Feistel Cipher Structure.

Feistel cipher is not a specific structure of block cipher

It is a design model from which many different block ciphers are derived.

DES is just one example of a feistel cipher.

A cryptography system based on feistal cipher structure ~~ad~~ use the same algorithm for both encryption and decryption.

In the feistal block cipher each block has to undergo many rounds where each round has the same function.

Function of Feistal structure

The plain text is divided in two equal halves L_0 and R_0

The two half of the data pass through n round of processing and then combine to produce the cipher text block.

On the right ~~data~~ half we apply a function and in the function we will use a sub key generated from the master key

The output of this is XoRed with the left half and then the output will be swapped (one single round)

Note: We will have (n round) → depend upon the algorithm all round will have the same structure

Note: If any algorithm we divided the plain text in two half and apply the function on right hand side and XOR it will left hand side and the output is swapped. Then that algorithm follow feistal structure.

Now,

Block size, Key size, subkey generation algo no of rounds and round function.

Block size larger block size means more security

Key size larger key size means more security (but it may decrease the processing of encryption and decryption)

no of rounds More round more secure

Subkey generation More complex algorithm difficult for attacker to steal data.

round function more complex function harder for the crypt analyser to attack.

Eg $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ encoding matrix

(PRE) (PAR) (E27t) (027N) (EGO) (LIA)

[16,8,5] [16,1,18] (5,27,20) (15,27,14) [5,7,15] (20,9,1)

[16,8,5] $\begin{bmatrix} -3 & -3 & -4 \\ 6 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ [-122 23 132]

[16,1,18] $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ [-123 19 139]

[5,27,20] $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ [-176 47 181]

[15,27,14] $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ [-182 41 191]

[5,17,15] $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ [-96 22 101]

[20,9,1] $\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$ [-183 32 203]

decoding matrix is $A^{-1} = \frac{1}{|A|} \text{adj } A$

$|A| = -3(4-3) + 3(0-4) - 4(0-4)$
$= 1 \neq 0$ A^{-1} exist

$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & -3 \\ 4 & -3 & 3 \end{bmatrix} = A^{-1}$

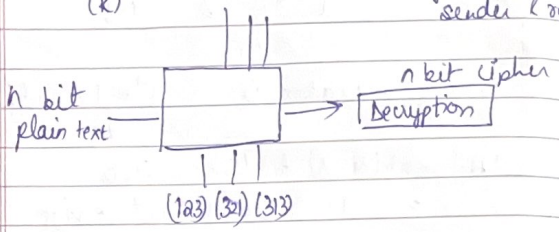
Components of Block ciphes
Modern Block cipher normally are key substitution cipher in which the key allow only partial mapping from the possible input to the possible output

① Modern Block cipher made of combination of transposition (permutations) (pbox or dbox) unit of diffusion called D-Box

② Substitution (confusion) (also called S-box)

A symmetric key modern block cipher encrypt an n bit block of plain text or decrypt n bit of cipher text.

The encryption or decryption algorithm use n bit (K) (will be same for both sender & receiver)



Substitution and Transposition
A modern block cipher can be design to either act as a substitution cipher or transposition cipher

Traditional cipher unlike here the symbol to be substituted or transposed bit instead of character.

Note Modern Block cipher are designed as substitution cipher.

Substitution Technique
Ceaser Cipher
Playfair cipher
Hill Cipher

Ceaser Cipher $1 \leq K \leq 25$
- It is also called shift cipher/additive cipher.
- Each letter in the plaintext is replaced by a letter corresponding to a no of shifts in the alphabet.
- It is monoalphabetic ceaser cipher
- It is one of the earliest and simplest method of encryption technique.

Eg He used a key of 3 for communication
plain → Meet Me | Zebra
Cipher →

Encryption $C = E(K, P) = (P + K) \bmod 26$ (message)

Decryption $P = D(K, C) = (C - K) \bmod 26$ (cipher text)

Numerical values assigned to each letters

a	b	c	d	- - -	x	y	z
0	1	2	3	- - -	23	24	25

If the cryptanalist/attacker knows a cipher text, then he can apply brute force technique to find the plain text by using all the possible 25 keys.

Question on Pg. (19 - 22) Since it is a part of symmetric encryption same key is used for encrypt & decrypt

Sunil
DATE
PAGE
"Rough 'n' Fair"

Playfair cipher (digraph substitution cipher) created

- developed by charles in 1845
- In this we encrypt a pair of alphabets (digraphs) instead of a single alphabet
- fast to use

Key → Sheep
Plain text → Communication

S	H	E	P	A
B	C	D	E	G
I/J	K	L	M	N
O	Q	R	T	U
V	W	X	Y	Z

CO MX MU NI CA TI ON
BQ LY NT IK GH OM VI

Sunil
DATE
PAGE
"Rough 'n' Fair"

Key → Information
Plain Text → Attack on Sunday

I/J	N	F	O	R
M	A	T	B	C
D	E	G	H	K
L	P	Q	S	U
V	W	X	Y	Z

at ta ck on Su nd ay

TB BT KU RF UL IE BW

Sunil
DATE
PAGE
"Rough 'n' Fair"

Hill Cipher

- Developed by Lester Hill in 1929
- Encrypt a group of letters called polygraph (like in playfair cipher)

This method makes use of Maths

To encrypt
$C = KP \bmod 26$

Step1- Choose a key (key Matrix must be a square matrix

eg Key: VIEW $\begin{bmatrix} V & I \\ E & W \end{bmatrix}$

$\begin{bmatrix} 21 & 8 \\ 4 & 22 \end{bmatrix}$

eg Key = QUICKNESS

$\begin{bmatrix} Q & U & I \\ C & K & N \\ E & S & S \end{bmatrix}$

$\begin{bmatrix} 16 & 20 & 8 \\ 2 & 10 & 13 \\ 4 & 18 & 18 \end{bmatrix}$

Sunil
DATE
PAGE
"Rough 'n' Fair"

Plain text - Attack

Key $= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

Since the key is a 2x2 matrix plain text should be converted into vectors of length 2

Plain text

$\begin{bmatrix} A \\ T \end{bmatrix} \begin{bmatrix} T \\ A \end{bmatrix} \begin{bmatrix} C \\ K \end{bmatrix}$

① $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix}$

$\begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$

② $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix}$

$\begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 \quad \begin{bmatrix} M \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$

③ $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26$

$\begin{bmatrix} 8 \\ 14 \end{bmatrix}$ I O

FKMFIO

For decryption

$$P = K^{-1} C \bmod 26$$

FKMFIO

$$Key = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$

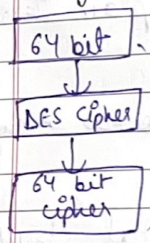
$$\begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix}$$

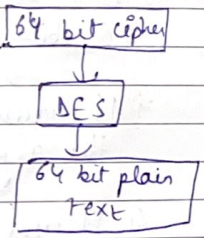
30 - 30

DES - Data Encryption Standard System
Symmetric algo
Block cipher
64-bit - plain text
(16- rounds) Fiestal structure
Key size - 64 bit Key
56 bit (take) → 48 bits
↓
sub key - 16 sub key

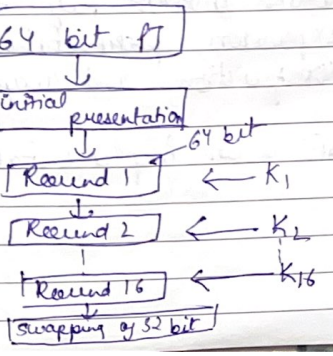
Encryption



Decryption



DES algo (General Structure)



Sunil
DATE
PAGE
"Rough 'n' Fair"

↓

Final permutation

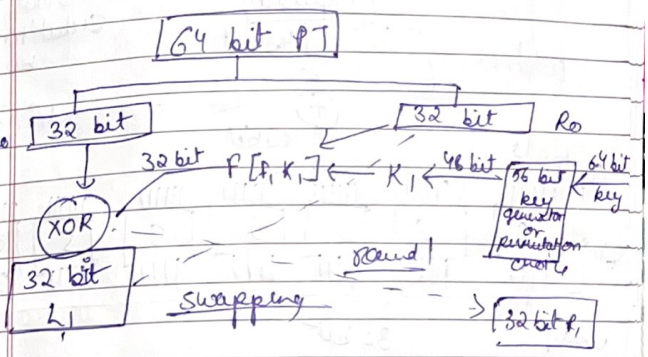
↓

64 bit cipher

Note:
1) DES i.e Data encryption standard, it is a symmetric key block ciphes
2) Published by NIST i.e National institute of Standard and Technology
3) DES encrypt 64 bit plain text to 64-bit cipher text
4) 16 round in DES provide strengthness the algorithm...!
6) It uses 16 round feistal structure
7) Each round has the same function which involve key transformation expension, permutation, s-box, p-box XOR function and swapping
5) DES is an implementation of a feistal cipher

Sunil
DATE
PAGE
"Rough 'n' Fair"

Rounds in DES (what function will be applied in round function)



Till swapping it is round 1

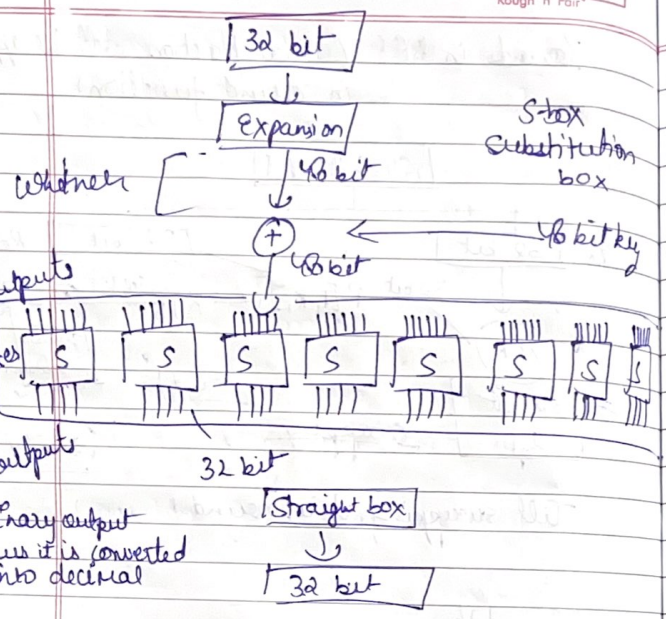
Round 16

DES Function
The heart of the cipher is the DES function (F) which is already defined in DES function or in DES round.

It apply 48 bit key to the rightmost 32 bit to produce 32 bit output

↓

Expansion p-box
whitener (xored), substitution
group of substitution box (S-box), straight box (p-box)



Shannon's theory of confusion & diffusion

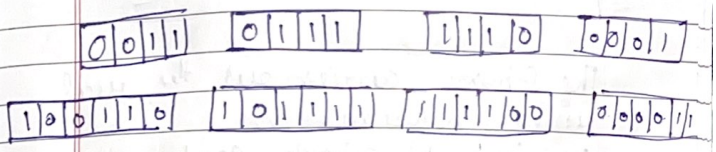
The terms confusion and diffusions were introduced by claude Shannon

Shannon's concern was to prevent crypt analysis, based on statistical analysis. The reason is as follows

Assume attacker has some knowledge of the statistical characteristics of the plain text (eg in a msg, the frequency distribution of the various letters may be known)

function of Expansion inside the function of DES.

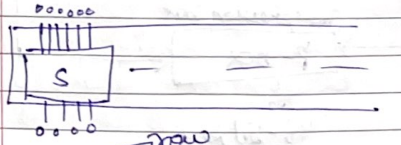
Note - $4 \times 8 = 32$ bit
$6 \times 8 = 48$ bit



Expansion permutation box
since right input is 32 bit and second key is a 48 bit key we must need to expand right input to 48 bit

Note
Whitener
XOR operation b/w 48 bit key and 48 bit output from expansion box.

Substitution box



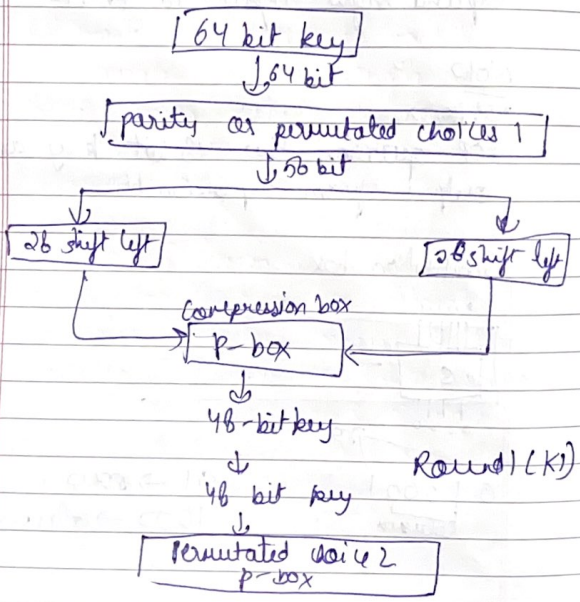
01 → row
1000 → column

S-box Table 1

	0	1	2	—	—	—	15
0	16	23	19	—			—
1	2	3	45	—	—	—	
2	—		—		—		
3	—		—		—		—

The S-boxes carries out the real mixing (confusion)
DES uses 8 s-boxes each with a six bit input and 4 bit output.

Generation of keys in DES



48 bit key → K2

Q Find out weakness & strength of DES algo

Strengths

a) The use of 56-bit keys : 56 bit key is used in encryption, there are 2^{56} possible keys. A brute force attack on such number of keys is impractical.

b) The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristics of DES algorithm but no one has succeeded in finding out the weakness.

Weakness

weakness has been found in the design of the Cipher

a) Two chosen input to an S-box can create the same output

b) The purpose of initial & final permutation is not clear

Sunil
DATE
PAGE
"Rough 'n' Fair"

How does block cipher work?

Design principle of Block ciphers
A block ciphers is design on the following three principles

1. No of rounds
2. Function F design
3. Key schedule algorithm

No of rounds
This block ciphers design principle indicates the overall strength of the ciphers algorithms.
In short the more the no of rounds the greater is the strength of the block cipher making it more difficult to break into or decrypt the algorithm.

Function F design
Based on the feistal structure the encryption process consist of multiple rounds of plain text processing where the input block of each round is denoted by two half i.e left half and right half.

Function F is essentially an encrypting function that takes the encryption key (K) and (r) as the input and produce the encrypted output. It is the block cipher design principle that determine security. Function f should be designed in such a way that it cannot be substituted.

function F provide the strength to the algorithms

Key schedule algorithm
The key schedule algorithms calculates the round key
This algorithm defer according to the block scheme / cipher / method.

For eg The key schedule algorithm in the DES scheme divide the 56 bit key into two half of 28 bit each then these two go into the p-box and converted into 48 bit key by compression.

Eg: DES, 2DES, 3DES, AES, IDEA, etc.