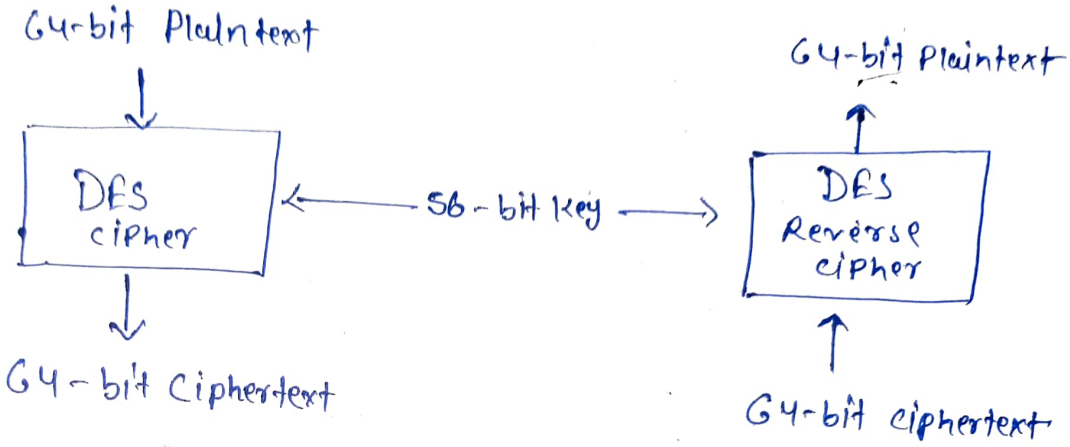
Data Encryption Standard (DES)

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

DES is a Block cipher (use 56 Bit key)

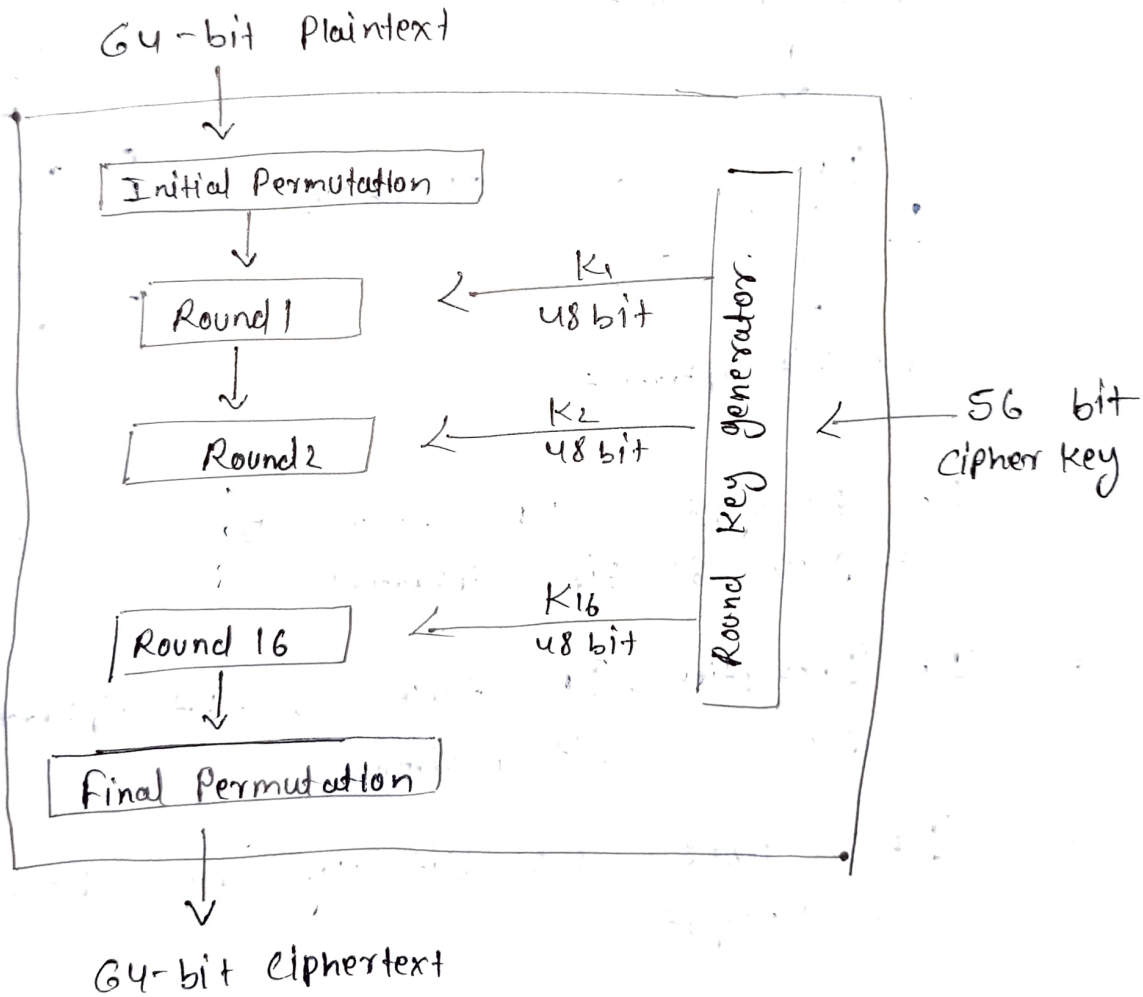


→ In Encryption, DES takes ~~56~~ 64 bit Plaintext & gives 64 bit Ciphertext

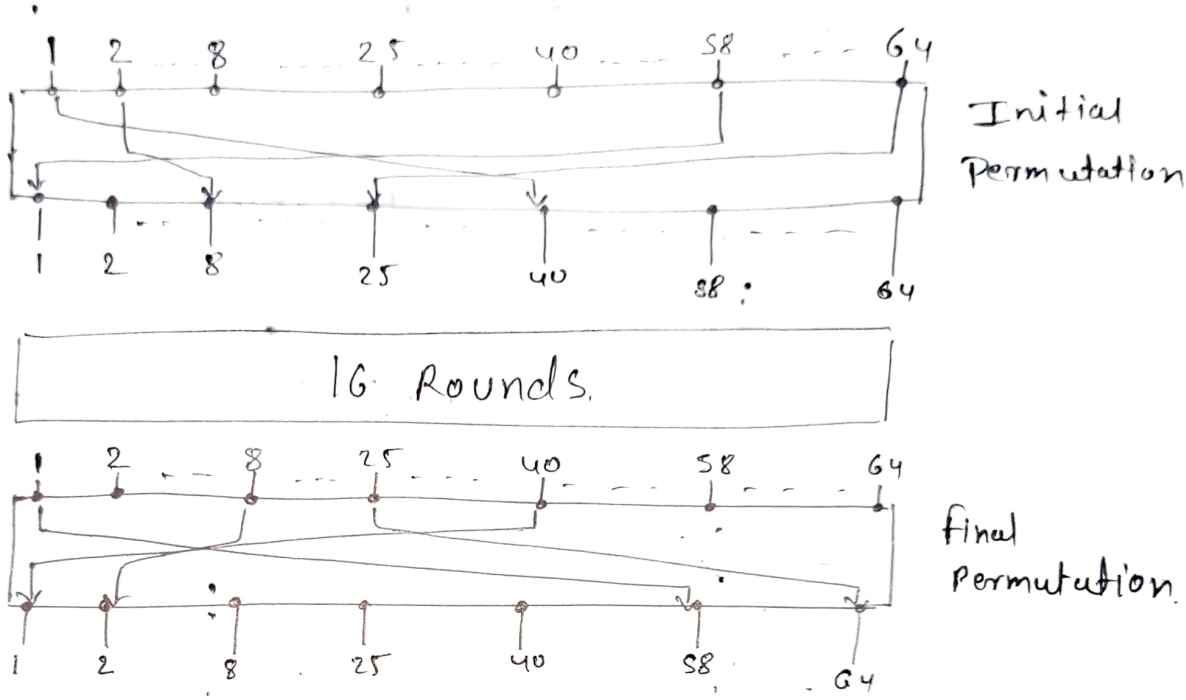
→ In Decryption, DES takes 64-bit ciphertext & gives 64-bit plaintext

→ 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 :-



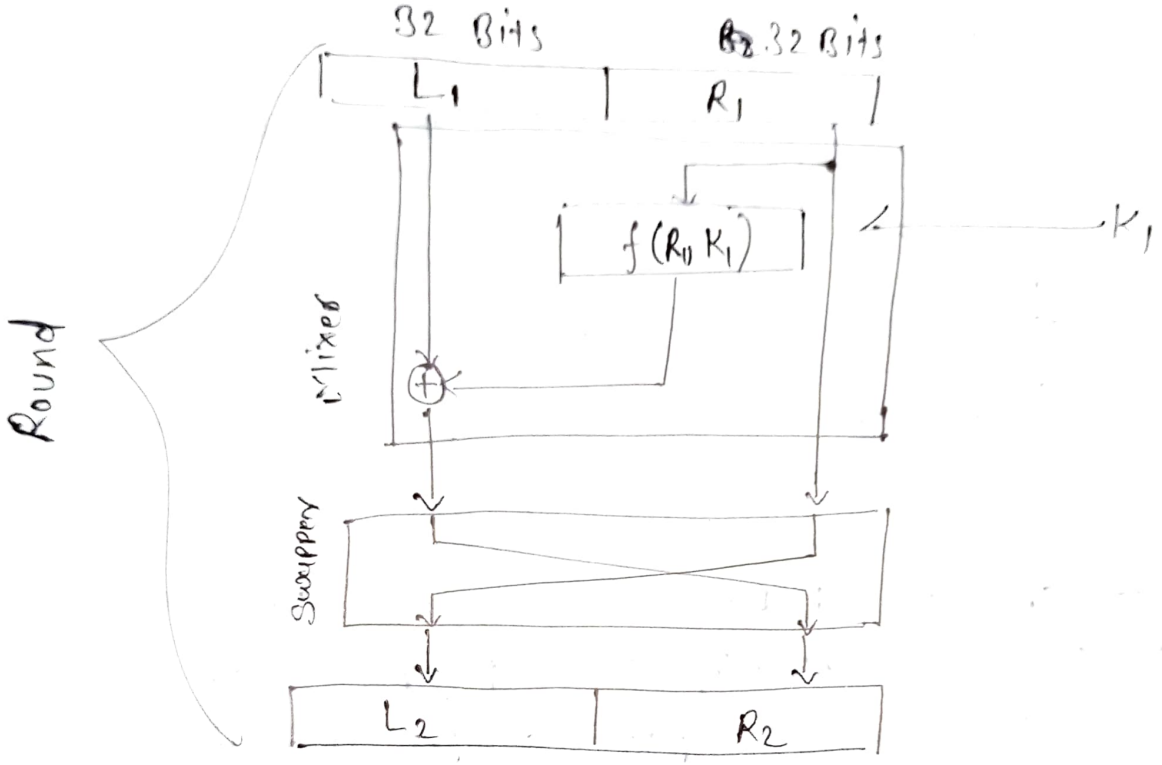
Each of these P-Box take 64-bit input and Permutes them according to a predefined rule. These P-Box uses keyless Straight Permutation that are inverse of each other.

* 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 take the input from the Prevous Round or Initial P Box.
& Gives the output to the Next round or final P-Box.

Each Round has 2 component, one is Mixer & another one is swapper.

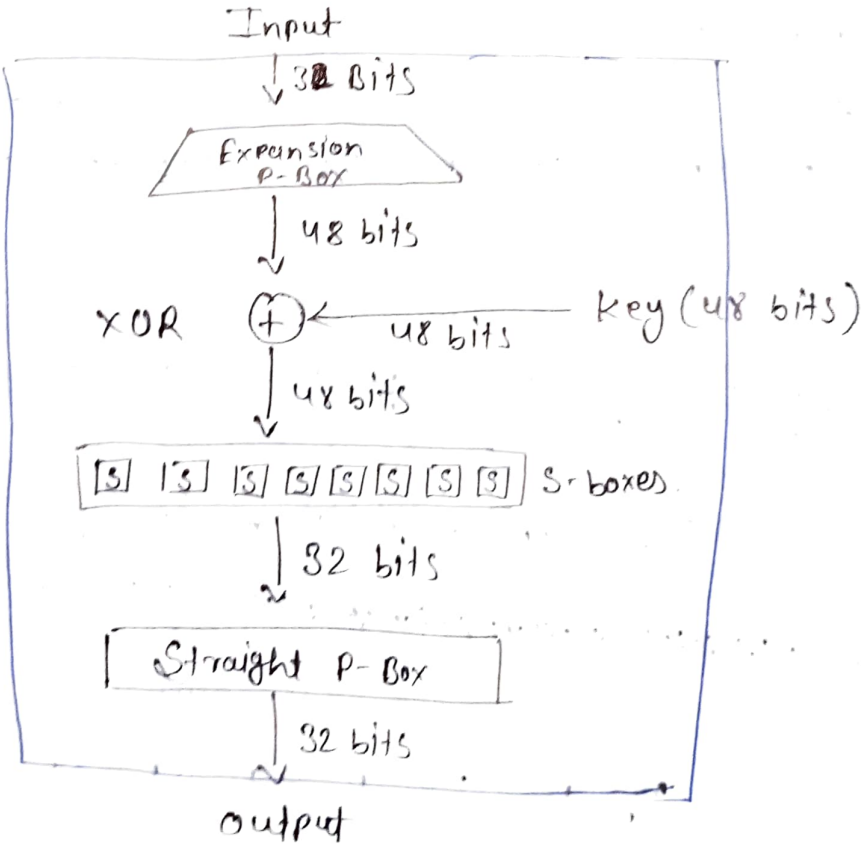
Each component is invertible,
The swapper is obiously invertible. The Mixer is also Invertible Because it is using XOR operation.
All the Non-invertible components are contained in $f(R_1, K_1)$

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

$f(R, K) =$

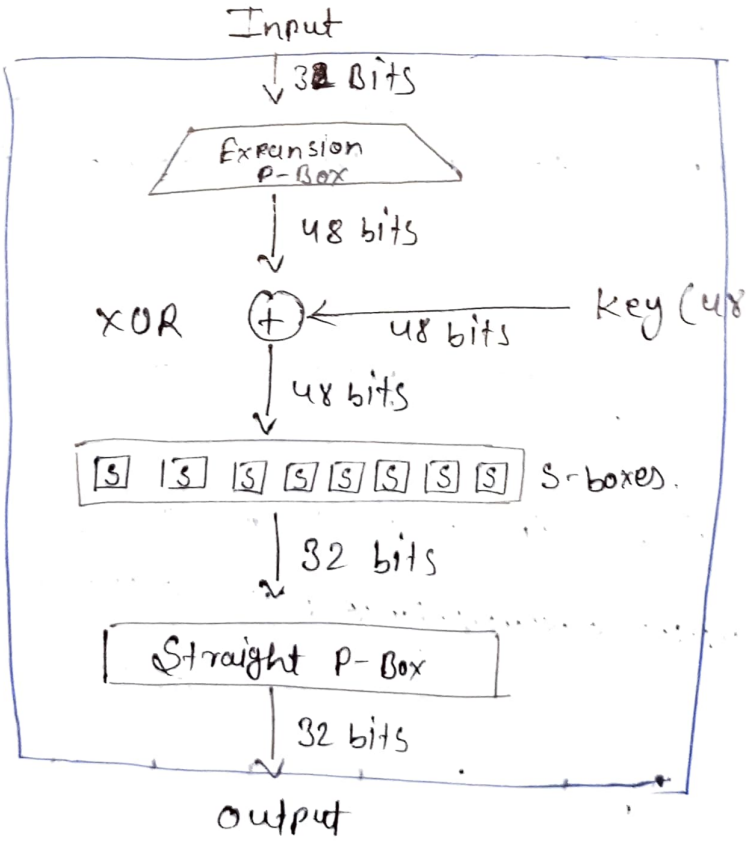


DES function :- The heart of DES is DES function. The DES function applies 48-bit key to the Rightmost 32 bits (R) to produce 32 bit output.

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.

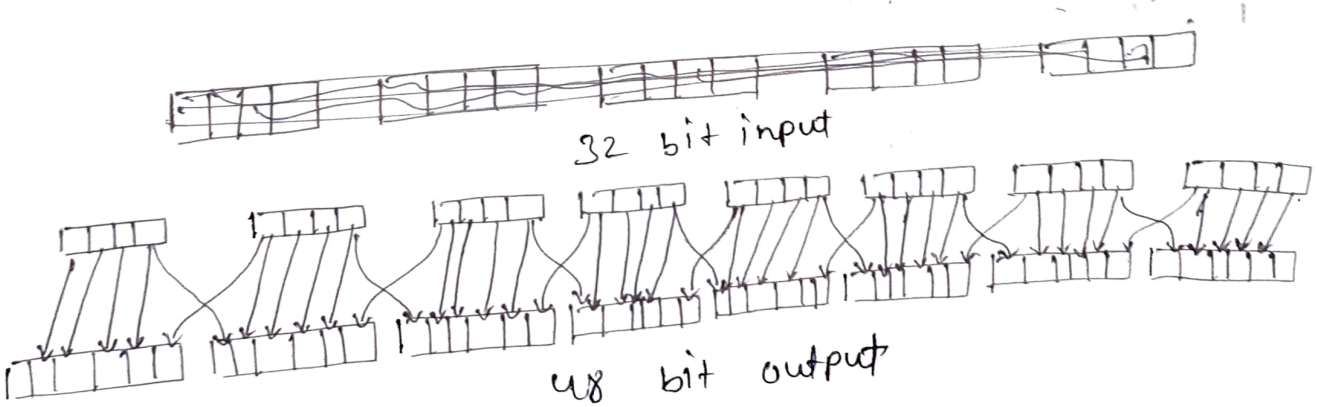
We first need to Expand 32 bit to 48-bits.

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

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

the first & the Last section is considerd to be the adjcent to each other.



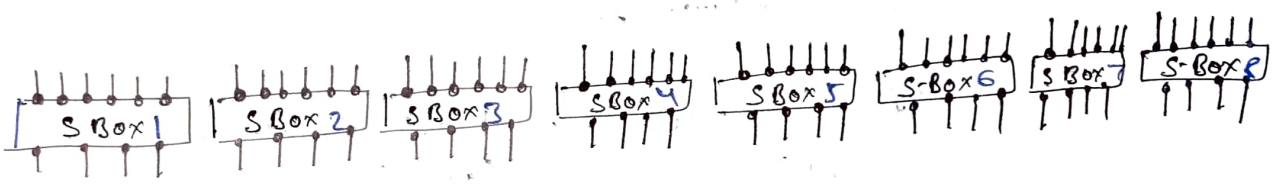
Expansion P-Box Table =>

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 devided 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 predetermind 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-box1 is 100011. What is the output.

write first bit & the sixth bit together

we get 11 → 3 (decimal). the remaining Bits are 0001 → 1 (decimal)

So we have to look

~~3rd column & 1st~~

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

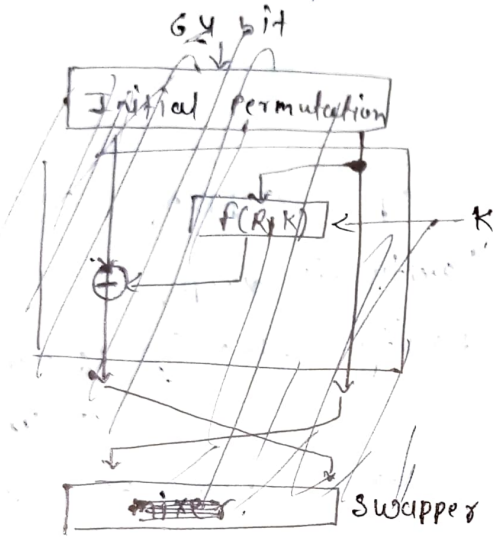
the output is 12 → 1100 (binary)

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 approch to achieve cipher & reverse cipher :-

(1) first approch :- 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 round1 uses K1 & round 16 uses K16. at the decryption side, round1 uses K_{16} & Round 16 uses K_1.

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

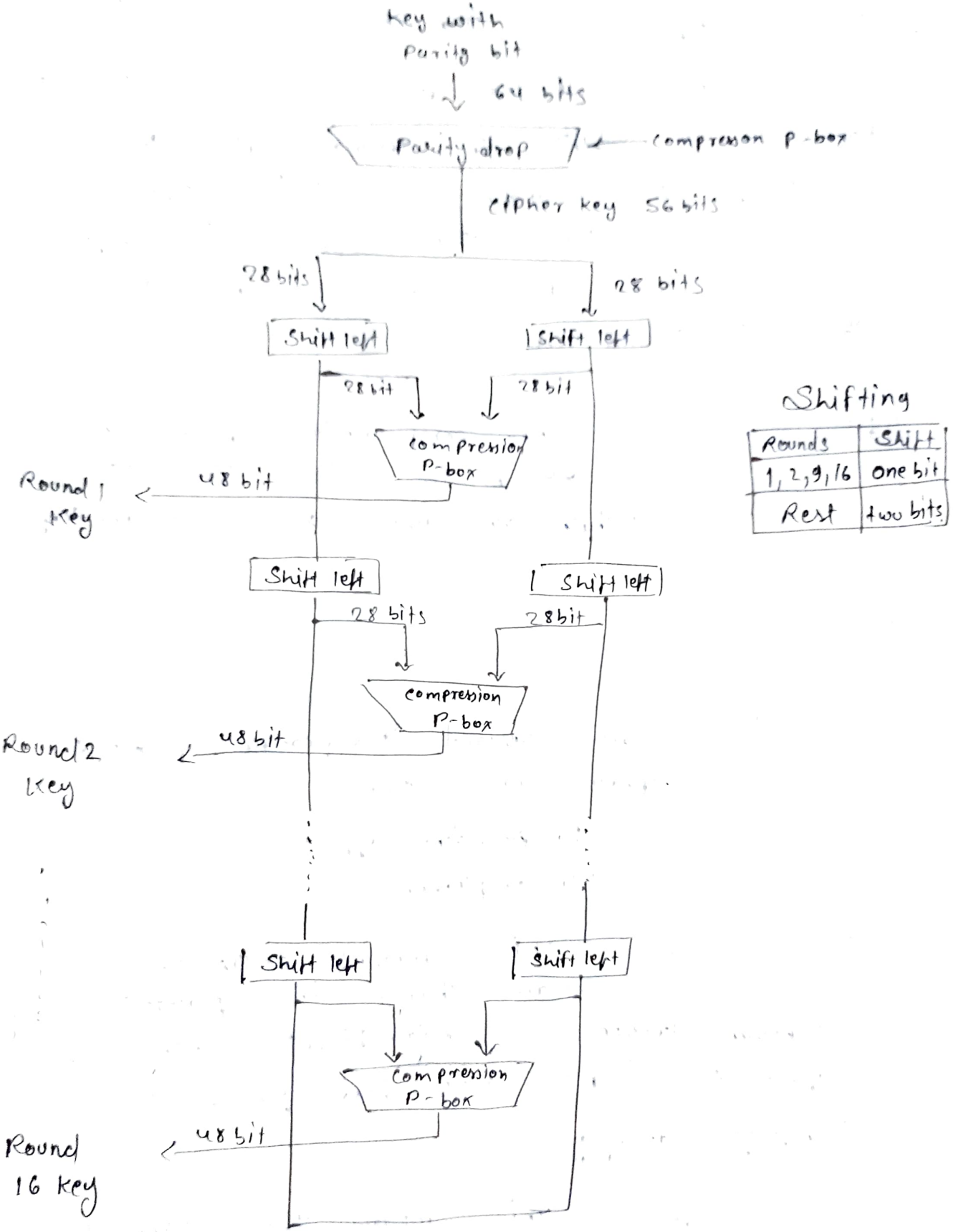
Key Generator :-

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 bit 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.



Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Rest	two bits

Shift left :- After the Pparity 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-bit round key.

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

DES Analysis :-

Properties :- Two desired Properties of block cipher are the

(1) Avalache effect
(2) Completnes

(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) Completnes 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 completnes effect.

DES weaknesses :-

- **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 benifits.

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.