IS Experiment No. 03

Aim:

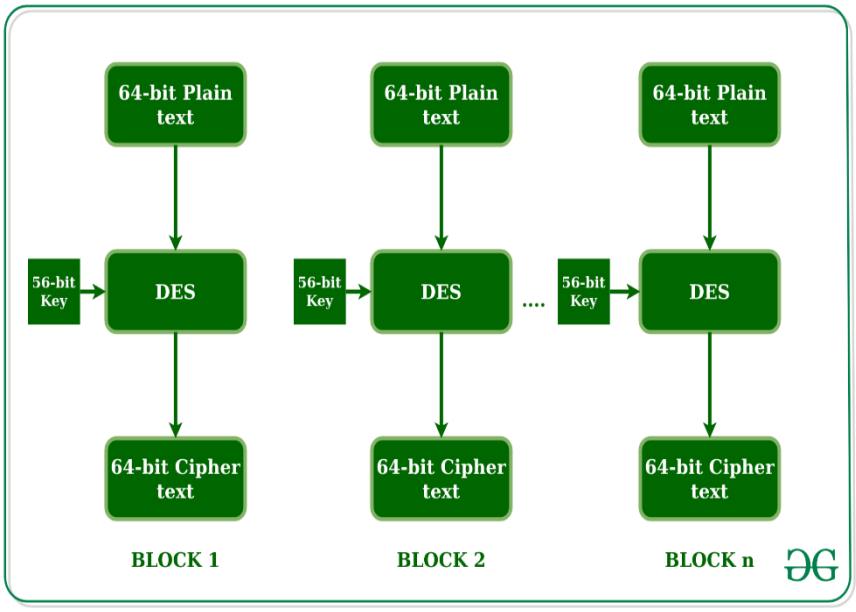
Write a Java/C/C++/Python program to implement DES algorithm.

Theory:

The Data Encryption Standard (DES) is the classic among the symmetric block cipher algorithm. DES was developed in the 1970's as a US-government standard for protecting non-classified information and was published as Federal Information Processing Standard.

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on the decline.

DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text goes as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The basic idea is shown in the figure.



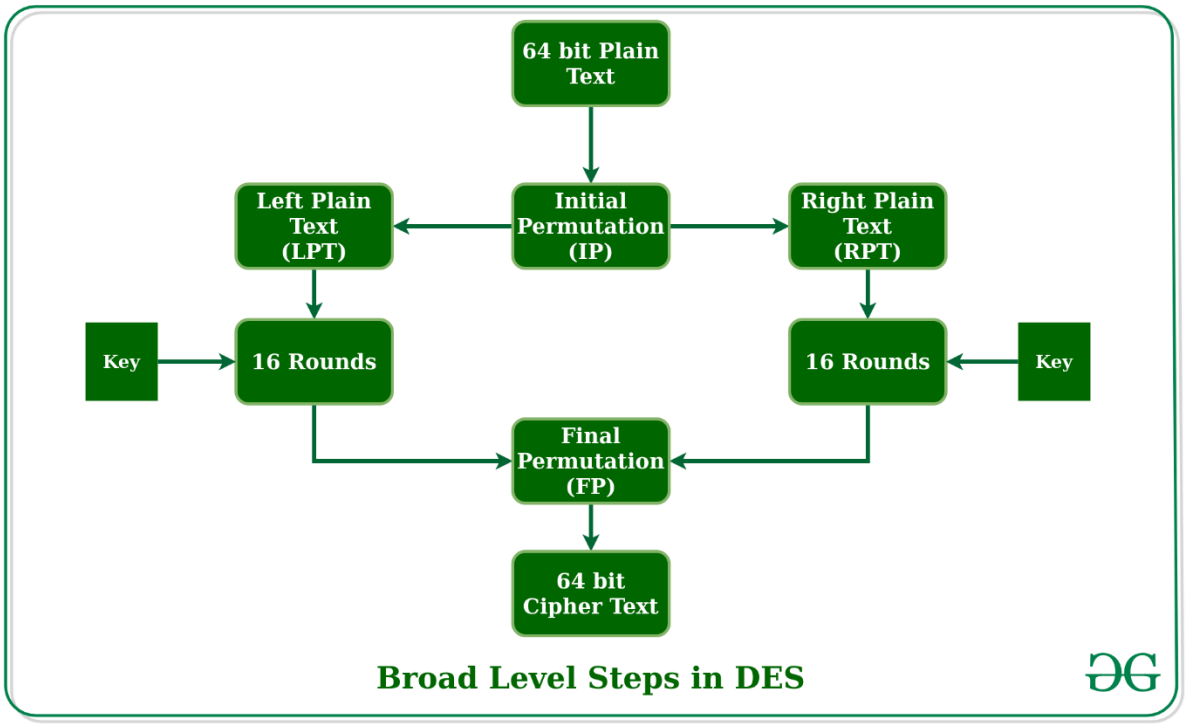
We have mentioned that DES uses a 56-bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

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

Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key.

DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition.



Steps:-

1.64-Bit plain text block is handed over to an Initial Permutation (IP) function

2. Initial Permutation (IP) is performed on plain text

3. IP produces two halves of permuted block

Left plain text (LPT) and Right plain text (RPT)

4. Each LPT and RPT goes through 16 rounds of encryption process, each with its own key.

5. In the end LPT and RPT are rejoined and final Permutation (FP) is performed on combined block

6. The result is 64 bit cipher text.

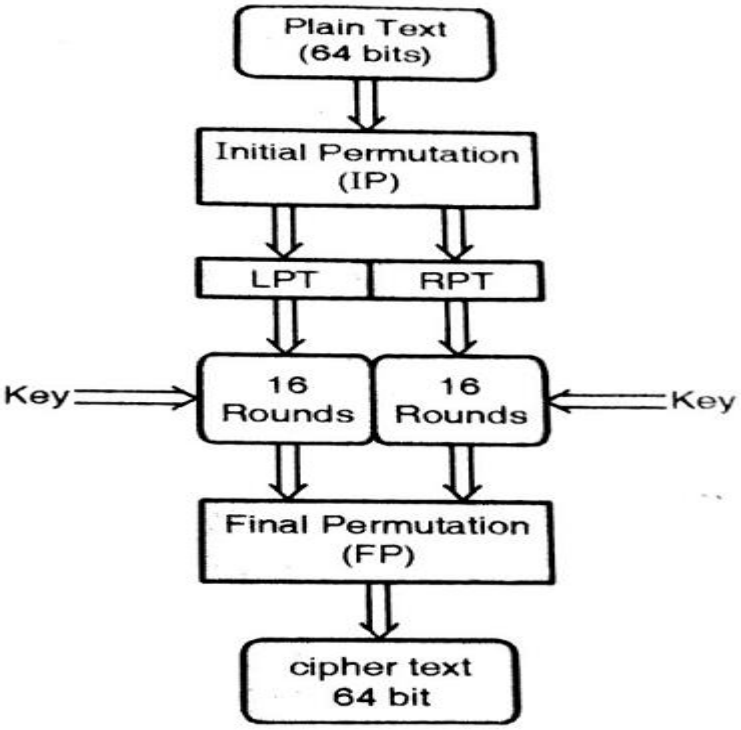


Fig: - Steps in DES

Initial Permutation (IP)

As we have noted, the initial permutation (IP) happens only once and it appens before the first round. It suggests how the transposition in IP should proceed, as shown in figure.

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.

This is nothing but jugglery of bit positions of the original plain text block. the same rule applies to all the other bit positions shown in the figure.

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

Figure - Initial permutation table

As we have noted 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 outlined in the figure.

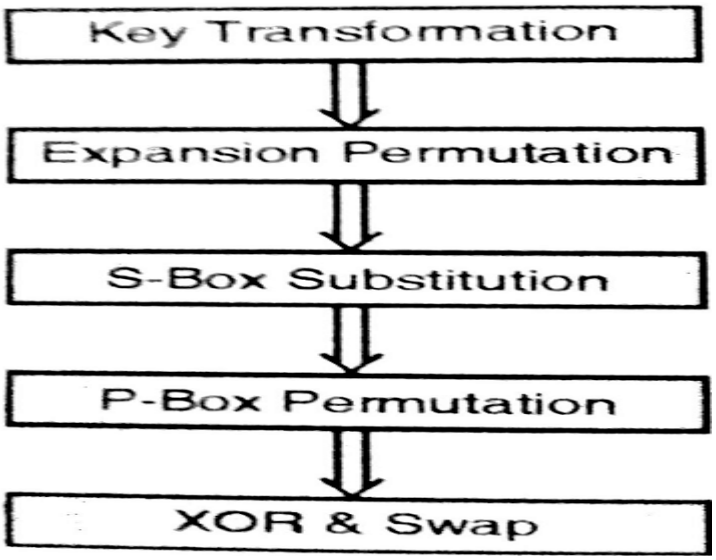


Fig: -Rounds in DES

Step-1: Key transformation –

We have noted initial 64-bit key is transformed into a 56-bit key by discarding every 8th bit of the initial key. Thus, for each a 56-bit key is available. From this 56-bit key, a different 48-bit Sub Key is generated during each round using a process called key transformation.

For this, the 56-bit key is divided into two halves, each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round.

For example, if the round numbers 1, 2, 9, or 16 the shift is done by only position for other rounds, the circular shift is done by two positions. The number of key bits shifted per round is shown in the figure.

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure - number of key bits shifted per round

After an appropriate shift, 48 of the 56 bits are selected. for selecting 48 of the 56 bits the table is shown in the figure given below. For instance, after the shift, bit number 14 moves on the first position, bit number 17 moves on the second position, and so on. If we observe the table carefully, we will realize that it contains only 48-bit positions. Bit number 18 is discarded (we will not find it in the table), like 7 others, to reduce a 56-bit key to a 48-bit key. Since the key transformation process involves permutation as well as a selection of a 48-bit subset of the original 56-bit key it is called Compression Permutation.

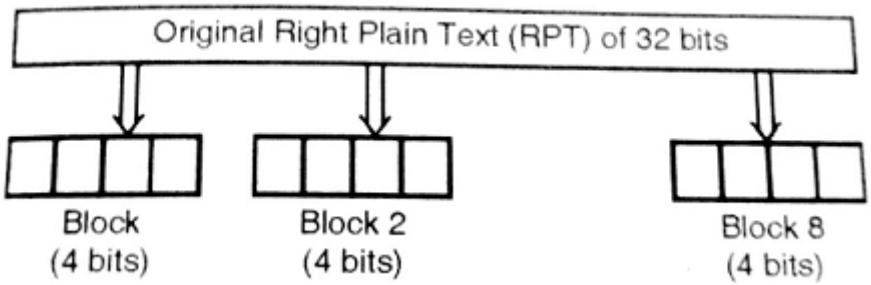
14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Figure - compression permutation

Because of this compression permutation technique, a different subset of key bits is used in each round. That makes DES not easy to crack.

Expansion Permutation

During Expansion permutation the RPT is expanded from 32 bits to 48 bits. The 32-bit RPT is divided into 8 blocks, with each block consisting of 4- bits.



Each 4-bits block of the previous step is then expanded to a corresponding 6-bit block. Per 4-bit block, 2 more bits are added. They are the repeated 1st and 4th bits of the 4-bit block.

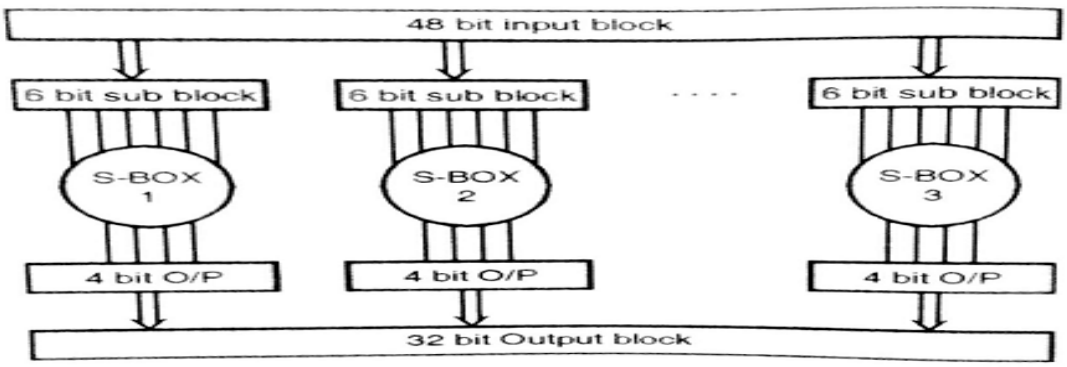
The 2nd and 3rd bits are written as they were in the input.

The 48 bit key is XORed with the 48-bit RPT and the resulting output is given to the next step.

S-box substitution

It accepts the 48-bits input from the XOR operation involving the compressed key and expanded RPT and produces 32-bit output using the substitution techniques.

Each of the 8 S-boxes has a 6-bit input and a4-bit output as shown below.



P-box permutation

The output of S-box consists of 32 bits. These 32 bits are permuted using a P-box. It involves simple permutation.

For eg., a 16 in the first block indicates that the bit at position 16 of the original input moves to bit at position 1 in the output and a 10 in the block number 16 indicates that the bit at the position 10 of the original input moves to bit at position 16 in the output.

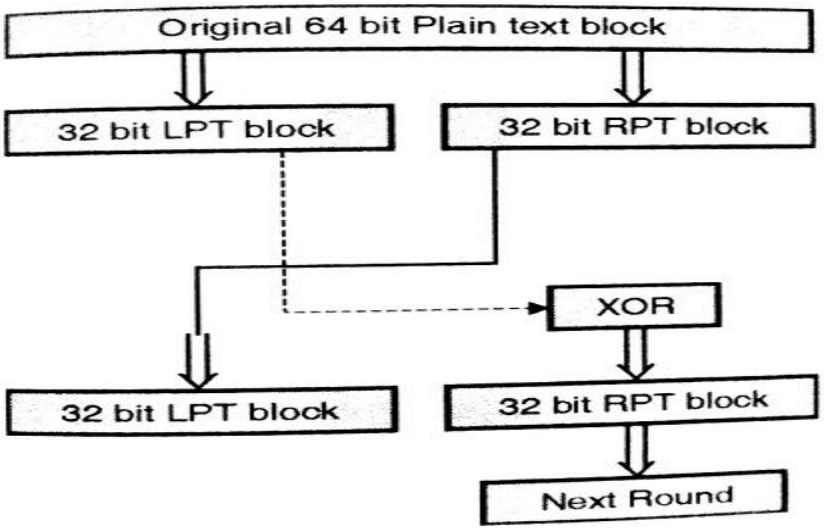
16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

XOR and swap

The LPT of the initial 64-bit plain text block is XORed with the output produced by P-box permutation.

The result of this XOR operation becomes the new RPT.

The old right half (RPT) 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 (simple transposition).

The output of Final Permutation is the 64 bit encryption block.

Conclusion:

Thus we have studied encryption and decryption using DES algorithm