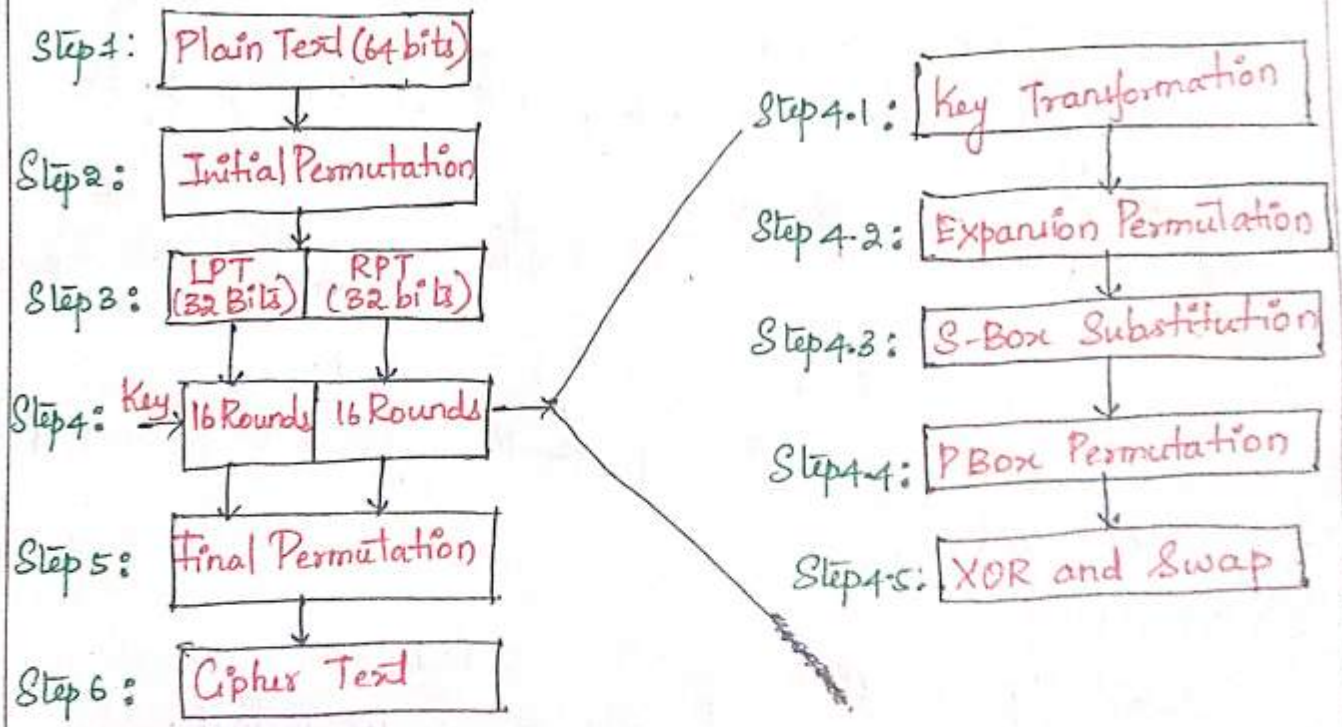
Semester: VI Subject: CSS Academic Year: 2023-2024

DES (Data Encryption Standard):

* DES is a block cipher.
* It encrypts data in blocks of size of 64bits
* 64 bits of plain text goes as an input to DES, which produces 64bits of cipher text.
* The same algorithm and key are used for encryption and decryption, with minor difference.
* The key length is 56 bits.

Broad level steps in DES (or) Block diagram of DES.



Step 2: Initial Permutation

* There are pre-defined permutation rules for initial permutation. (Initial Permutation Table) Refer PPT.
* for example, the 58th bit position in the plain text takes 1st position in new plain text, the 50th bit position in

the plain-text ~~becomes~~ takes 2nd bit position in the new generated plain text.

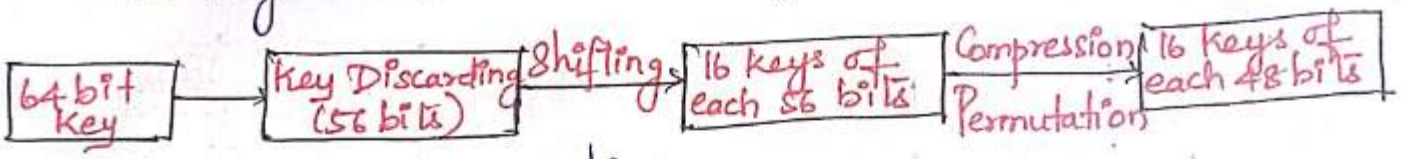
* After initial permutation, a new 64 bit plain text is derived.

Step 3 : LPT and RPT

* The resulting 64-bit permuted text block is divided into two half blocks.
* Each half block consists of 32 bits.
* LPT (Left Plain Text → 32 bits) and RPT (Right Plain Text → 32 bits).

Step 4.1 : Key Transformation

The key transformation undergoes the following steps:



* DES uses 16 rounds.
* For each round a unique key is used.
* Using 1 key a total of 16 keys are generated for each round.

Key Discarding :

* Initially a 64bits key is selected.
* Every 8th bit of original key is discarded.
* ~~From~~ After discarding one key of 56 bits are generated.

Semester: VI Subject: CSS Academic Year: 2023-2024

Generate 16 keys of 56 bits:

To generate 16 keys, it will follow the below rule. It will perform left circular shift according to this table.

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

Example:

1111000^{7} 1010101^{14} 0011010^{21} 0000101^{28}

0101010^{35} 1100110^{42} 0011110^{49} 1100101^{54}.

According to the table, for the 1st key it will do 1 bit left circular shift.

L_1: 1110001 0101010 0110100 0001011

R_1: 1010101 1001100 0111101 1001010

⋮

L_{16}

R_{16}.

L_2R_2 is derived from L_1R_1 by performing 1 bit left circular shift.

L_3R_3 is derived from L_2R_2 by performing 2 bit left circular shift.

The same procedure is repeated for 16 times and 16 different keys of each 56 bits are generated.

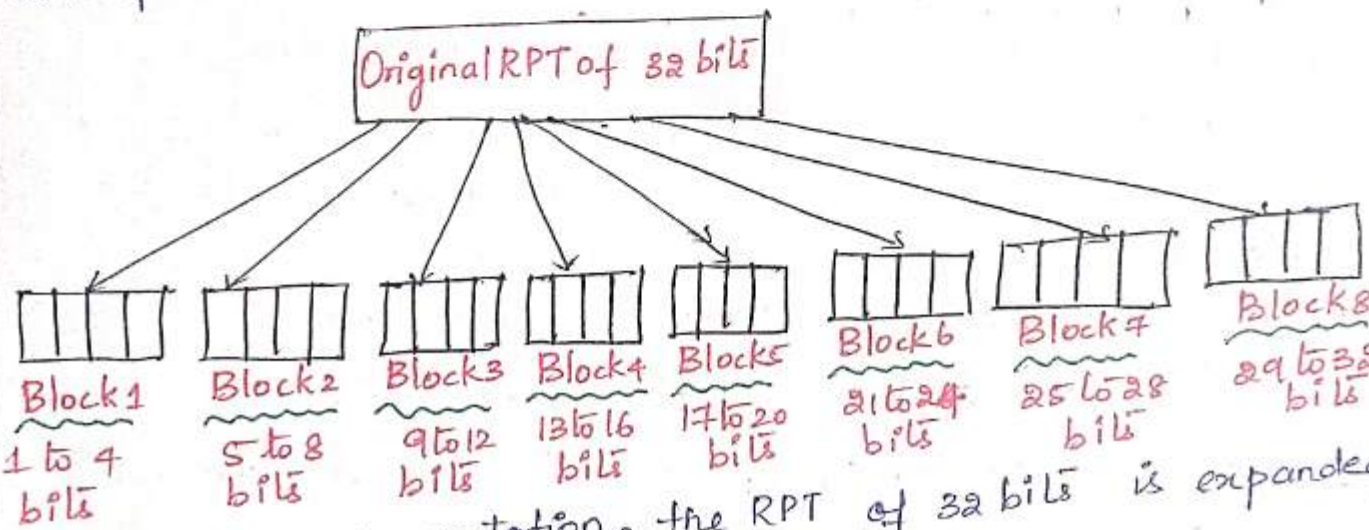
Compression Permutation:

* Apply compression permutation using compression permutation table on $L_1R_1, L_2R_2 \ldots L_{16}R_{16}$ (Refer PPT)
* The process is continued and 16 keys of 48 bits ($K_1, K_2, K_3, K_4 \ldots K_{16}$) are generated.

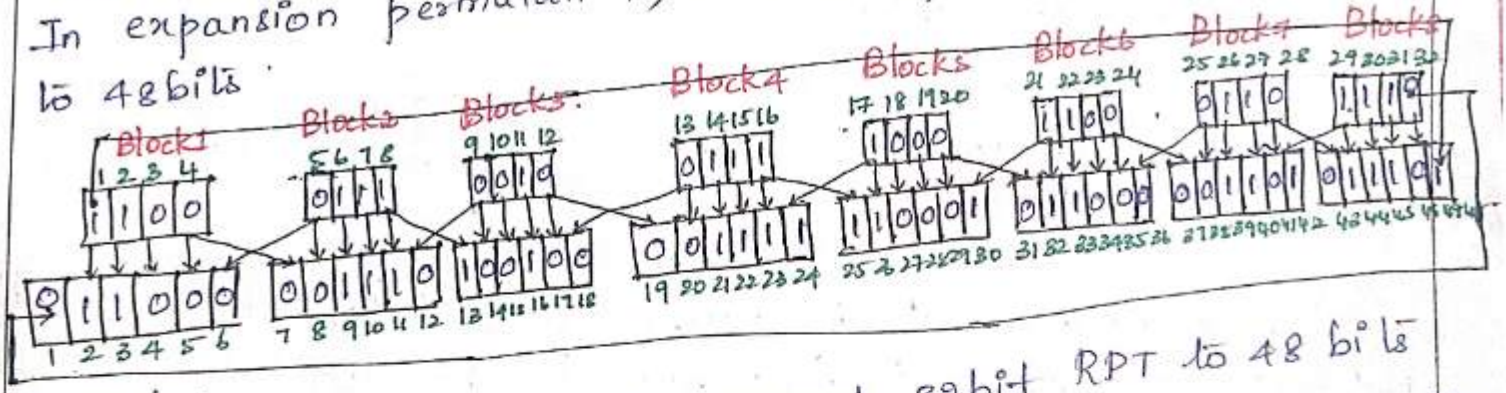
Semester : VI Subject : CSS Academic Year: 2023-2024

Step 4.2 :- Expansion Permutation:

The expansion permutation is applied on the original RPT of 32 bits.



In expansion permutation, the RPT of 32 bits is expanded to 48 bits.



Example:
Using Expansion permutation expand 32bit RPT to 48 bits

1100 0111 0010 0111 1000 1100 0110 1110 → 32bits
011000 001110 100100 001111 110001 011000 001101 011101

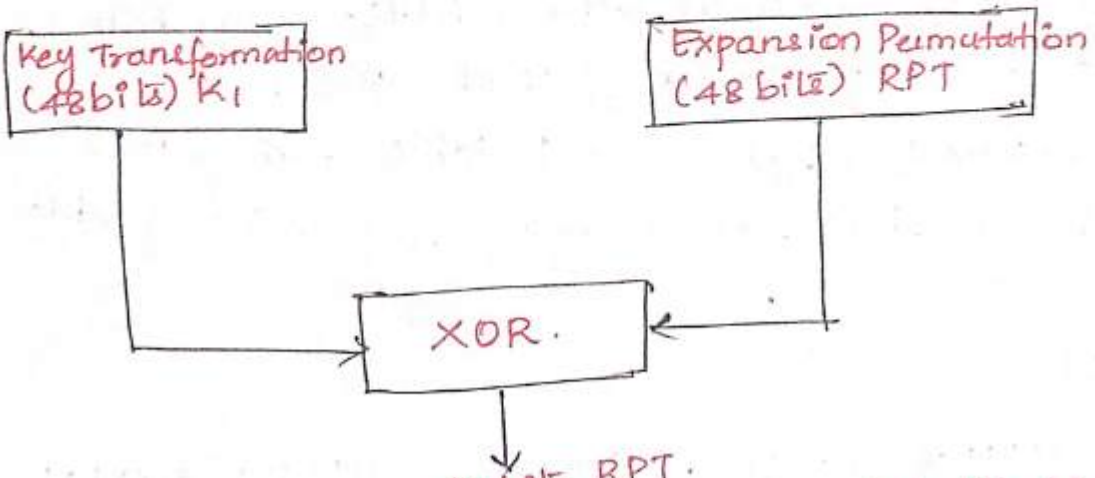
48 bits RPT

Way to S-Box Substitution:

* The first key (K1) of 48bits is XORed with the 48bit RPT generated in Expansion permutation
* A new 48bits RPT is generated which will undergo

Semester : VI Subject : CSS Academic Year: 2023-2024

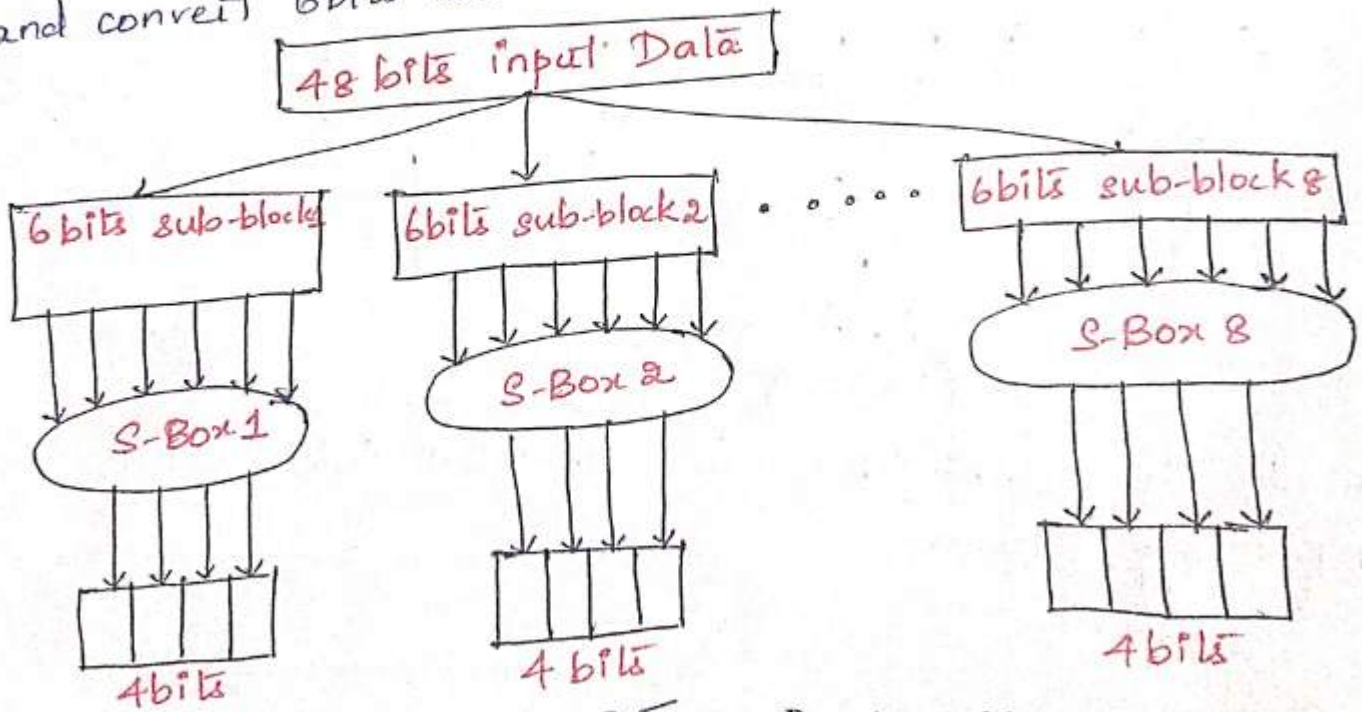
S-Box substitution.



S-Box Substitution:

* The 48bits RPT is divided into 8 sub-blocks with 6bits in each block.
* Each sub-block will refer to S-Box 1 to S-Box 8.

and convert 6bits block to 4bits block.



Semester : VI Subject : CSS Academic Year: 2023-2024

* The 1st and the last bit will refer the row value of respective SBox, whereas the middle four bits will refer the coloumn value of that S-Box.

* For S-Box 1 refer S-Box 1 table, for S-Box-2 refer S-Box 2 table, for S-Box 3 refer S-Box 3 table and so on.

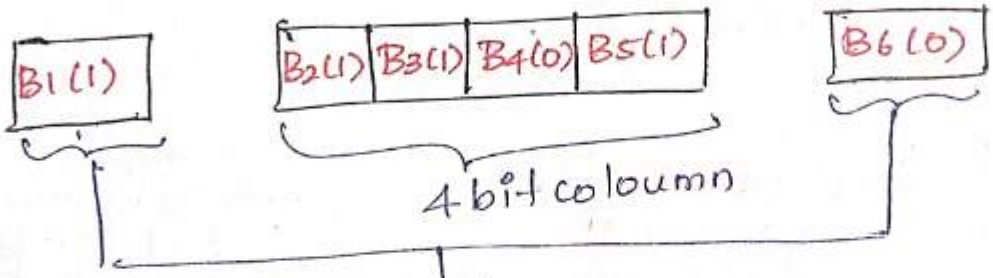
Example:

111010	111110	100101	110000	011101	011111	011100
SBox 1	SBox 2	SBox 3	S-Box 4	S-Box 5	S-Box 6	S-Box 7
1010	1111	1101	1111	1000	1000	0110

100111 .
S-Box 8
0111

S-Box 1: 111010 .

B1 (1)	B2 (1)	B3 (1)	B4 (0)	B5 (1)	B6 (0)



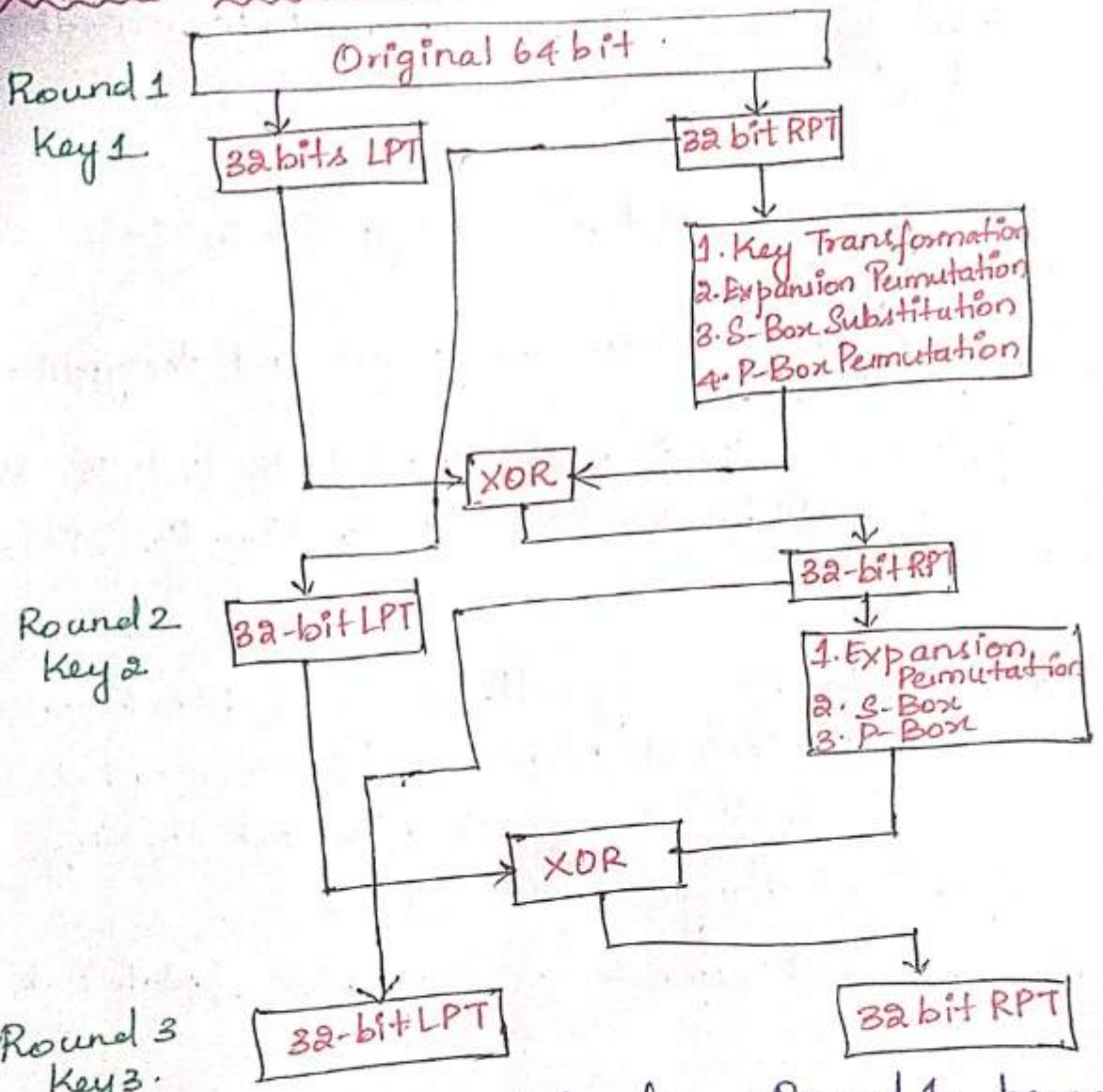
Finally the 48 bit RPT is converted into 32 bits RPT using S-Box.

Semester : VI Subject : CSS Academic Year: 2023-2024

Step 4.4 – P-Box Permutation:

The 32bits RPT generated from S-Box undergoes P-Box Permutation and new 32bits RPT is generated.

Step 4.5 : XOR and swap



* The output generated from Round 1 becomes new RPT. and the previous 32bits RPT is new 32 bits LPT.
* The process is repeated 16 times with 16 different keys and 64bit output is generated

Semester: VI Subject: CSS Academic Year: 2023-2024

Step 5: Final Permutation:

* The 64 bits output generated in the previous step undergoes final permutation and new 64 bits is generated.
* The output generated after final permutation is the 64 bit Cipher Text

DES Decryption:

* The same algorithm used for encryption in DES also works for decryption.
* The only difference between encryption and decryption is reverse of key position.
* For encryption key (K) is ~~used~~ divided into $K_1, K_2, K_3 \ldots K_{16}$ for decryption key should be used as $K_{16}, K_{15}, K_{14} \ldots K_1$ for all 16 rounds.

DES Analysis:

DES has proved to be a very well-designed block cipher. DES satisfies both the desired properties of block cipher.

Avalanche effect:- A small change in plaintext (or) key results in significant change in the ciphertext.

Completeness:- Each bit of cipher text depends on many bits of plaintext.