Expansion D-box: This is a D-box with n bits of input and m bits of output where $m > n$

Ex: 4×6 - Exp. D-box

$\boxed{2\ 1\ 3\ 1\ 2\ 4}$

Note: A straight D-box is invertible while Comp D-box & Exp. D-box are not invertible.

S-Boxes (Substitution Boxes): An S-box is an m×n substitution unit, where m & n are not necessarily the same.

Ex: S-box of size 3×2

	00	01	10	11
0	00	10	01	11
1	01	11	10	00

→ Rightmost two bits.

↓ Leftmost bit

010

Input	Output	In	Out
010	01	110	10

Note : An S-box may or may not be invertible.

In an invertible S-box no. of input bits & no. of output bits should be same.

Exclusive -OR
Circular shift $\boxed{P_1\ P_2\ \cdots\ P_n} \longrightarrow \boxed{P_3\ P_4\ \cdots}$
Swap.

Product Cipher : A product cipher is a complex cipher combining permutation, substitution and other components of MBC.

Shannon's Theory of diffusion and Confusion:

① Diffusion: The idea of diffusion is to hide the relationship b/w plaintext & Ciphertext.

This implies that each symbol in ciphertext is dependent on some or all symbols in the plaintext.

② Confusion refers to making the relationship b/w the key and the ciphertext as complex and involved as possible.

Confusion hides the relationship b/w the key & the ciphertext.

Types of Product Ciphers :

① Fiestal Cipher

use both invertible & non-invertible components of MBC (e.g. DES - Data Encryption Standard)

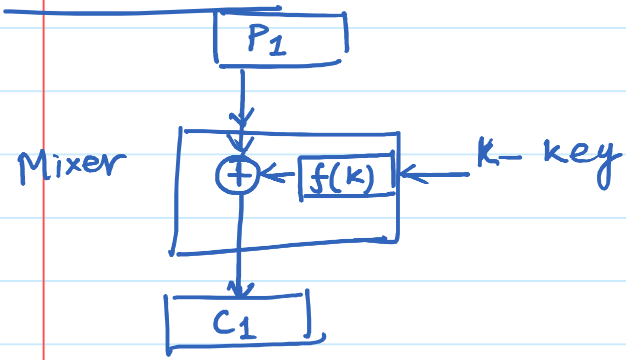
② Non-Fiestal Cipher. (e.g. AES).

use only invertible components.

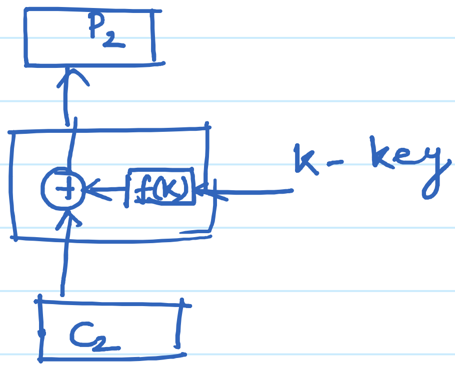
Fiestal Ciphers : A Fiestal ciper uses three types of components

(i) self invertible
(ii) Invertible
(iii) Non-invertible

First though :



Encryption



Decryption

$f(K)$ is a non-invertible function

Let $C_1 = C_2$

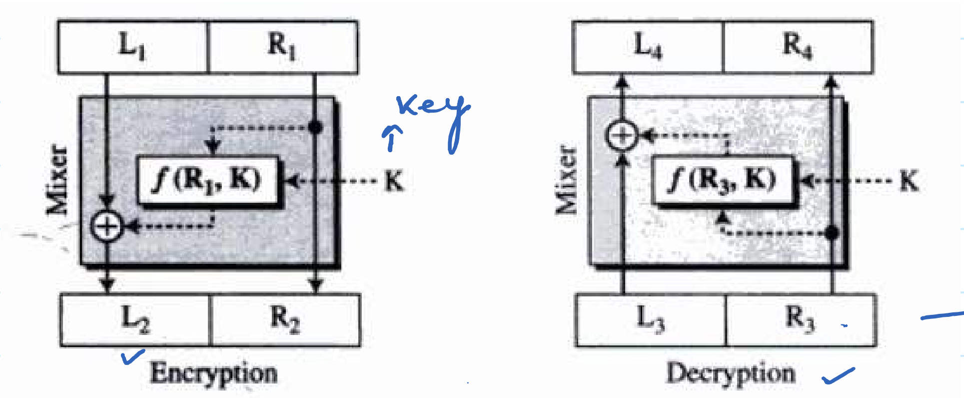
$$P_2 = C_2 \oplus f(K) = C_1 \oplus f(K) = (P_1 \oplus f(K)) \oplus f(K)$$

$$= P_1 \oplus (f(K) \oplus f(K))$$

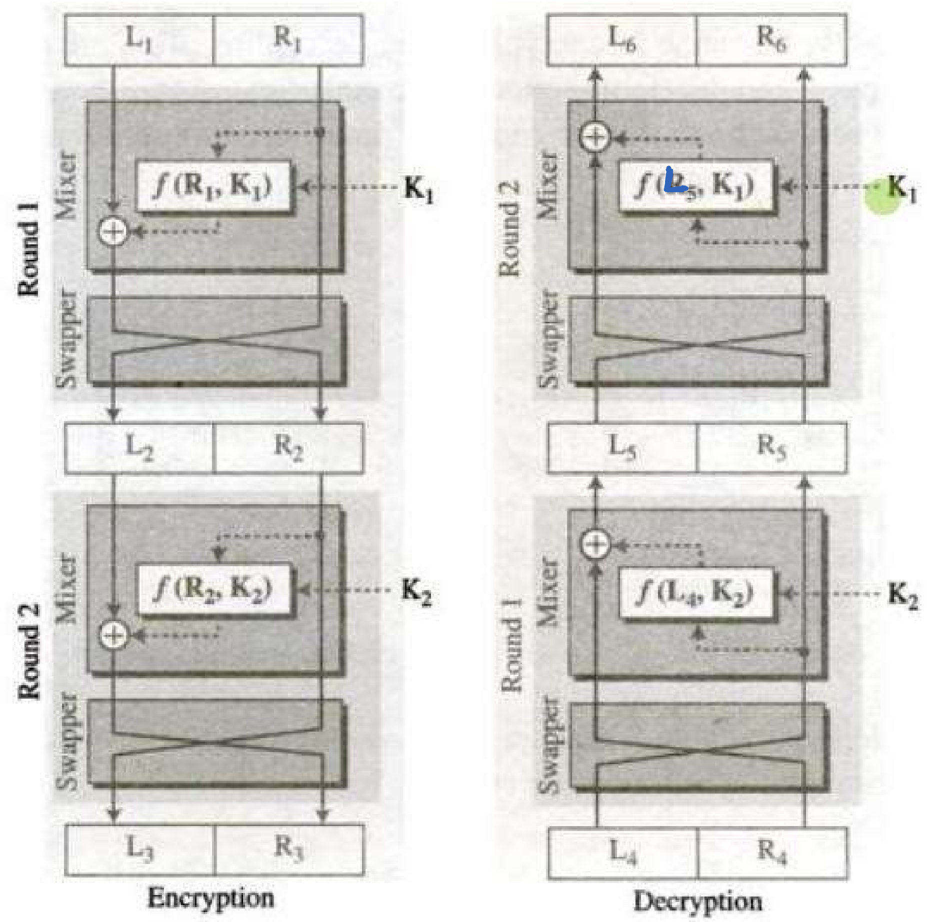
$$= P_1 \oplus (00 \cdots 0)$$

$$= P_1$$

$\Rightarrow$ Encryption & Decryption are inverses of each other.



Improvement



Final Feistal Cipher Structure

To show that Encryption & Decryption are inverses of each other we need to show that

$L_1 = L_6$ & $R_1 = R_6$ when $L_3 = L_4$ & $R_3 = R_4$.

Let $L_3 = L_4$ & $R_3 = R_4$

$$
\begin{aligned}
L_6 &= R_5 \oplus f(L_5, K_1) \\
&= L_4 \oplus f(R_4 \oplus f(L_4, K_2), K_1) \\
&= L_3 \oplus f(R_3 \oplus f(L_3, K_2), K_1) \\
&= L_3 \oplus f(L_2 \oplus \underline{f(R_2, K_2) \oplus f(R_2, K_2)}, K_1) \\
&= L_3 \oplus f(L_2, K_1) \\
&= R_2 \oplus f(R_1, K_1) \\
&= L_1 \oplus \underline{f(R_1, K_1) \oplus f(R_1, K_1)}
\end{aligned}
$$

$$L_6 = L_1$$

$$
\begin{aligned}
R_6 = L_5 &= R_4 \oplus f(L_4, K_2) \\
&= R_3 \oplus f(L_3, K_2) \\
&= L_2 \oplus f(R_2, K_2) \oplus f(R_2, K_2) \\
&= L_2 \oplus (000 \cdots 0) \\
&= L_2 = R_1
\end{aligned}
$$

$$\Rightarrow \underline{R_6 = R_1}$$

$\Rightarrow$ Decryption is the inverse of Encryption.