DES Algorithm

(Data Encryption Standard)

- 64 bit plain text
- 56 bit key
- 64 bit cipher text

- 64 bit original key
- Key discarding process

(Every 8th bit of original key is discarded)

- 56 bit resulting key

DES (Data Encryption Standard)

❖ Steps of DES

1. 64-bit plain text block is given to Initial Permutation (IP) function.

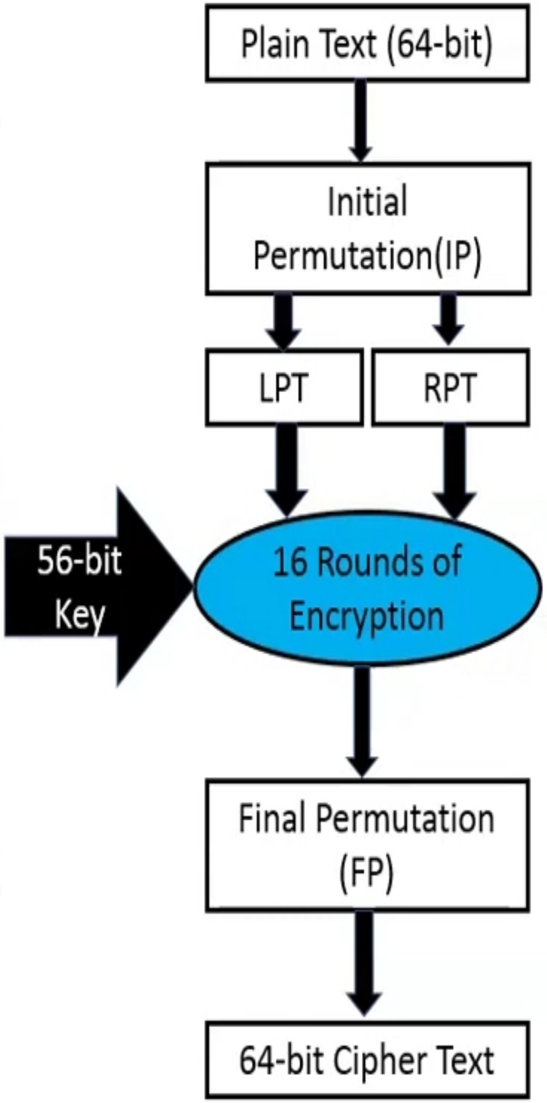
2. IP performed on 64-bit plain text block.

3. IP produced two halves of the permuted block known as Left Plain Text (LPT) and Right Plain Text (RPT).

4. Each LPT and RPT performed 16-rounds of encryption process.

5. LPT and RPT rejoined and Final Permutation (FP) is performed on combined block.

6. 64-bit Cipher text block is generated.



Plain Text (64-bit)

Initial Permutation(IP)

LPT

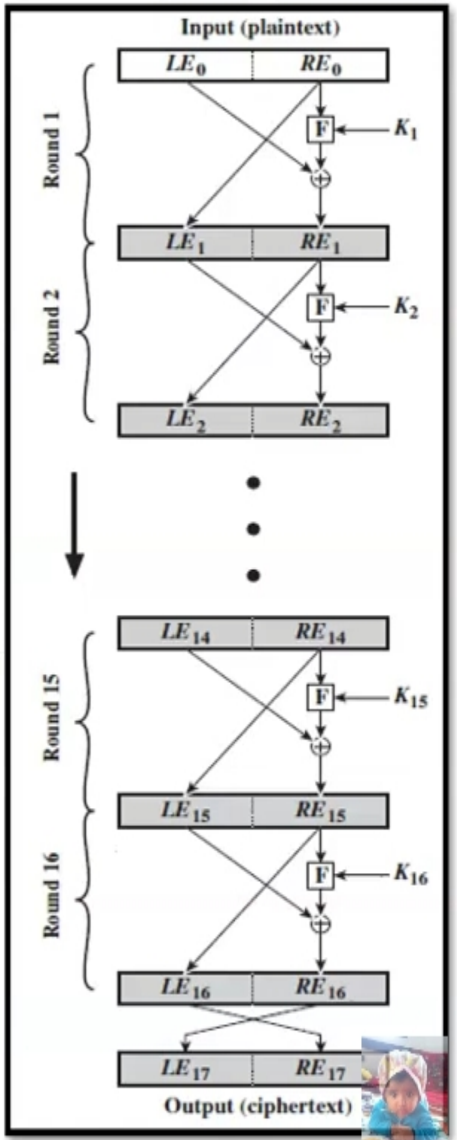
RPT

56-bit Key

16 Rounds of Encryption

Final Permutation (FP)

64-bit Cipher Text



Feistel Cipher Structure

DES (Data Encryption Standard)

al Permutation (IP) & Generate LPT -RPT

al Permutation performed only once.

equence have changed as per IP table.

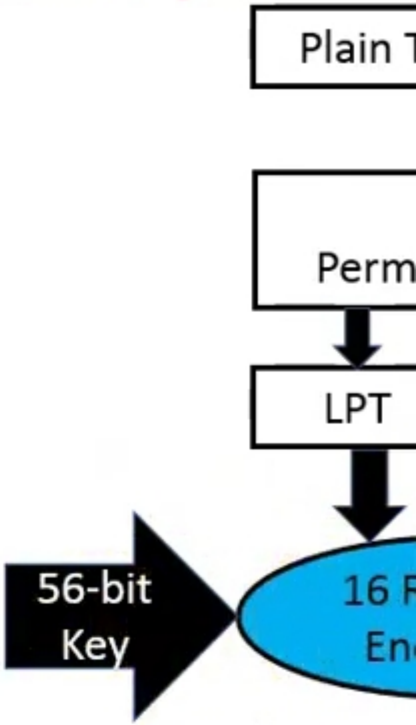
Example:

t bit take 40th Position

3th bit take 1st position

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

out of IP is divided into two equal halves known as LPT, (LPT – 32 bit, RPT – 32 bit)



DES (Data Encryption Standard)

unds of Encryption

Transformation (56-bit key)

Bit Shifted per round

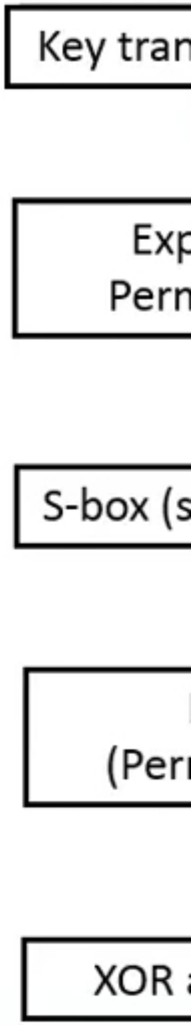
pression Permutation

nsion permutation of Plain Text and X-OR (P.T. size: , C.T. size: 48 bit)

Substitution

(Permutation)

and Swap.



DES (Data Encryption Standard)

it Shifted per Round

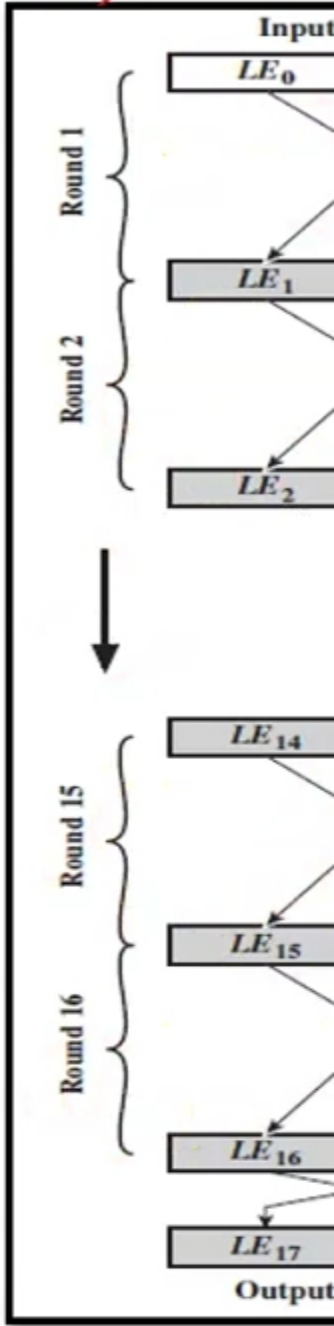
-bit key is divided into two halves each of 28-bits

rcular left shift is performed on each halves

ifting of Bit position is depending on round

- For *round number* 1,2,9 and 16 shift is done by one position
- For remaining rounds shift is done by 2 position

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



DES (Data Encryption Standard)

pression Permutation

-bit input with bit shifting position

nerates 48-bit key (Compression of Key bit)

op 9, 18, 22, 25, 35, 38, 43 and 54 bits.

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

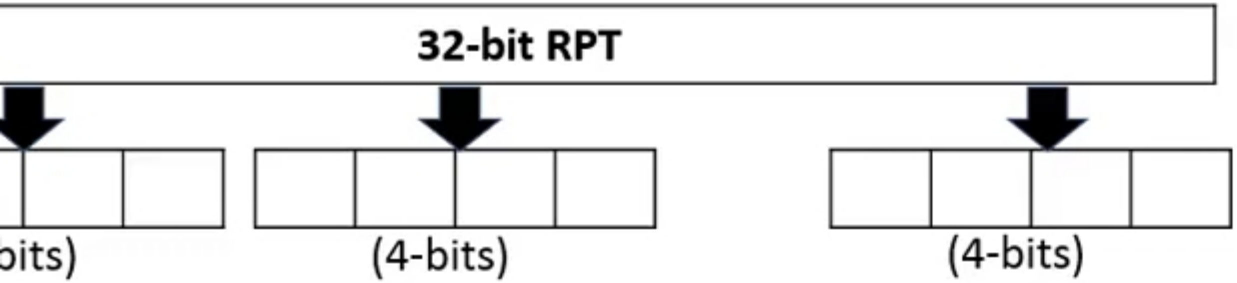
DES (Data Encryption Standard)

sion Permutation

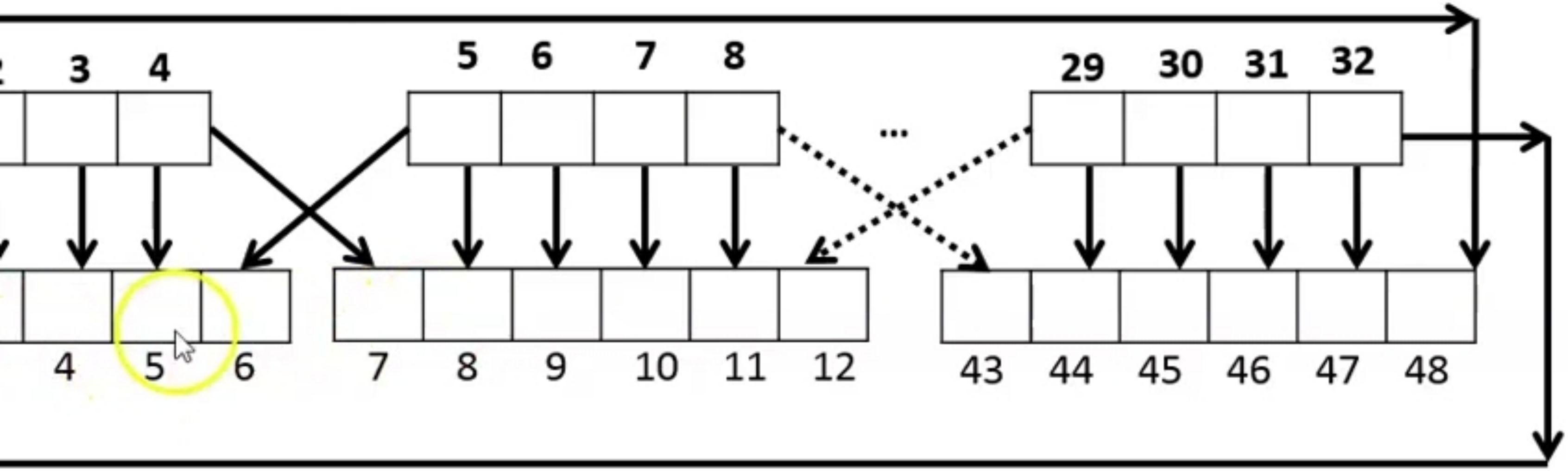
RPT of IP is expanded to 48-bits

sion permutation steps:

2-bit RPT is divided into 8-blocks each of 4-bits

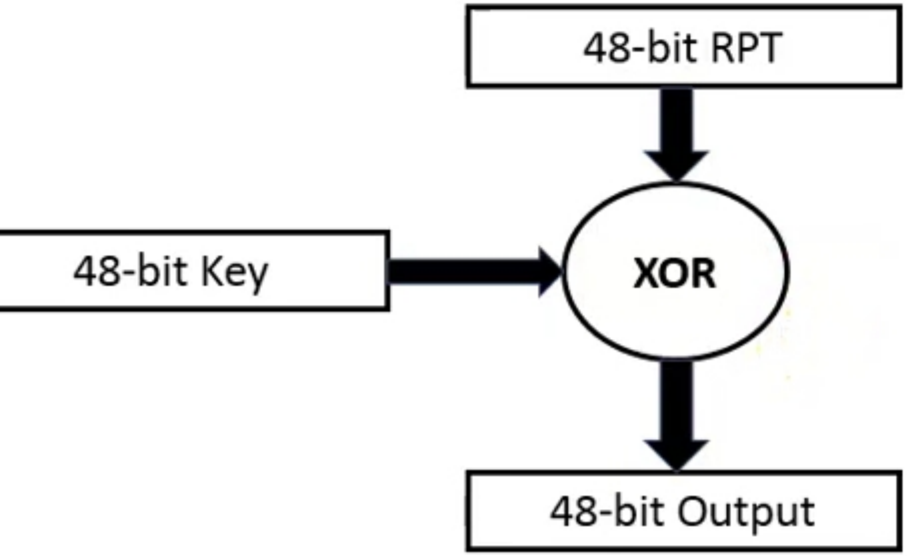


-bit block is expanded to 6-bit and produce 48-bit output



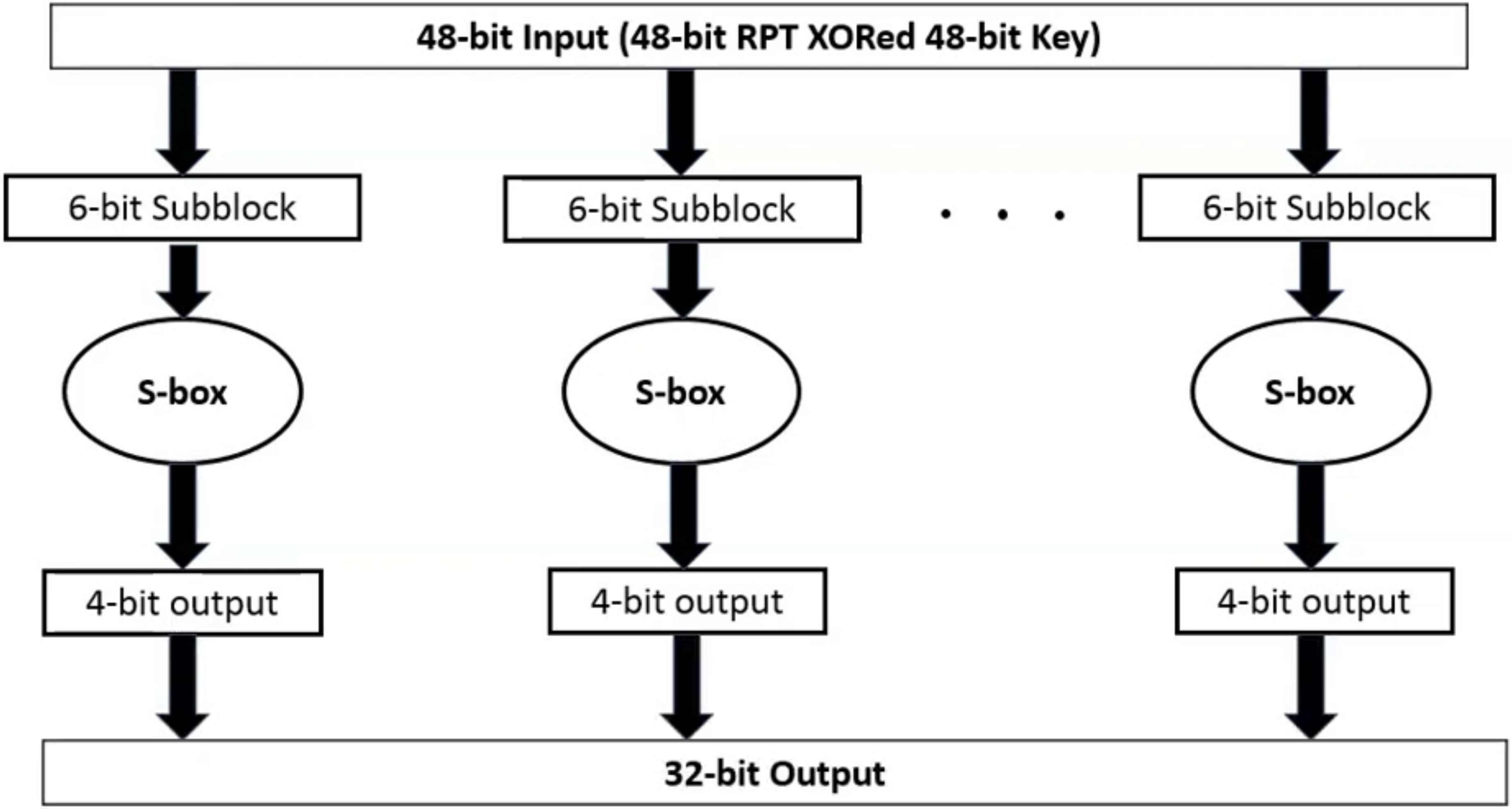
DES (Data Encryption Standard)

nsion Permutation



DES (Data Encryption Standard)

S-BOX Substitution



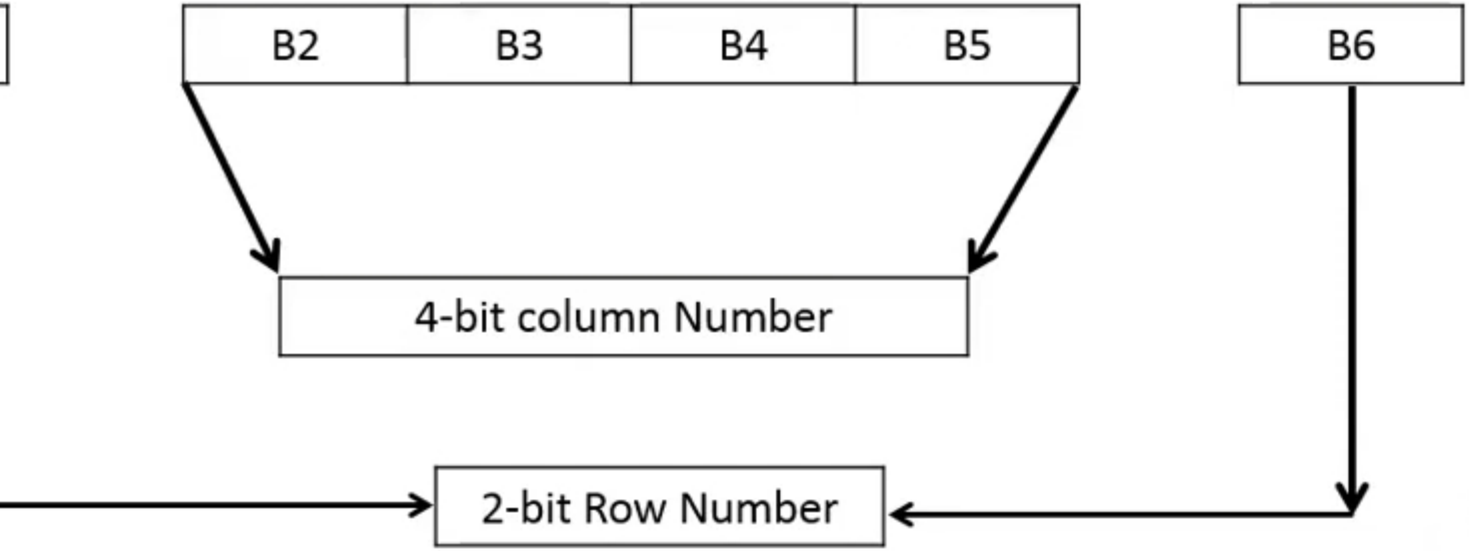
DES (Data Encryption Standard)

X Working

Key tran

Exp
Pern

S-box (s



	Middle 4 bits of input															
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Example: 011011 → 1001

DES (Data Encryption Standards)

X Permutation

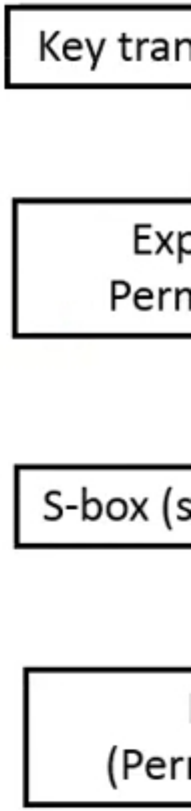
t of s-box is given to p-box

is permuted with 16 x 2 permutation table

xample:

bit of S-box take 1st Position as per below permutation le.

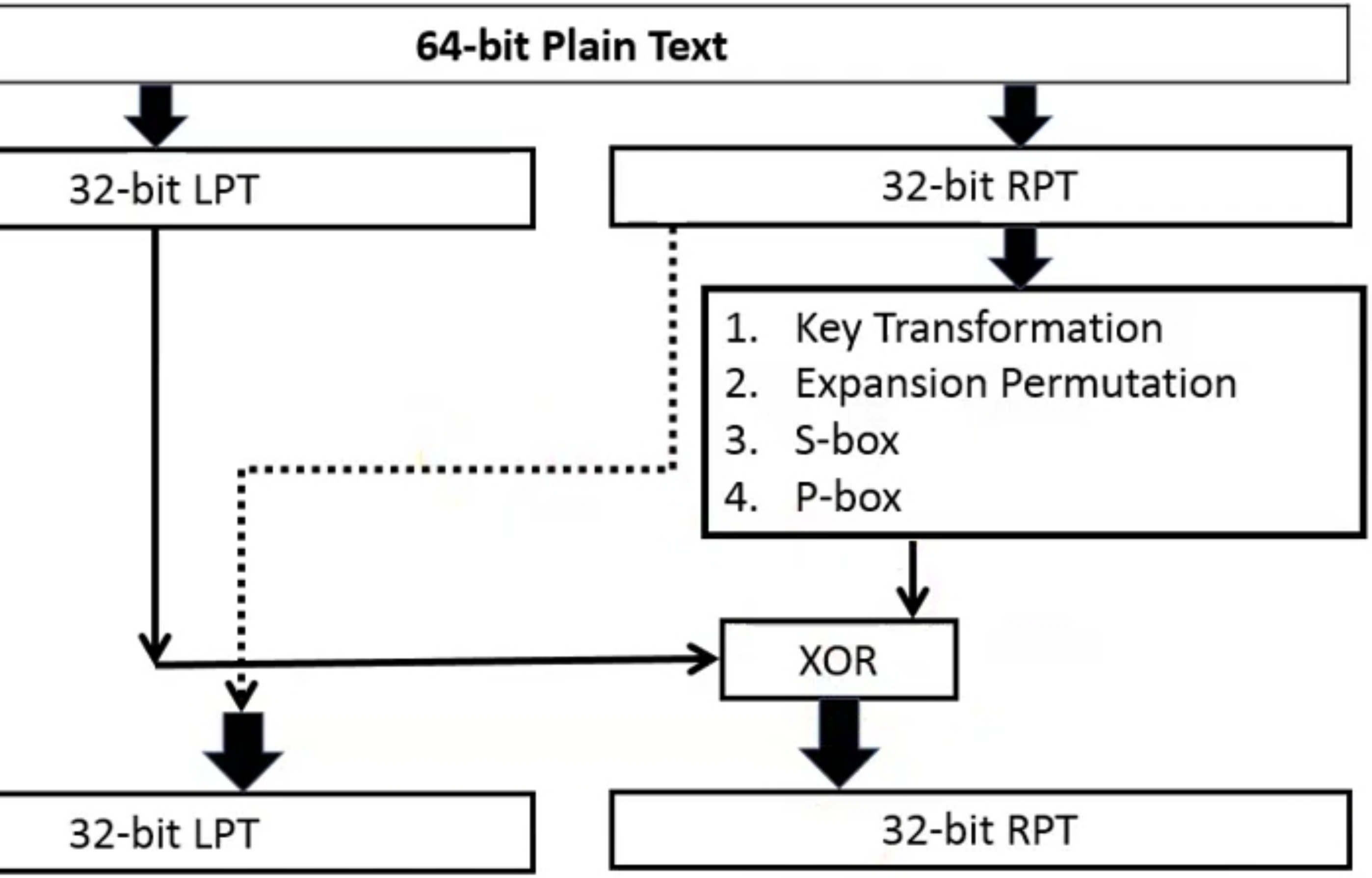
P – Box Table													
20	21	29	12	28	17	1	15	23	26	5	18	31	10
24	14	32	27	3	9	19	13	30	6	22	11	4	25



DES (Data Encryption Standard)

and SWAP

bit LPT is XORed with 32-bit p-box.



64-bit Plain Text

32-bit LPT

32-bit RPT

1. Key Transformation
2. Expansion Permutation
3. S-box
4. P-box

XOR

32-bit LPT

32-bit RPT

round of encryption is completed. Now remaining 15 rounds will be formed same as 1st round.

DES (Data Encryption Standard)

Permutation

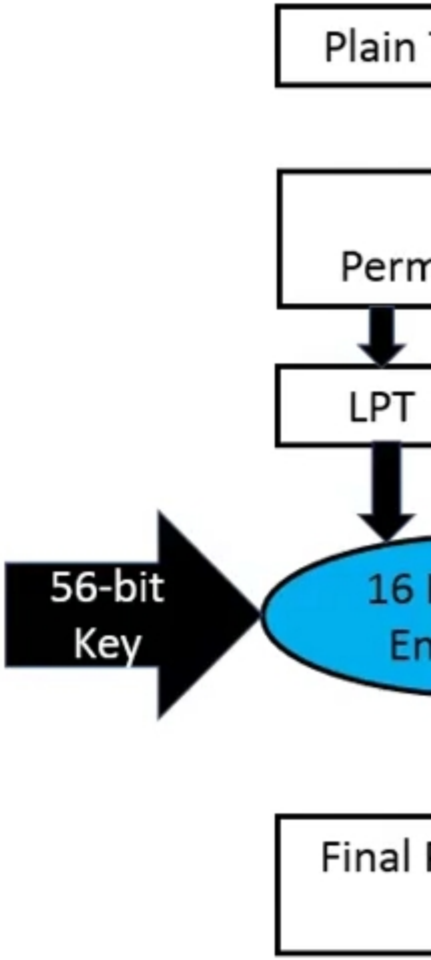
he end of the 16 rounds, the final permutation is rmed (only once).

xample:

bit of input take 1st Position as per below permutation table.

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

utput of the final permutation is ***the 64-bit encrypted (64-bit cipher text block).***


Plain T
Perm
LPT
56-bit Key
16 I
En
Final I