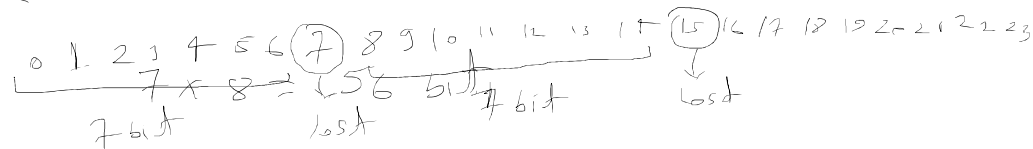


# DES (Data Encryption Algorithm):

would given in

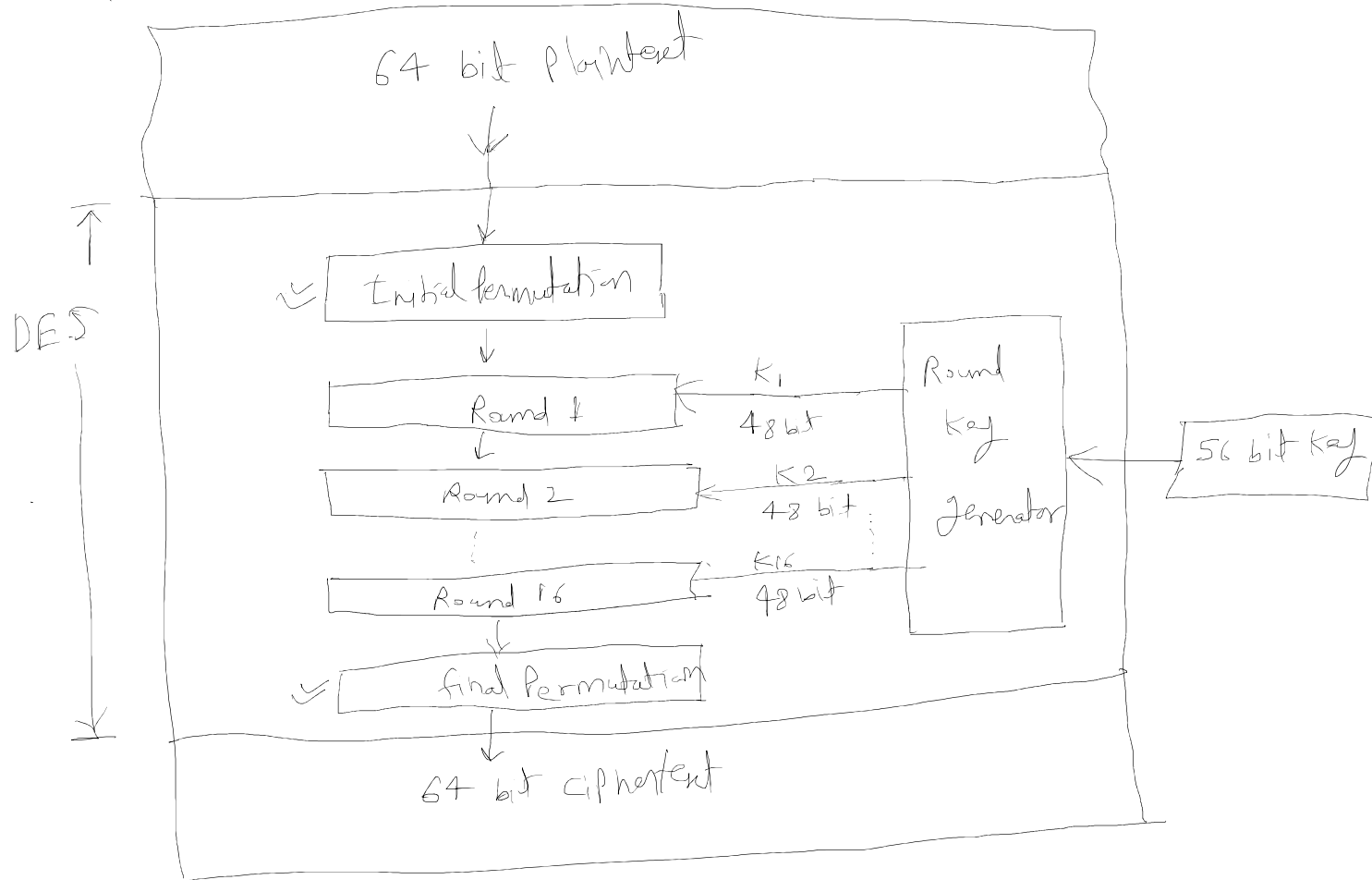
- Developed by NIST (National Institute of Standard Technology)
- Symmetric key Block cipher (64 bit)
- It is implementation of Feistel cipher Model. (16 Rounds)
- DES has 16 Rounds.
- Block size is 64 bit. (Plaintext & ciphertext)
- Key length is 56 bit. (original key is 64 bit but 8 bit are not used)



## main functionality of DES:

- ① Round function
- ② Key schedule
- ③ Additional processing (Initial & final permutation)

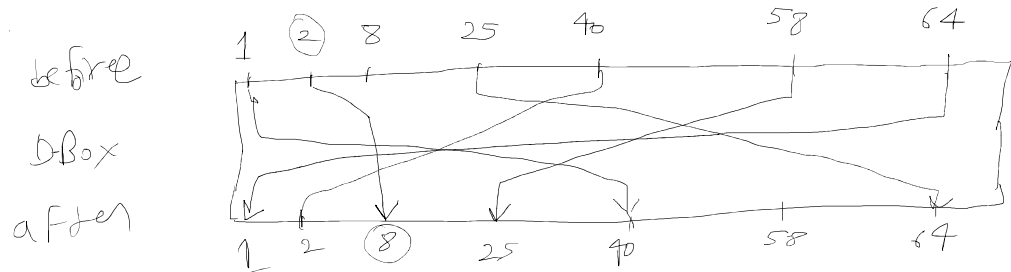
## Structure of DES:



① Initial Permutation:

+ S-Box & Final Permutation are Straight Permutation Box used do (1-1)

apply substitution operation on plaintext/intermediate text. [D-Box] (straight)



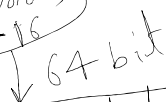
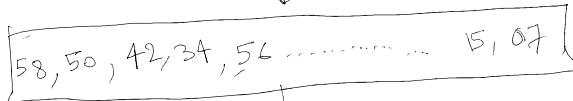
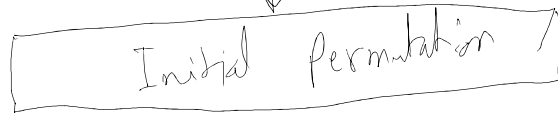
D-Box (output)

	2	3	8	...	25	...	40	...	64
	40		2		58		1		25

Example of permutation & final permutation table

Initial  
8 x 8 = 64

Initial Permutation															
58	50	42	34	26	18	10	02								
60	52	44	36	28	20	12	04								
62	54	46	38	30	22	14	06								
64	56	48	40	32	24	16	08								
57	49	41	33	25	17	09	01								
59	51	43	35	27	19	11	03								
61	53	45	37	29	21	13	05								
63	55	47	39	31	23	15	07								



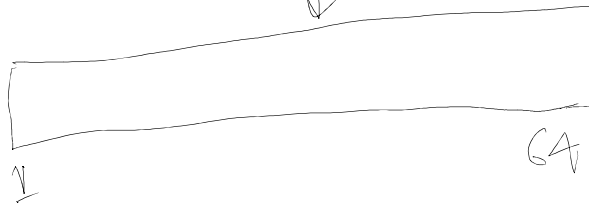
61 53 45 37 29 21 13 05  
63 55 47 39 31 23 15 07

Final permutation

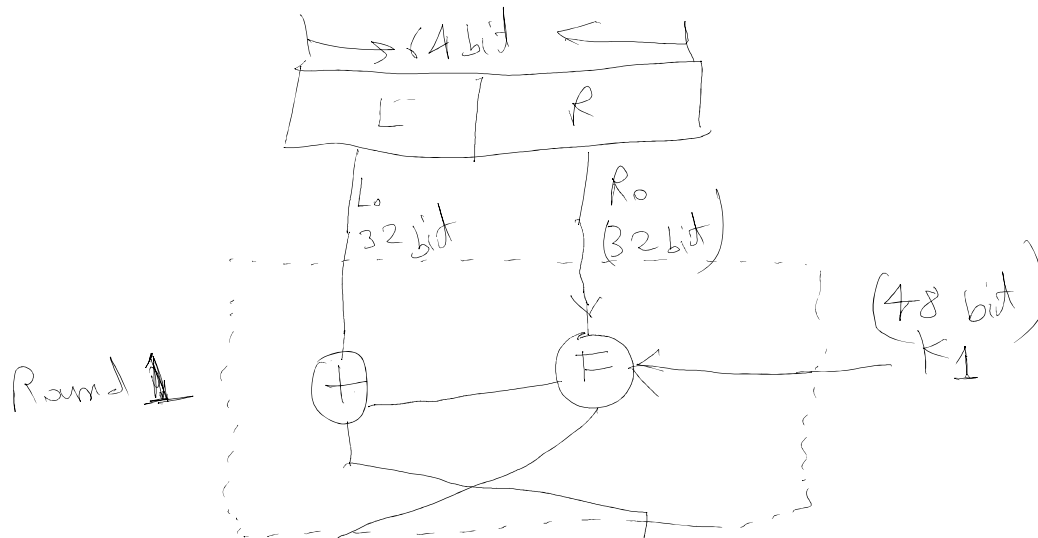
Final Permutation							
40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

1-16  
64 bit  
Final permutation

ciphertext



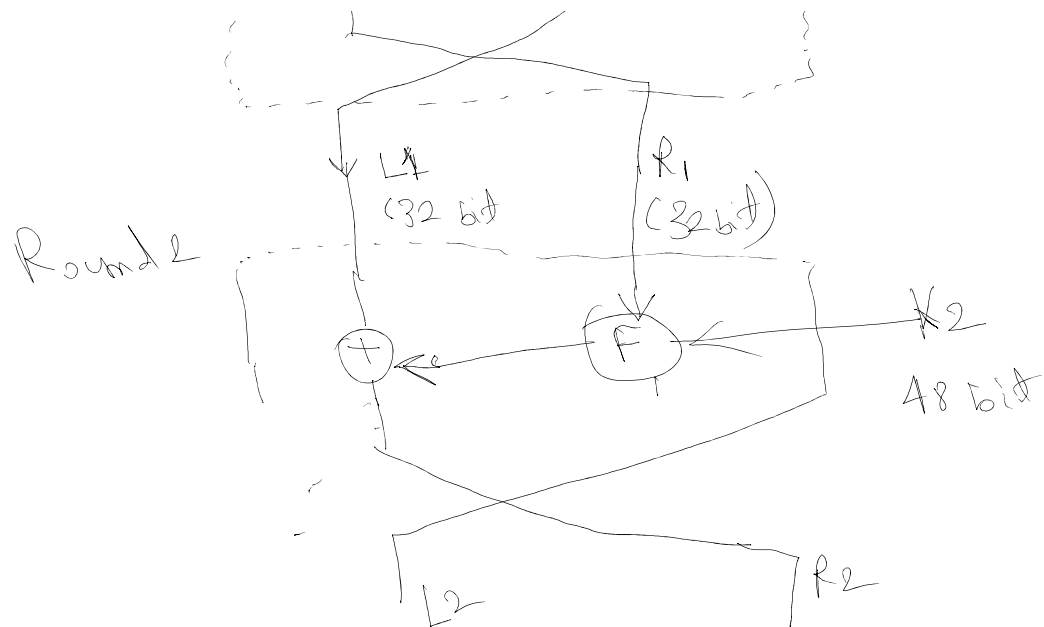
Functionality of Rounds in DES based on Feistel structure



Block features

- ① Block size (n)
- ② No. of Round (d)
- ③ Encryption method
- ④ Key size (48)

Round 1: Input (L<sub>0</sub>, R<sub>0</sub>, K<sub>1</sub>)  
output (L<sub>1</sub>, R<sub>1</sub>)



$$R_1 = f(R_0, K_1) \oplus L_0$$

$$L_1 = R_0$$

Round 2: Input ( $L_1, R_1, K_2$ )  
output ( $L_2, R_2$ )

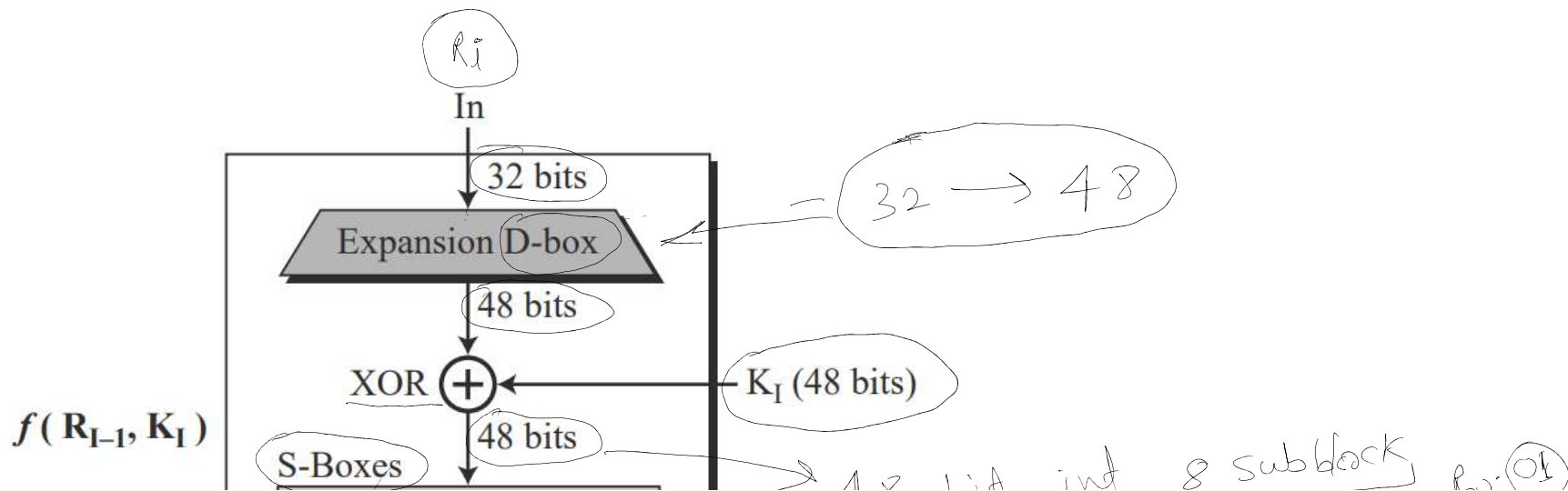
$$R_2 = f(R_1, K_2) \oplus L_1$$

$$L_2 = R_1$$

Heart of DES

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

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



$f(R_{i-1}, K_i)$

