

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)**

Initial Permutation

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



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	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7



Inverse Initial Permutation



Follow
@nesoacademy

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



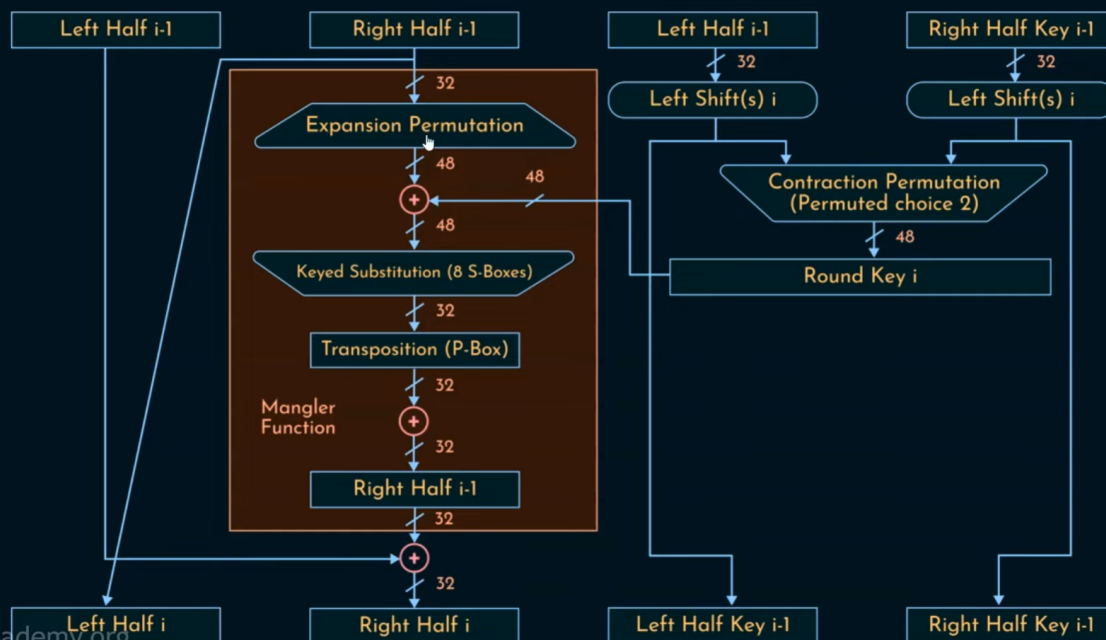
like
this

nesoacademy.org



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

Single Round of DES Algorithm



nesoacademy.org



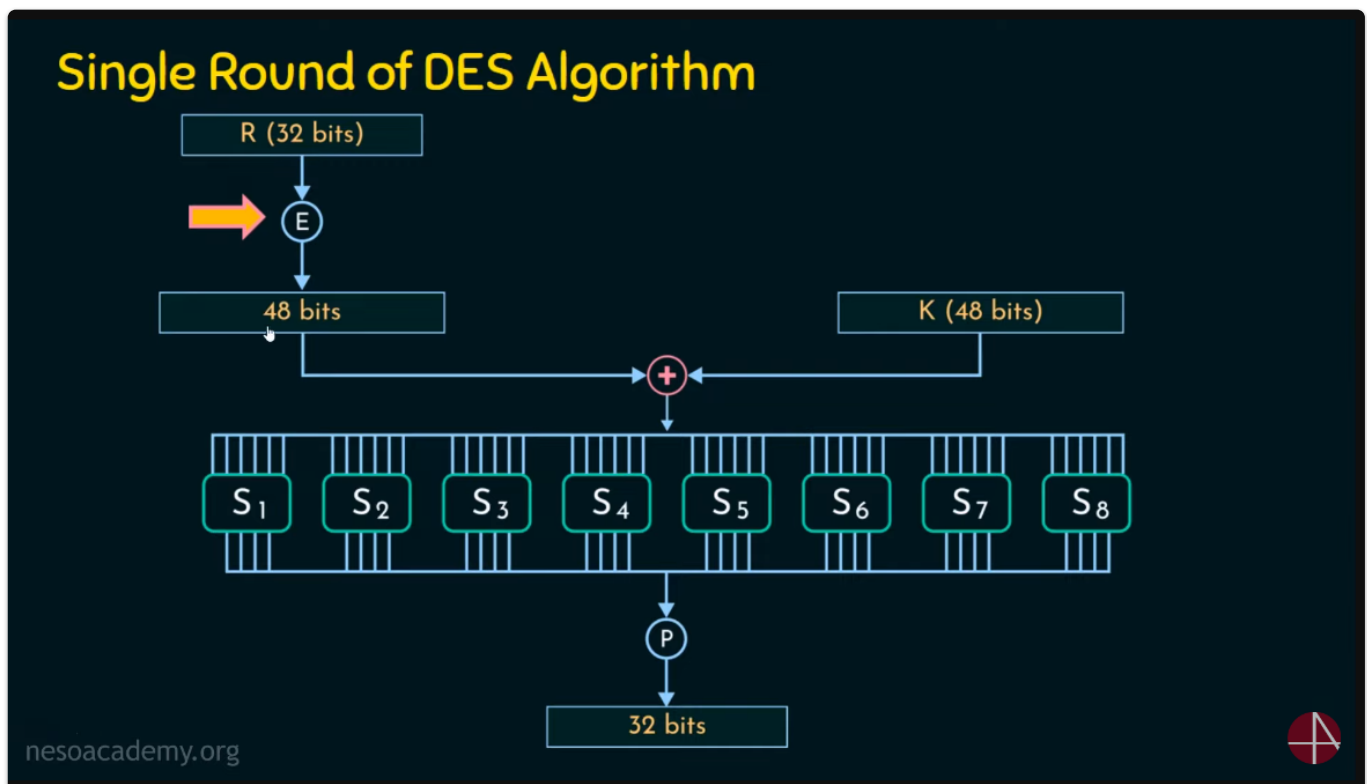
- Red Area is Function (F) called Mangler Function =>
 - Doing Expansion (32 bits to 48 bits)
 - XOR (Round Key and 48 bits)
 - Apply Confusion and Diffusion by S-Box and P-Box (Generate 32 bits).
 - Perform XOR (Output 32 bits)

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.

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

1. L_i and R_i are Outputs (which is our Cypher Text).
2. L_{i-1} and R_{i-1} are Initial Inputs (Acquired after Initial Permutation : IP).
3. K_i is Key for Current i th Round.



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

The Expansion Permutation

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

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 $4 \times 8 = 32$ 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**)
 $64 - 8 = 56 \Rightarrow$ Which 8 Bits are Dropped ?
 Bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.
- Left Circular Shift \Rightarrow
- In Which Way Shifts Applied for
- Each Round ?

[+] $LS_i = 1$ shift for
 $i = 1, 2, 9, 16.$

[+] $LS_i = 2$ shift for
 $i = \text{other rounds}.$

- 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