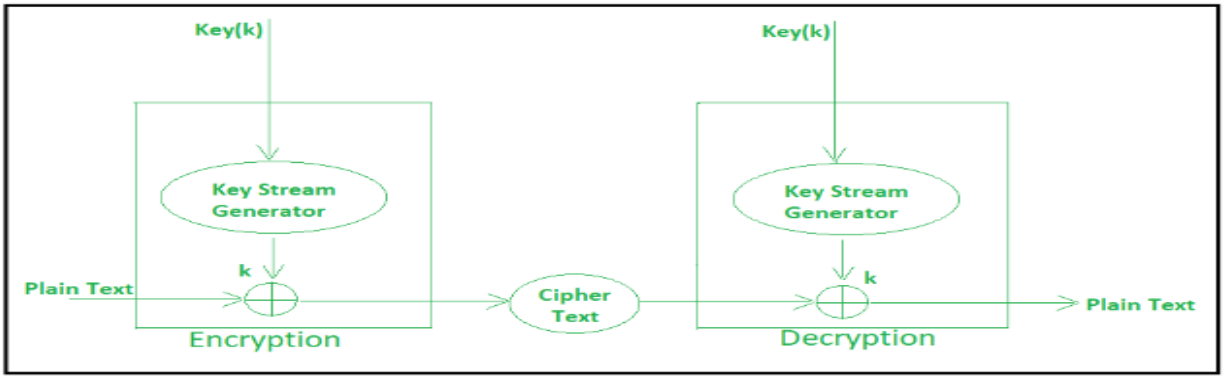
BLOCK CIPHER

A. Stream Cipher:

A stream cipher is an encryption technique that works byte by byte to transform plain text into code that's unreadable to anyone without the proper key. It is a symmetric key cipher (the same key both encrypts and decrypts messages).



(Explain the above diagram in examination. Make sure the diagram is not skipped at all.)

Encryption :

For Encryption,

- Plain Text and Keystream produces Cipher Text (Same keystream will be used for decryption.).
- The Plaintext will undergo XOR operation with keystream bit-by-bit and produces the Cipher Text.

Plain Text : 10110110
⊕ **Key** : 01010101

Cipher Text : 11100011

Using XOR Table		
1	0	**1**
0	1	**1**
1	1	**0**
0	0	**0**

Decryption :

For Decryption,

- Cipher Text and Keystream gives the original Plain Text (Same keystream will be used for encryption.).
- The Ciphertext will undergo XOR operation with keystream bit-by-bit and produces the actual Plain Text.

Using XOR Table		
1	0	1
0	1	1
1	1	0
0	0	0

⊕

Cipher Text : 11100011
Key : 01010101

Plain Text : 10110110

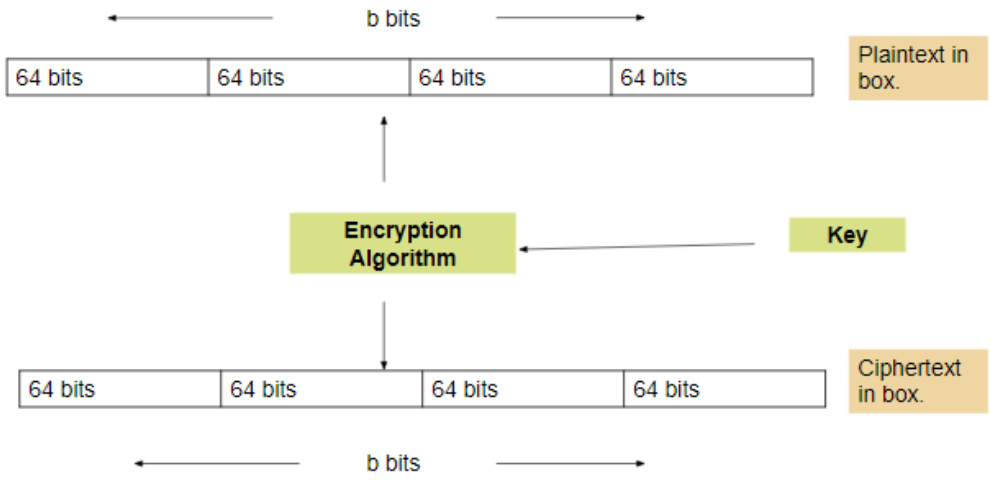
For practice solve the following-

1. **P.T-** 10111001 and **Key Stream-** 10101011
2. **P.T.-** 11100011 and **Key Stream-** 01010101
3. **P.T-** 10011001 and **Key Stream-** 11000011
4. **P.T-** 010111001 and **Key Stream-** 100101011

****

B. Block Cipher:

A block cipher encrypts data in blocks using a deterministic algorithm and a symmetric key. As in the case of stream ciphers, most encryption methods encrypt bits one by one (stream ciphers). In this, a block of plain text is treated as a whole and used to produce the cipher text of equal length. Typically, the block size is 64 bits and 128 bits.



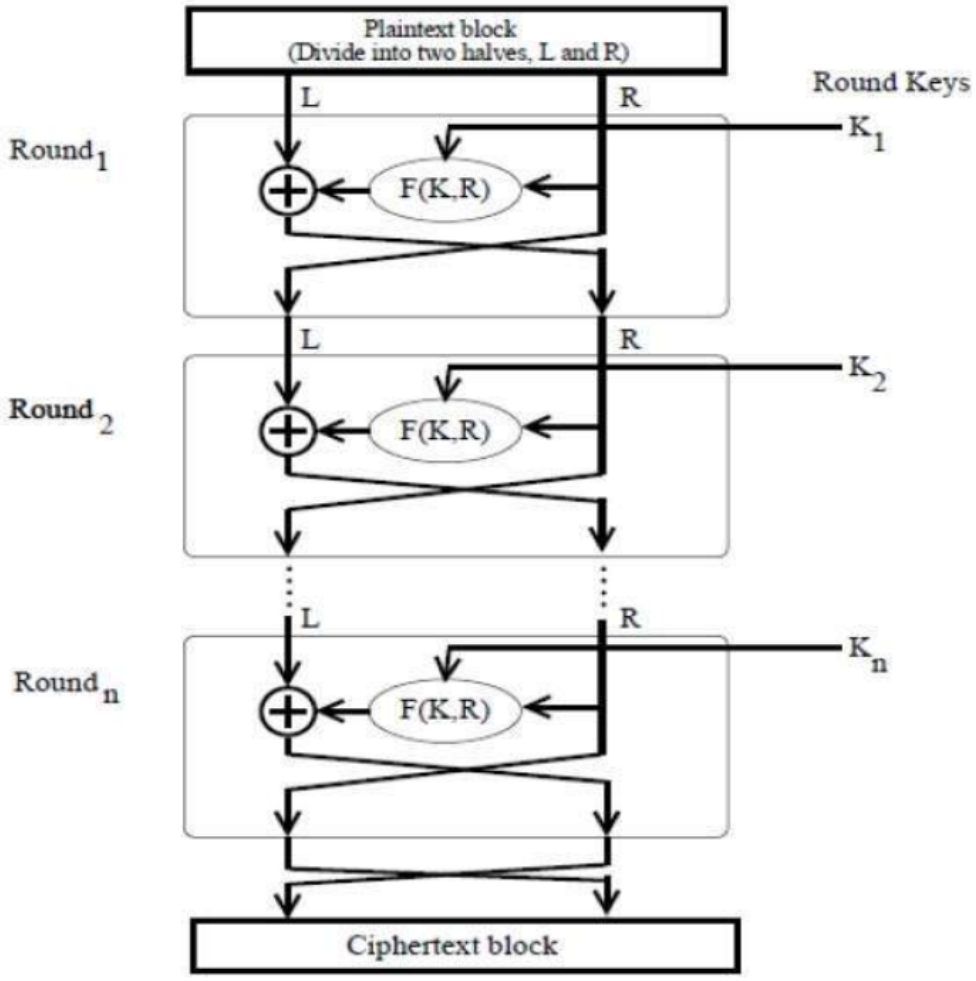
➔ Best example of Block Cipher is DES (Data Encryption Standard)

FEISTEL STRUCTURE AND ITS WORKING

Feistel Block Cipher:

Feistel Cipher is not a specific scheme 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 cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.

Following is the Feistel structure/ Block diagram of Feistel cipher:



Encryption Process:

1. PlainText/ Input block of n bits is divided into 2 equal halves. I.e. LPT (Left Plain Text) and RPT (Right Plain Text).
2. RPT remains unaffected in each round.
3. But on LPT operation is performed. An encrypting function 'f' which accepts t inputs namely- Key and RPT. The function 'f' generates output f(k,RPT). And then XORed with the LPT.
4. Further, modified LPT and unmodified RPT are swapped at the end of each round.
5. After completion of the last round LPT and RPT are combined/merged to produce CipherText.

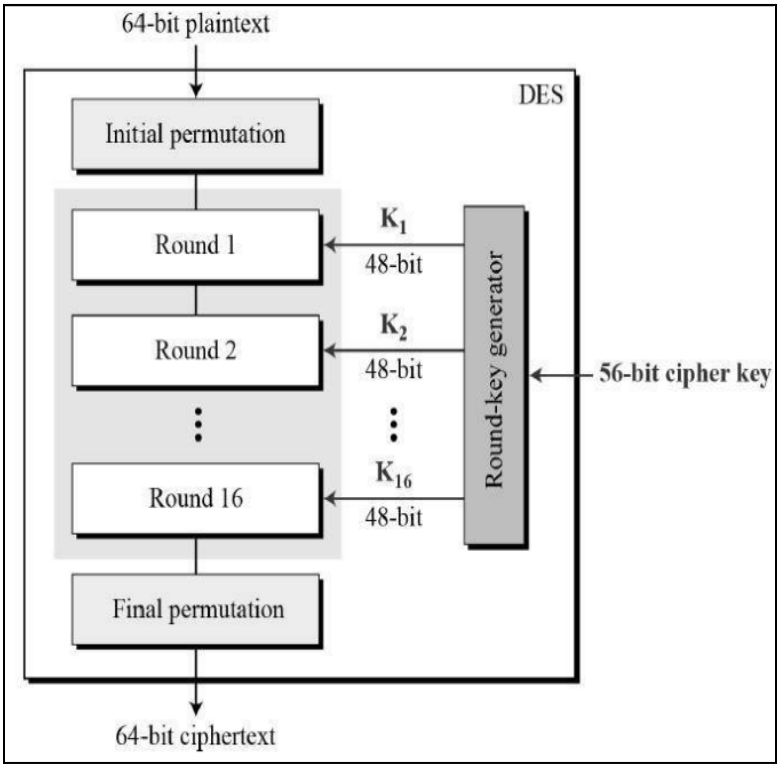
Decryption Process:

The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same as described in the above diagram.

****

DES (DATA ENCRYPTION STANDARD)

Data Encryption Standard:



- It is a block cipher.
- The Data Encryption Standard (DES) is a symmetric-key block cipher.
- 64 bit Plain Text block.(it encrypts the data in block of size 64 bits each).
- 16 rounds each is a Feistel round.

Steps:

1. Initial **Permutation.**
2. 16 Feistel round.
3. Swapping/ left right swap.
4. Final permutation/ Inverse initial permutation.

➔ **Conversion of 62 bits of key into 56 bits(KEY TRANSFORMATION)-**

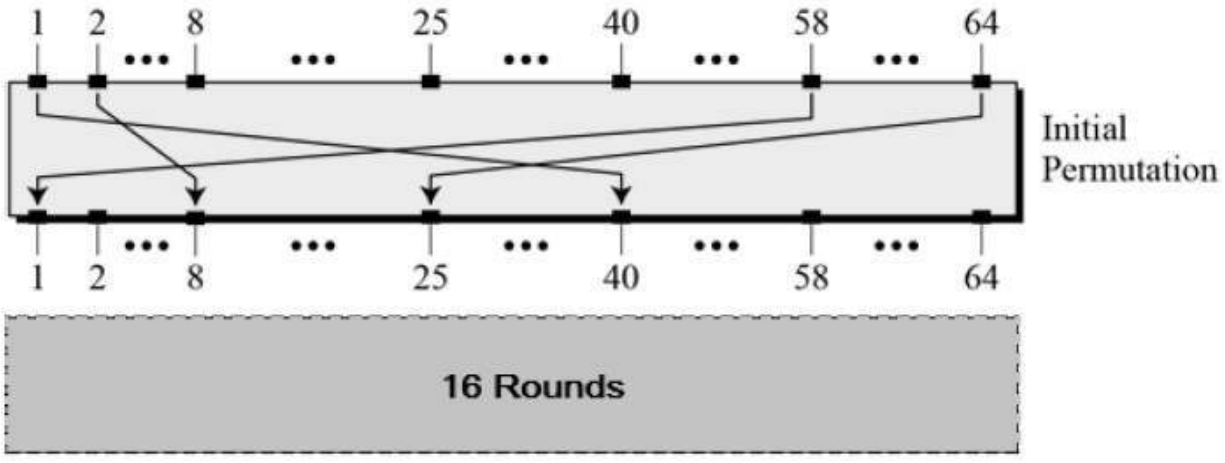
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Figure - discording of every 8th bit of original key

- The initial key consists of 64 bits.
- However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key.
- That is, bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.
- From this 56 bit key, a different 48 bit sub- key is generated during each round using a process called Key Transformation. *(Selection of the 48- bit sub-key has some different working. For now, we will just consider the that there is some transformation mechanism is used on 56 bit key to generate 48-bit sub-keys from it)*

STEPS:

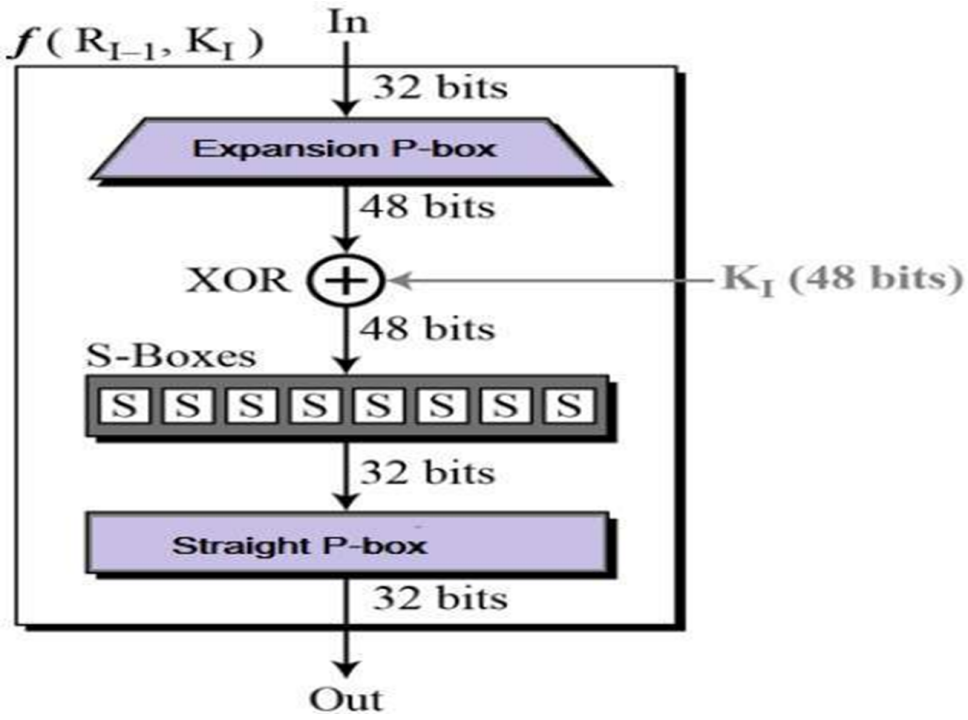
➔ **Initial Permutation:**



The initial permutation (IP) happens only once and it happens before the first round.This is nothing but jugglery of bit positions of the original plain text block. The same rule applies to all the other bit positions.For example, it says that the IP replaces the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block, and so on.

After IP is done, the resulting 64-bit permuted text block is divided into two half blocks. Each half-block consists of 32 bits, and each of the 16 rounds, in turn, consists of the broad level steps.

➔ **Working of Function:**



- **Expansion Box or Expansion Permutation:**

Expansion Box:

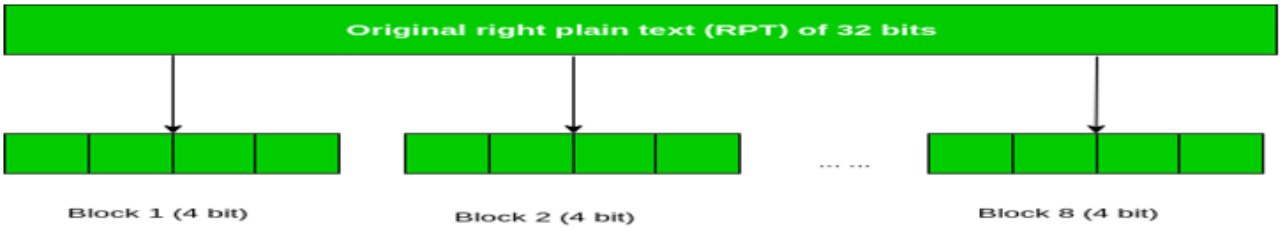
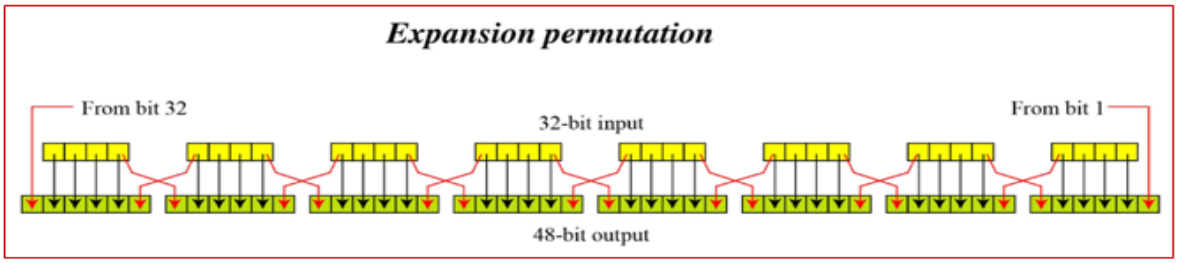
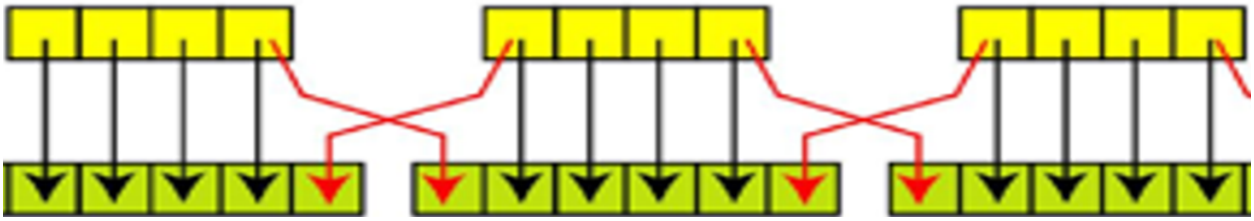


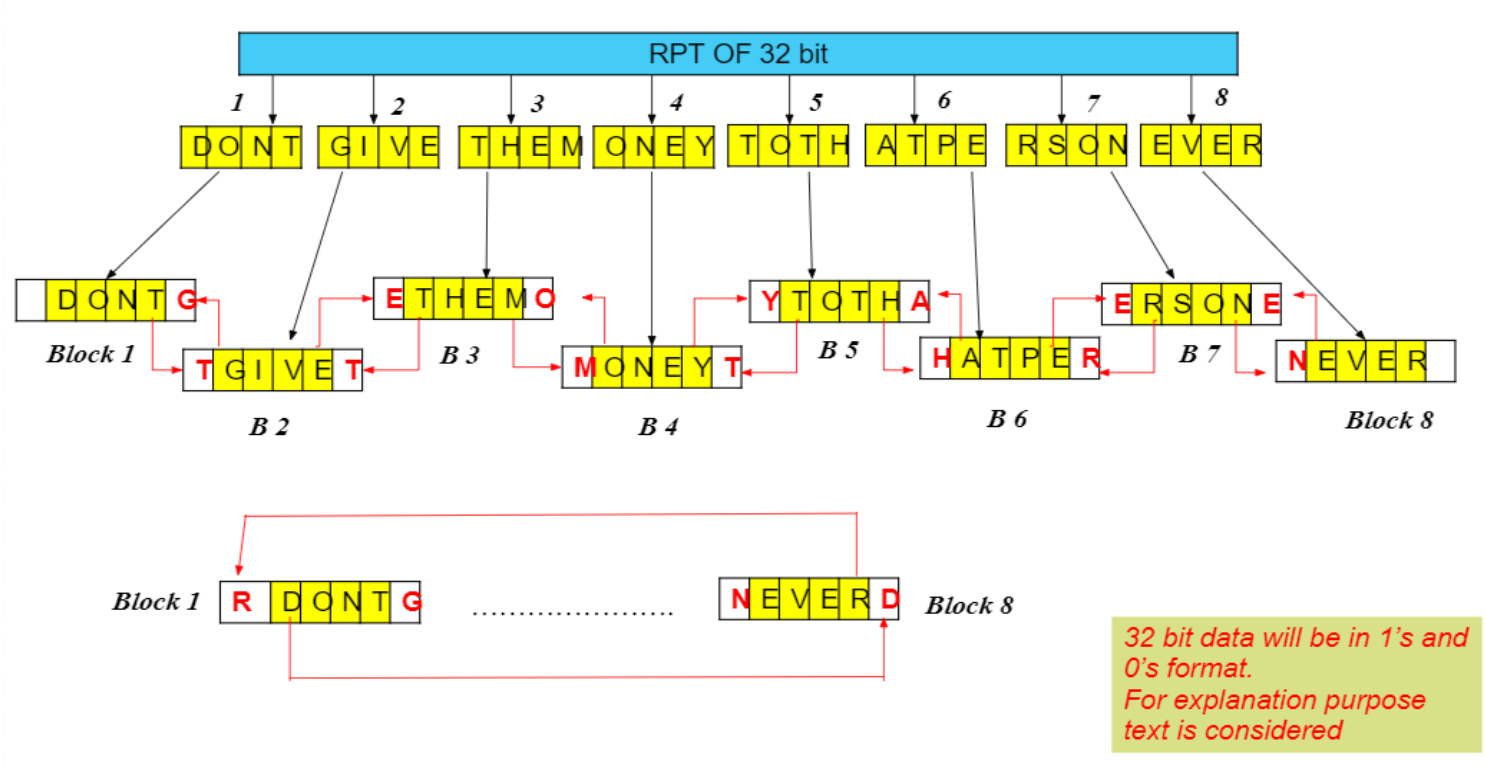
Figure - division of 32 bit RPT into 8 bit blocks



We had two 32-bit plain text areas called Left Plain Text(LPT) and Right Plain Text(RPT). During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. Bits are permuted as well hence called expansion permutation. This happens as the 32-bit RPT is divided into 8 blocks, with each block consisting of 4 bits. Then, each 4-bit block of the previous step is then expanded to a corresponding 6-bit block, i.e., per 4-bit block, 2 more bits are added.



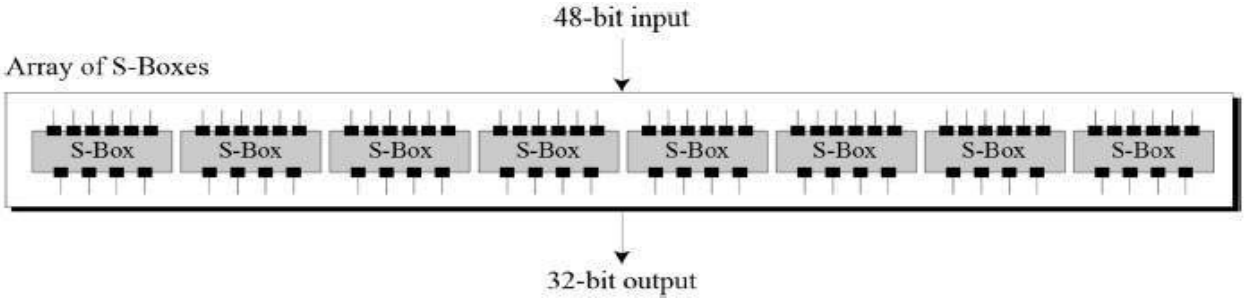
Just for understanding the working of conversion of 4 bit to 6 bit:



The expansion permutation process expands the 32-bit RPT to 48-bits. Now the 48-bit key is XOR with 48-bit RPT and the resulting output is given to the next step, which is the S-Box substitution.

- **S- Box Substitution:**

The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration −



For the conversion, S-box tables are used. There are 8 S-box tables for 8 blocks. Each table has (0-3) rows and (0-15) columns. Each cell of the table has a 4-bit number. *(You can explain, the following in short in your own words)*

Conversion of 6 bit into 4 bit:

Example:

001011

Column

01 – 1

0101- 5

Row

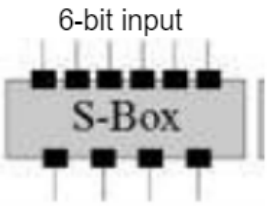
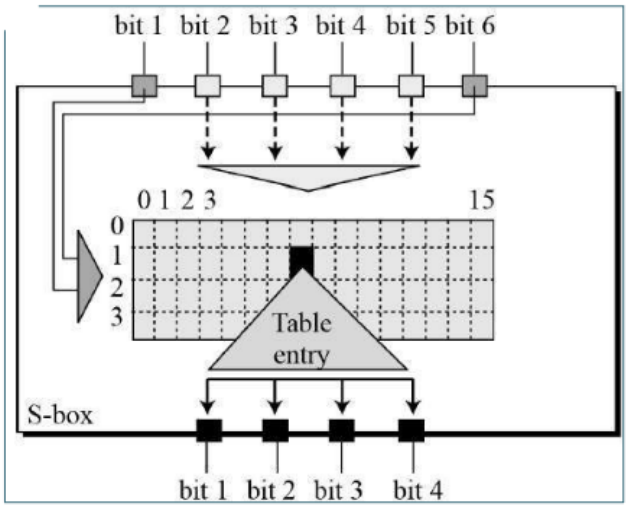
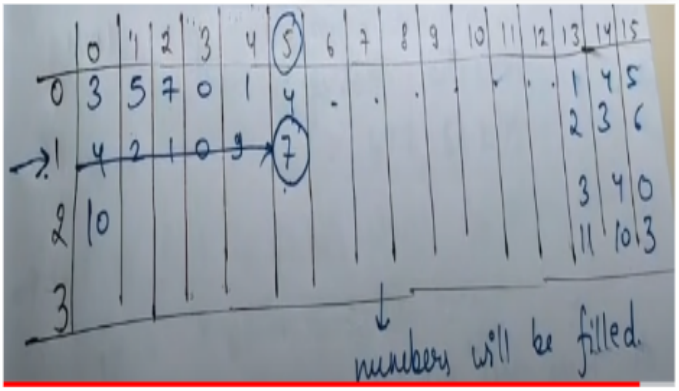


TABLE Binary-Coded Decimal (BCD) Numbers

Decimal number	Binary-coded decimal (BCD) number	
0	0000	↑ Code for one decimal digit
1	0001	
2	0010	
3	0011	
4	0100	
5	0101	
6	0110	
7	0111	
8	1000	
9	1001	↓
10	0001 0000	
20	0010 0000	
50	0101 0000	
99	1001 1001	
248	0010 0100 1000	





This way 6 bit is converted back to 4 bit. The output of all eight s-boxes is then combined into a 32 bit section.

- **P- Box Permutation:**

This mechanism involves simple permutation that is replacement of each bit with another bit, without any expansion or compression.

➔ **XOR and Swap:**

The untouched LPT, which is of 32 bits is XORed with the resultant RPT i.e with the output produced by P-Box Permutation. The result of this XOR operation becomes the new right half. The old right half becomes the new left half in the process of swapping.

➔ **Final Permutation:**

At the end of 16 rounds, the Final Permutation is performed only once. The output of the final permutation is a 64-bit encrypted block.

****

Double DES (2 DES)

Since, DES attack was vulnerable to brute force attack, variation of DES is called Multiple DES were introduced.

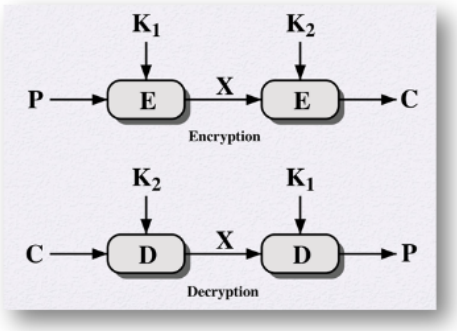
In Double DES:

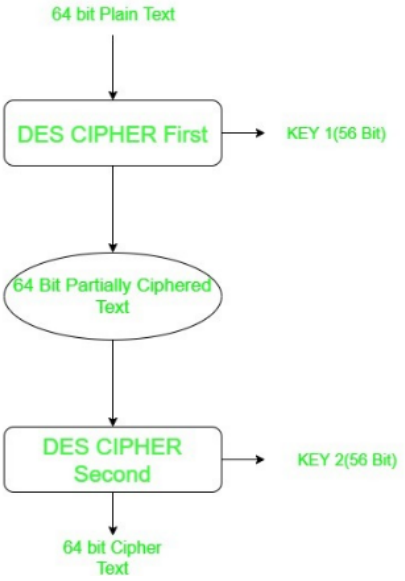
For Encryption,

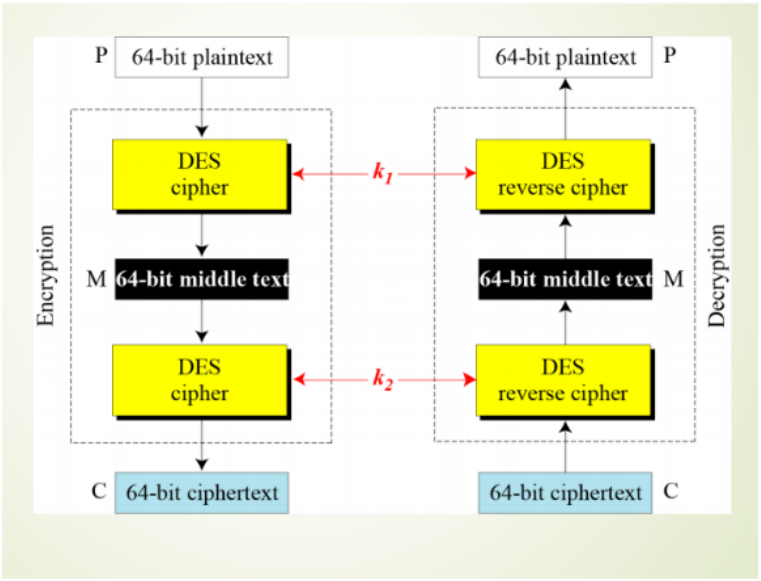
- 2 different keys are used. (56 +56) = 112 bit key.
- Double Encryption occurs as follows:

P → E(k1,p)

E(k2,E(k1,p)) = Cipher







❖ **For decryption:**

1st decryption process will be starting by using k2 which will produce single encrypted cipher text.

Next, temporary cipher text or partially ciphered text will use k1 and give us the plaintext.

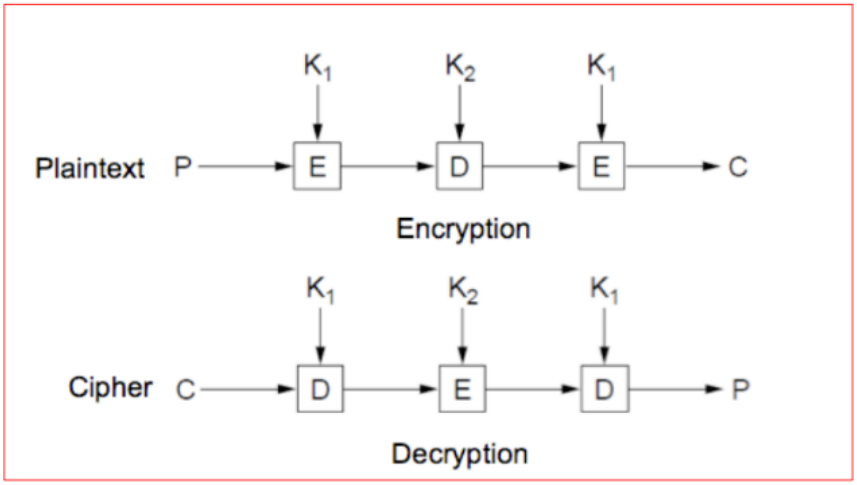
Plaintext = D(k1, D(k2,C))

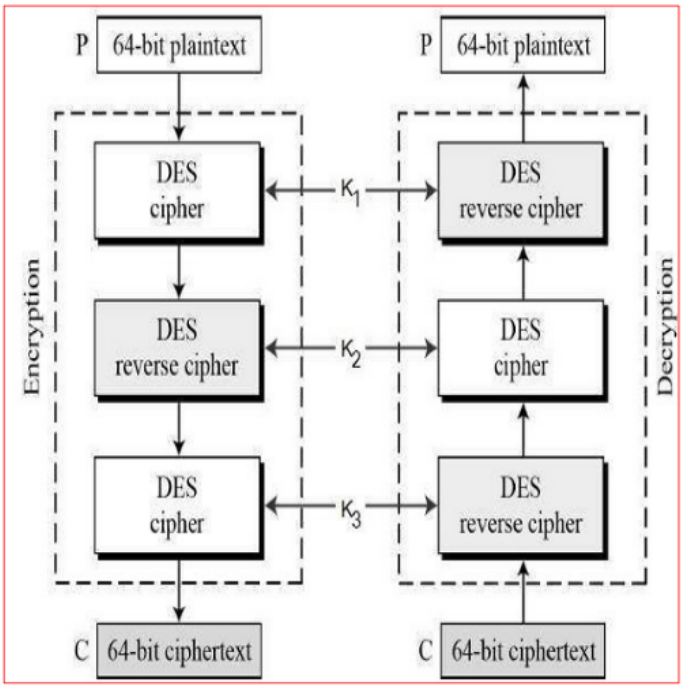
This happens first.

Triple DES (3 DES)

- Two or Three keys are used.
- Much stronger than 2 DES.

Encryption and Decryption using two keys:





Encryption and Decryption using three keys