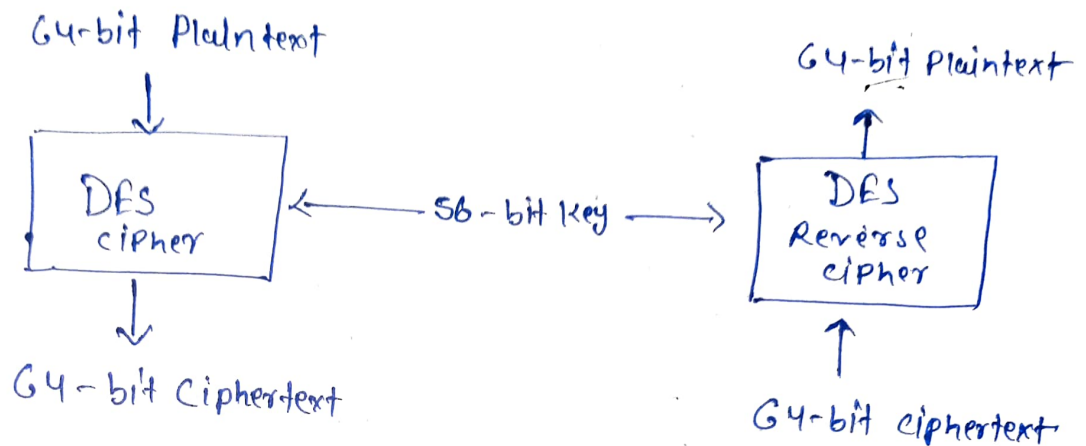


Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a Symmetric-key block cipher.

DES is a Block cipher (use 56 Bit Key)

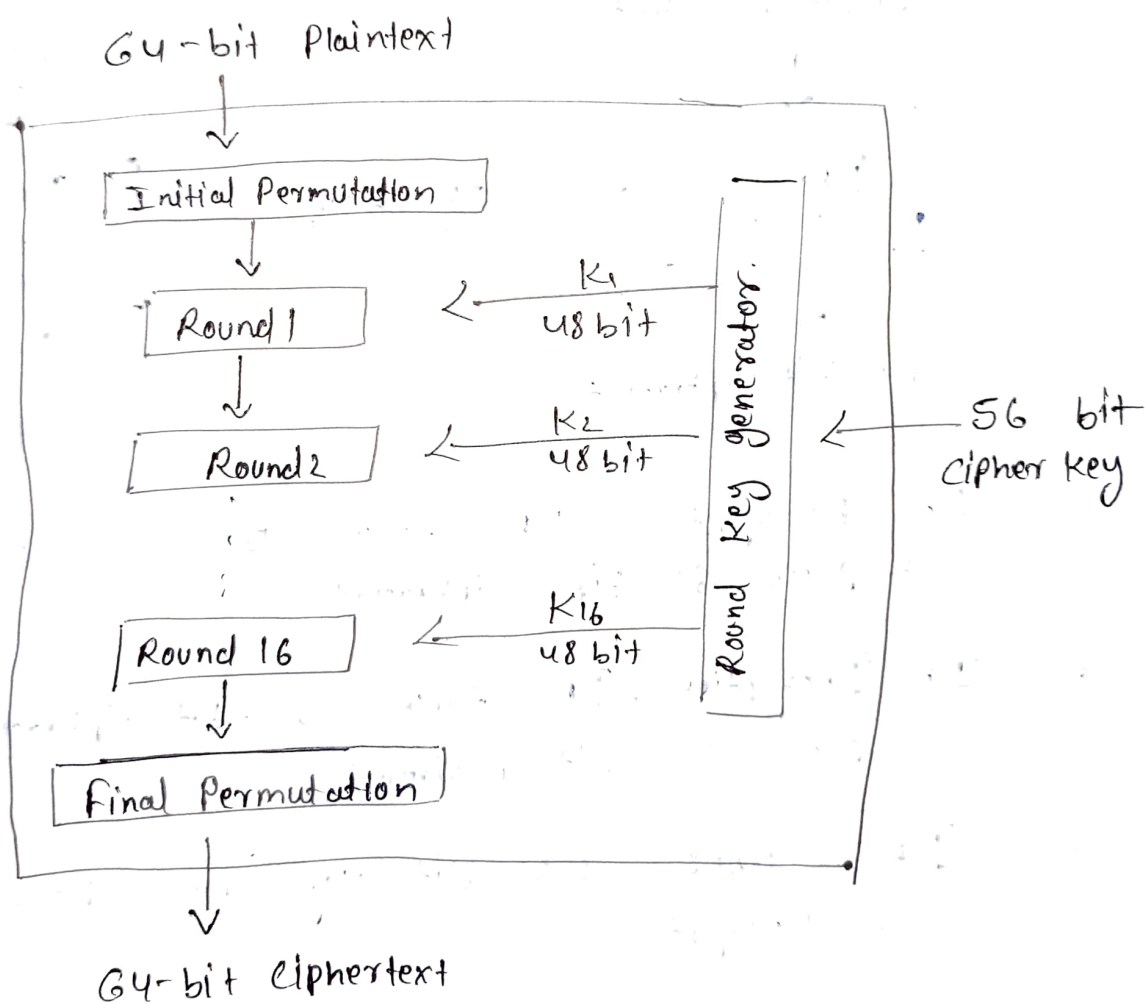


→ In Encryption, DES takes ~~56~~ 64 bit Plaintext & gives 64 bit Ciphertext

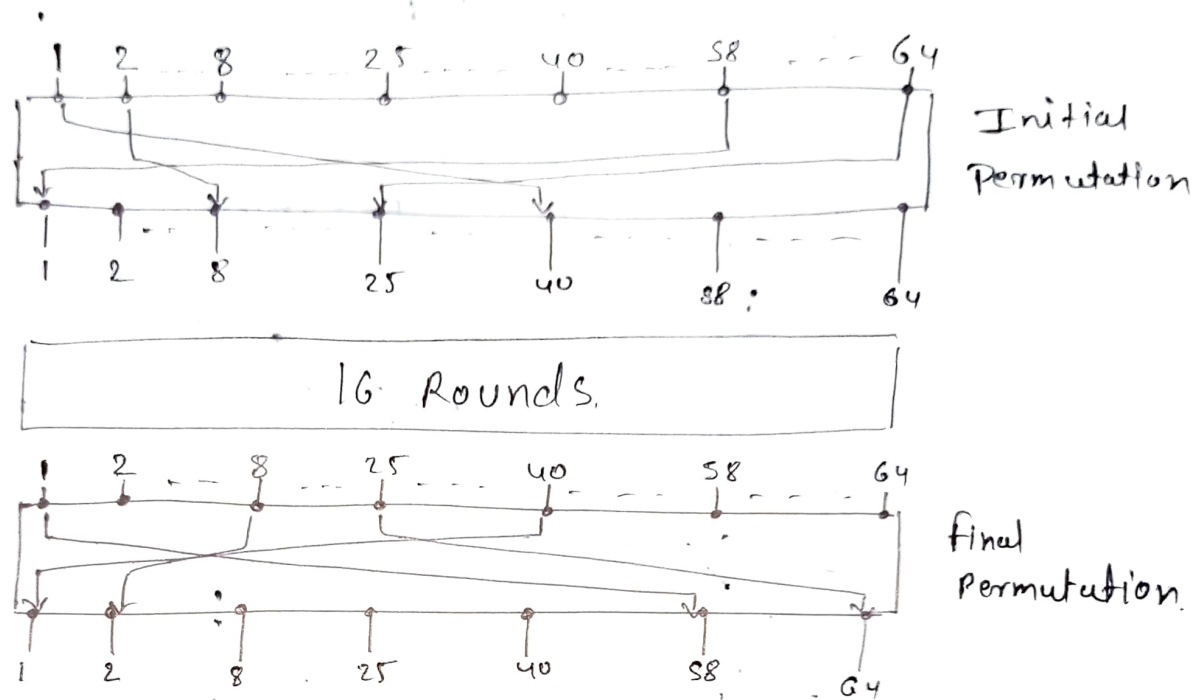
→ In Decryption, DES takes 64-bit ciphertext & gives 64-bit Plaintext

→ DES uses 56 Bit Key for Both encryption & Decryption.

DES Structure! The Encryption Process is made of two permutations (P-boxes) which are initial and final Permutation box. & Sixteen feistel rounds. Each round uses different 48-bit key generated from round-key-generator.



Initial & final Permutation P-Box Structure:-



Each of these P-Box take 64-bit input and Permutes them according to a predefined rule.

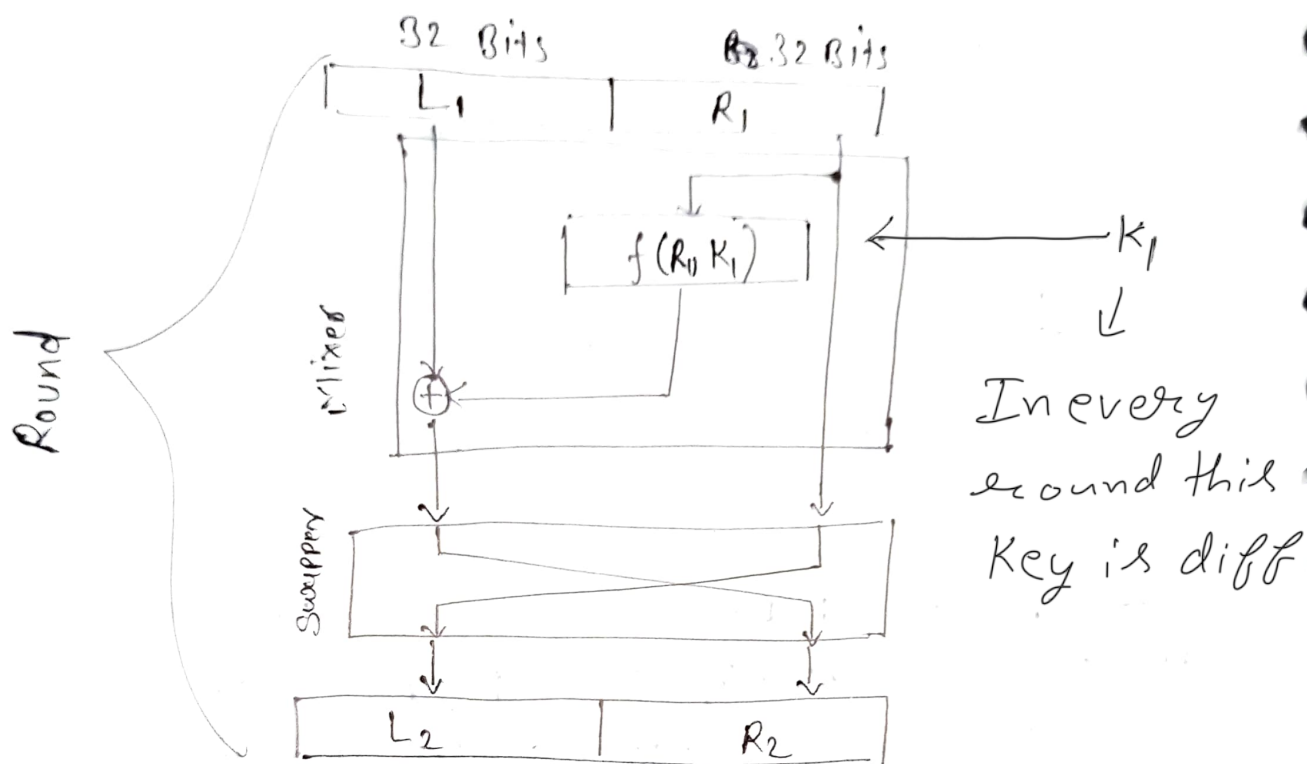
These P-Box uses keyless Straight Permutation that are inverse of each other.

* Initial & final P-Box are inverse of Each other.

Rounds :- DES uses 16 Round.

Each round of DES is feistel cipher.

One Single round in DES:-



The round takes the input from the previous round or Initial P-Box, & gives the output to the next round or final P-Box.

Each round has 2 components, one is Mixer & another one is Swapper.

Each component is invertible.

The Swapper is obviously invertible. The Mixer is also invertible because it is using XOR operation.

All the Non-Invertible components are contained in $f(R_1, K_1)$

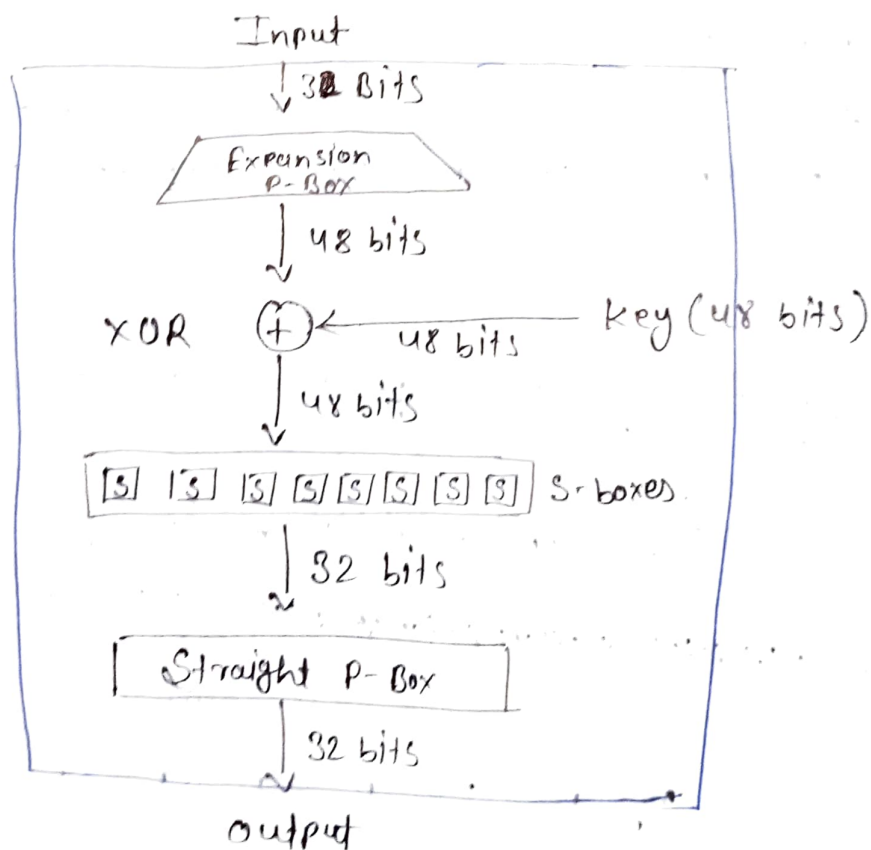
4. DES function :- The heart of DES is

DES function. The DES function applies 48-bit key to the Rightmost 32 bits (R) to produce 32 bit output.

This function is made up of four sections:-

- an Expansion P-Box
- whitener (for adding key)
- Group of S-Box
- Straight P-Box.

$$f(R, K) =$$



Expansion P-Box: Since R is 32 bit input

K is 48 bit key.

We first need to expand 32 bit to

48-bits.

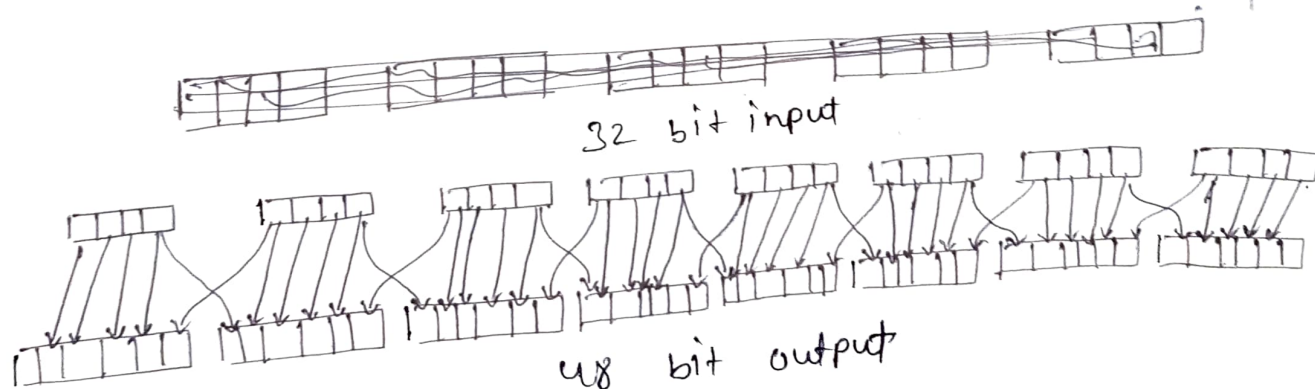
R divided into 8 4-bit group After this each 4-bit group is expanded to 6-bit group. This expansion follow some predetermined

Rule. for each section input 1,2,3,4 are copied to output 2,3,4,5, respectively.

output 1 come from the 6th bit from the previous section &

output 6 come from the 1st bit of the next section.

the first & the last section is considered to be the adjacent to each other.



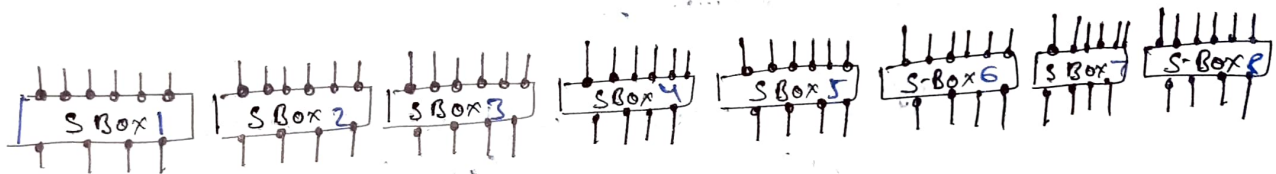
Expansion
P-Box
Table \Rightarrow

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	01

Whitener (XOR) :- After the expansion permutation, DES uses the XOR operation on the right section and the round key. Both right section and round key is of 48 bit. in length.

The round key is used in only this operation.

S-Boxes :- The S-Boxes do the real mixing (confusion)
~~Des~~ DES uses 8-S-Boxes. each with 6 input & 4 output.



The 48-bit data from the above operation is divided into eight chunks of 6 bit & feed to these boxes. The result of each box is 4 bit. After combining these bits the result is 32 bit. The Substitution in each box is predetermined based on 4x16 table.

The table for S-box 1 :-

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	10	3	6	12	11	09	5	3	8
2	4	1	14	8	13	16	6	2	11	15	12	9	7	3	10	5
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

How to read this table:-

Example: Input to S-box is 100011, what is the output.

write first bit & the sixth bit together

we get 11 \rightarrow 3 (decimal). the remaining bits are 0001 \rightarrow 1 (decimal)

So we have to look

~~3rd column & 1st~~

3rd row & first column.
(11) (0001)

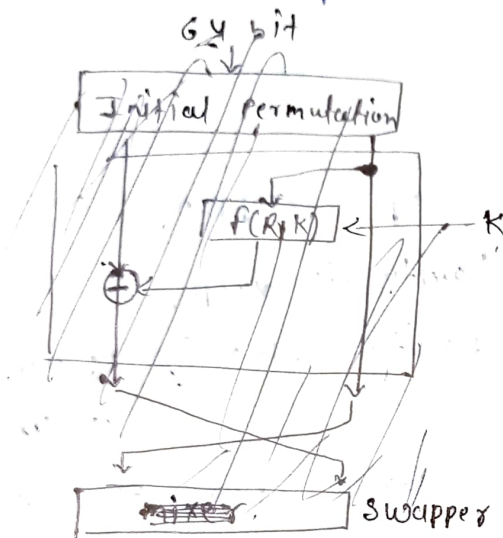
the output is 12 \rightarrow 1100 (binary)

Straight P-box: The last operation in DES function is straight permutation with a 32-bit input & 32-bit output.

Cipher and Reverse Cipher: Using mixer and swappers we can create the cipher and reverse cipher each having 16 rounds. The cipher at encryption side and reverse cipher used at decryption side.

We have different approach to achieve cipher & reverse cipher:-

- ① first approach :- To achieve this goal, one approach is to make the last round (round 16) different from other rounds. It has only mixer no swapper.



A very important point we need to remember about this cipher that the round key (K_1 to K_{16}) should be applied in reverse order. At the encryption side round 1 uses K_1 & round 16 uses K_{16} . At the decryption side, round 1 uses K_{16} & Round 16 uses K_1 .

In the first approach there is no swapper in the last round.

Key Generator :-

A Round Key Generator creates sixteen 48-bit key out of 56-bit cipher key.

However the cipher key is normally given as a 64 bit key in which 8 extra bits are the parity bits, which are dropped before actual key generation process.

Parity Drop :- The process of dropping the bit is called Parity-bit drop.

It drops the parity bits (8, 16, 24, 32, 40, 48, 56, 64)

from 64-bit key and permutes the rest of the bits.

The remaining 56-bit key is actual cipher key which is used to generate a 48 bit round key.

Key with
Parity bit
↓ 64 bits

Parity drop → Compression P-box

Cipher key 56 bits

28 bits 28 bits

Shift left

Shift left

28 bit

28 bit

Compression
P-box

48 bit

Round 1
Key

Shift left

Shift left

28 bits

28 bit

Compression
P-box

48 bit

Round 2
Key

Shift left

Shift left

Compression
P-box

48 bit

Round
16 Key

Shifting

Rounds	Shift
1, 2, 9, 16	One bit
Rest	Two bits

Shift left :- After the Parity drop the

key is divided into two 28-bit parts. Each part is shifted left (circular shift) one or 2 bits. In rounds 1, 2, 9, 16 Shifting is one bit. in the other rounds it shifts 2 bits. Two Parts are combined to form ~~56~~ - ~~112~~ round key.

Compression P-box :- The compression P-box changes ~~56~~ to 56 bits to 48 bits which are used as a round key.

DES Analysis :-

Properties :- Two desired Properties of block cipher are the

- ① Avalanche effect
- ② Completeness

① Avalanche effect :- This means that the small change in plaintext or key should create a significant change in the ciphertext. DES has been proved this Property Strongly.

② Completeness effect :- This means that each bit of the ciphertext needs to depend on many bits in the plaintext. The diffusion and confusion produced by P-boxes and S-boxes in DES, shows the very strong completeness effect.

DES weaknesses :-

② S-boxes :- Two specifically chosen inputs to an S-box array can create the same output.

P-boxes :- It is not clear why the Designers of DES used the initial and final permutations, these have no security benefits.

Weak Key :- 4 out of 2^{56} keys are called weak keys. A weak key is the one that, after parity drop operation, consists of either all 0's or all 1's or half 0's or half 1's.

Semi-weak Key :- There are 6 keys that are called semi-weak keys.

A semi weak key creates only two different round keys & each of them is repeated eight times.