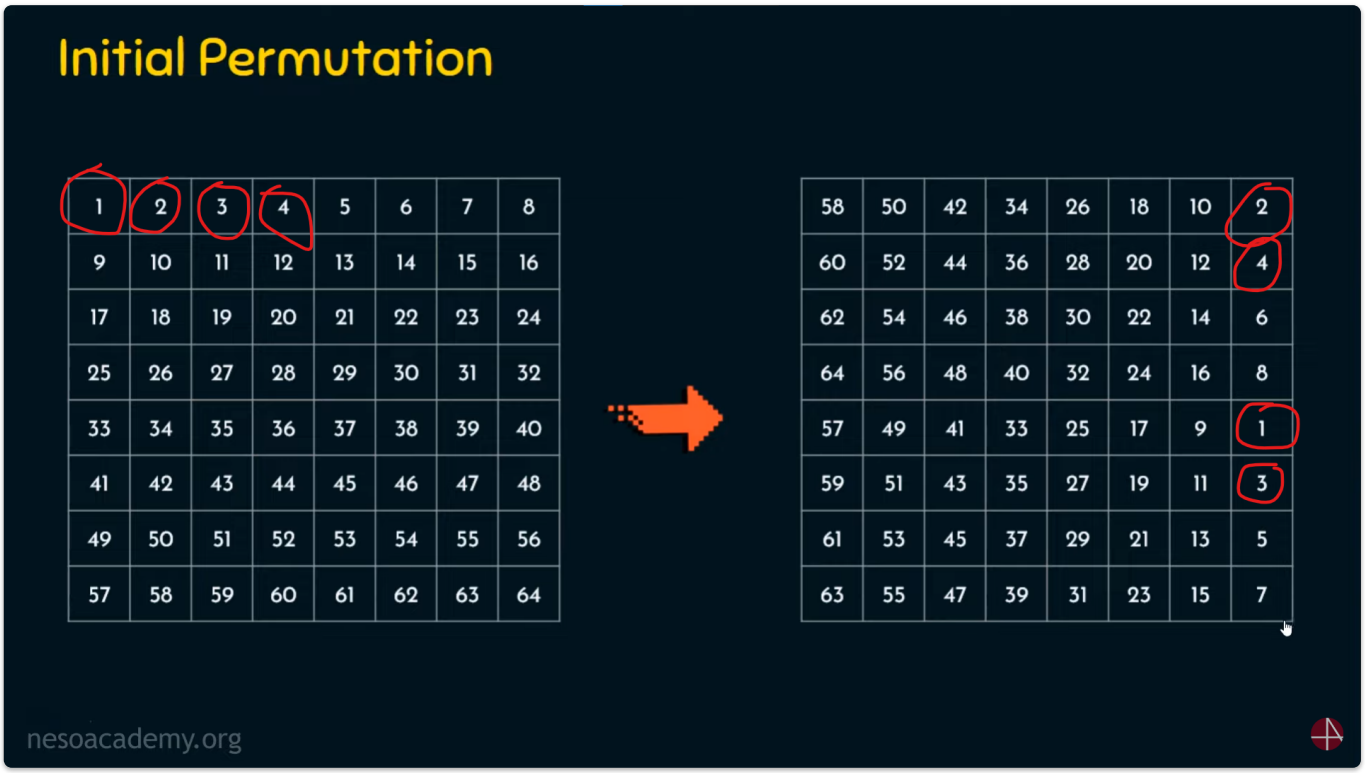
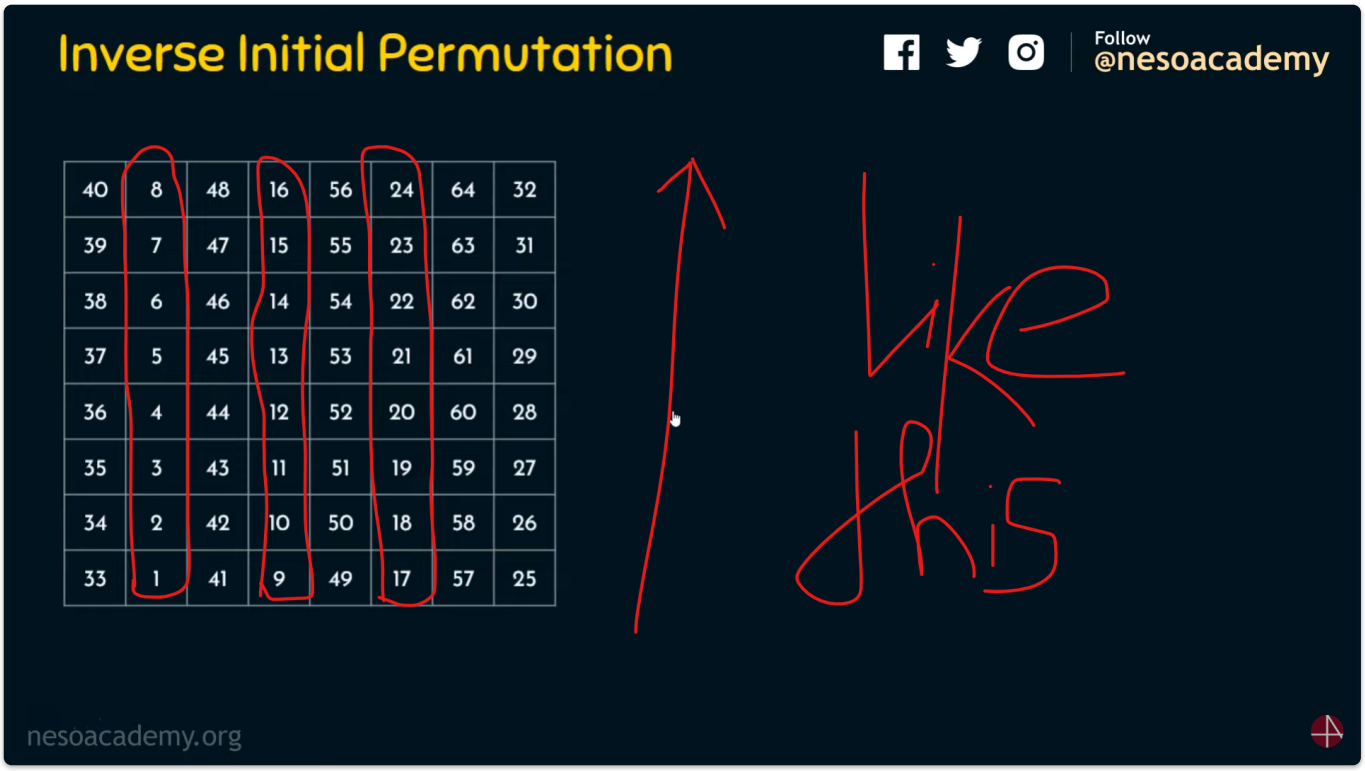
IS Notes

- DES (Data Encryption Standard) => Block Cypher => Fiestal Design
- It takes 64 Bits of Input Size while AES takes 128 bit Size.

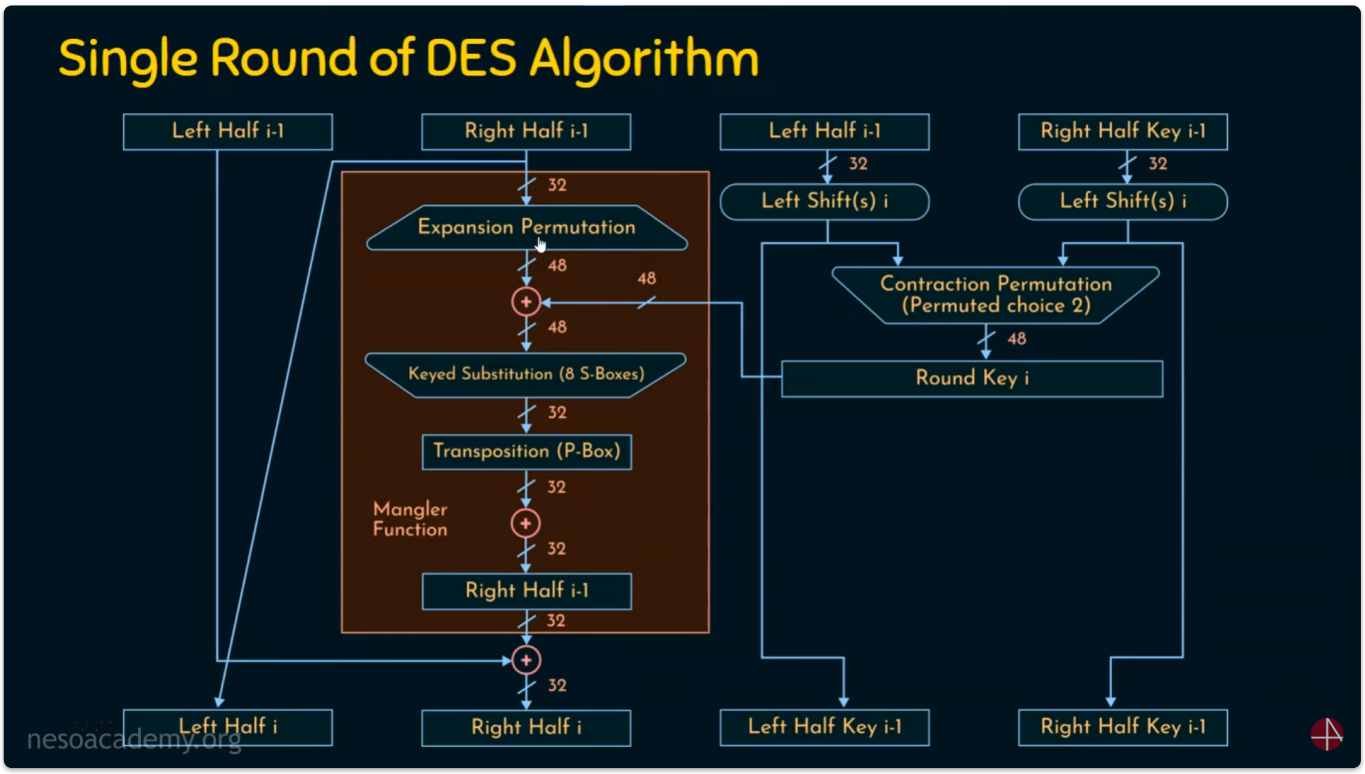
**Step By Step DES : [DES Algorithm | Working of DES Algorithm | DES Encryption Process | Data Encryption Standard - YouTube]

(He Missed the Last Swapping Step but remaining is COOL)**





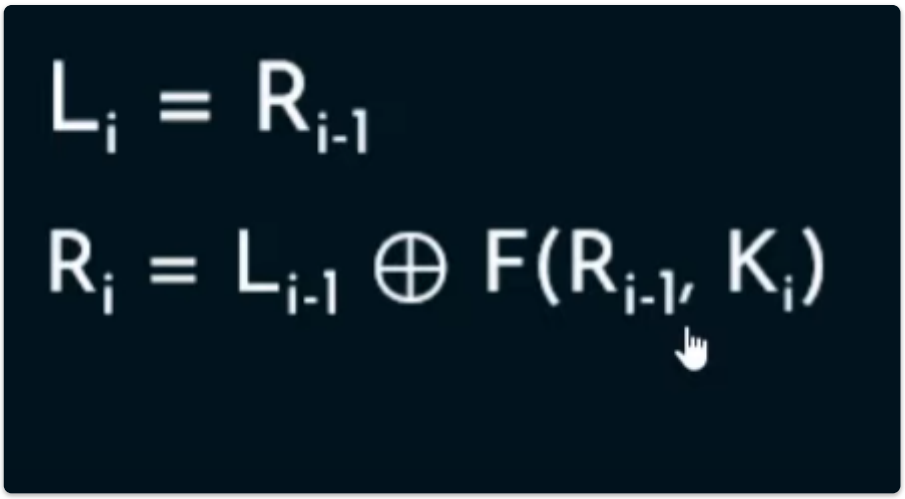
- Here these numbers are Index (Positions) and not Values (for sake of explanation)



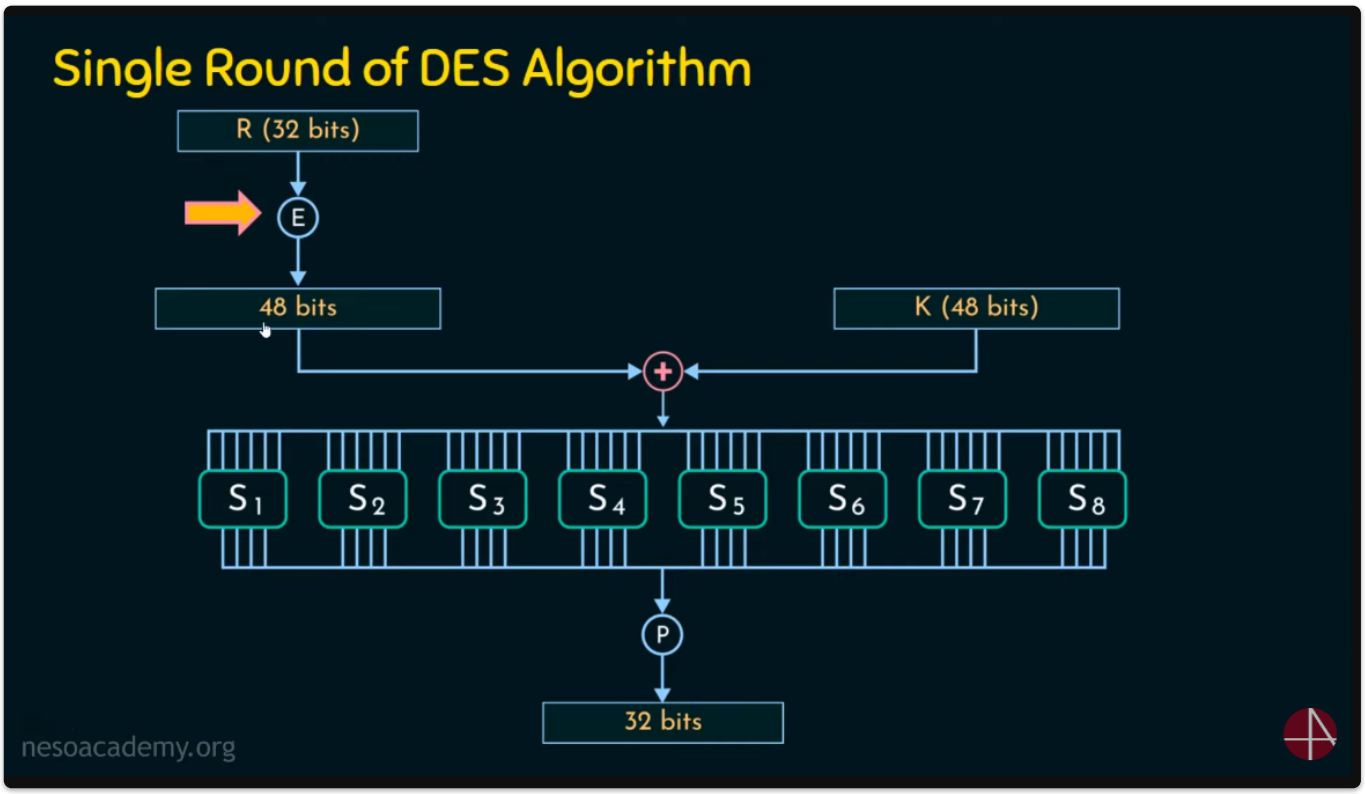
- Red Area is Function (F) called Mangler Function =>
  1. Doing Expansion (32 bits to 48 bits)
  2. XOR (Round Key and 48 bits)
  3. Apply Confusion and Diffusion by S-Box and P-Box (Generate 32 bits).
  4. Perform XOR (Output 32 bits)

5. Take XOR (Right Half with Left Half).
6. Now Output is 32 bit Right Half.
7. Initial Right Half (Before F Function) is now Left Half.

- Key is 64 bit (Broken to 32 bit Left and Right Half)
- Perform Left Shift on Both Halves.
- Pass both Halves to Permute Function to Generate 48-bit Round Key.



1. Li and Ri are Outputs (which is our Cypher Text).
2. Li-1 and Ri-1 are Initial Inputs (Acquired after Initial Permutation : IP).
3. Ki is Key for Current ith Round.



- How to Apply (E) => Expansion Function (32 bits to 48 bits) ?

This is how you displace the index positions.

- After XOR with Key we pass (48 bits) to
  8 S-Boxes, Each S-Box has 6 bits
  Each S-Box converts 6 bits to 4 bits

  Now 8 S-Boxes with 4 Bits as Output,
  Total Output is 4x8 = 32 Bits

- How S-Box converts 6-bits to 4-bits ?

Box S_1

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	6	5	3	8
10	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

For example, $S_1(101010) = 6 = 0110$.

- Now Pass 32 Bits to P-Box and it Outputs (Shuffled 32-Bits)
  Like this

The Permutation Function (P)

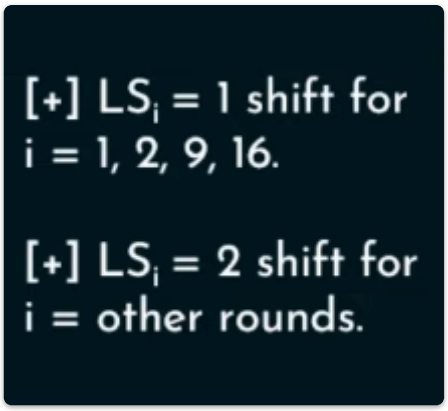
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

These are Index or Positions

So Basically inside (F) => Mangler Function,

1. Expansion
2. XOR with Key
3. S-Box
4. P-Box
5. Output of Mangler Function (F) : 32-Bits (Right Half)

- Now How does Main Key (64-Bit) convert into 56-Bit Sub-Key ??
- This Step is called (Permuted Choice 1)
  64 - 8 = 56 => Which 8 Bits are Dropped ?
  Bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.
- Left Circular Shift =>
- In Which Way Shifts Applied for
- Each Round ?



- 1 Shift for Rounds 1, 2, 9, 16
- 2 Shifts for all other rounds.

Now In (Permuted Choice 2),
We will drop 8 Bits from 56 Bits,
We will get 48-Bits Round Key

LINK FOR EXTRA STEPS NOT MENTIONED HERE
FOR EXAMPLE : Circular Left Shift and XOR:
Cryptography Basics - Bitwise XOR , Shift , Circular Shift Operations - Cyber Security - CSE4003 - YouTube

Circular Left Shift : Left se 1 ya 2 Bits uthao aur Right Side ke End pe Phenk do (SIMPLE) XDs

- An Advantage of DES but it was Broken by Some Chad Person XDD

DES has a 56-bit key which raises the possibility of 2^{56} possible keys. This statement deals with _____ attack.

a. Timing

b. Mathematical

c. Brute Force

d. DoS