DES (Data Encryption Algorithm):

Developed by NIST (National Institute of standard technology) would given in

- Symmetric key Block cipher (64 bit)
- It is implementation of feistal cipher Model (16 Rounds)
- DES has 16 Round.
- Block size is 64 bit. (plaintext & ciphertext)
- Key length is 56 bit. (original key is 64 bit but 8 bit are not used)

0 1 2 3 4 5 6 (7) 8 9 10 11 12 13 14 (15) 16 17 18 19 20 21 22 23

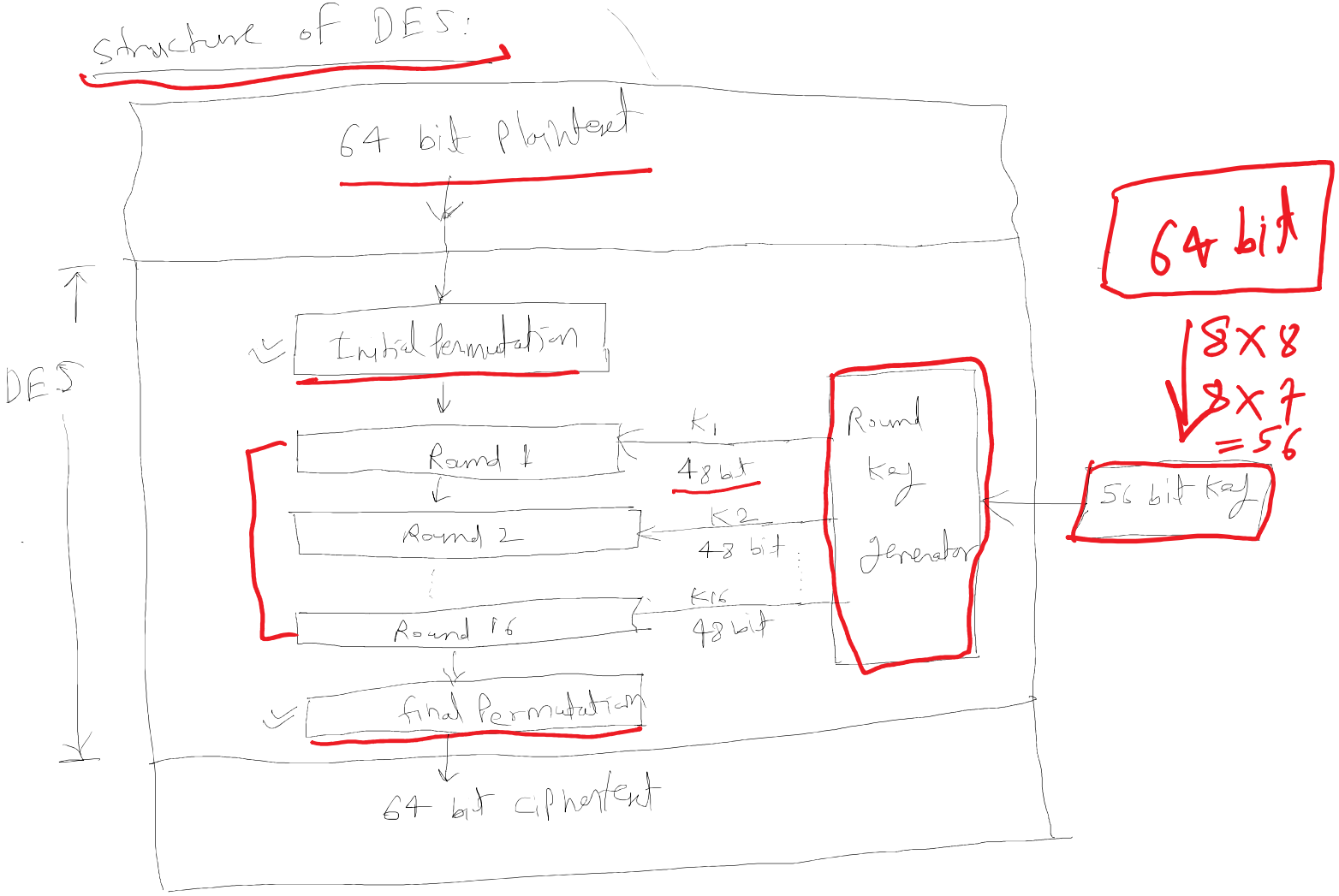
7 x 8 = 56 bit

7 bit lost 7 bit lost

---

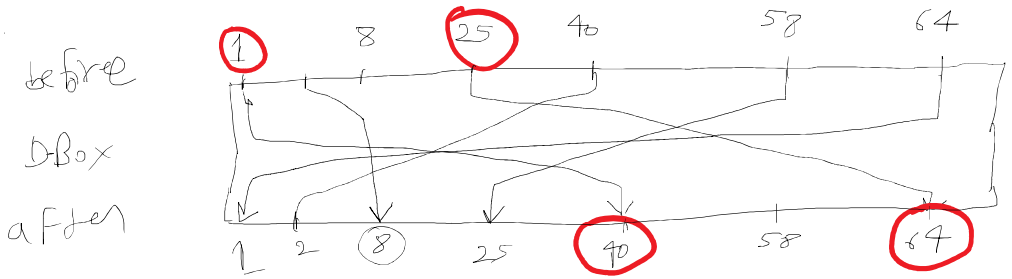
main functionality of DES:

1. Round function
2. key schedule
3. Additional processing (Initial & final permutation)



① Initial Permutation:

Initial & final Permutation are straight permutation Box used to 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

D-Box

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

40

64

Plaintext

1 2 3 4 ..... 63 64

Initial permutation

58, 50, 42, 34, 56 ..... 15, 07

Round 1-16

64 bit

Final permutation

Final permutation

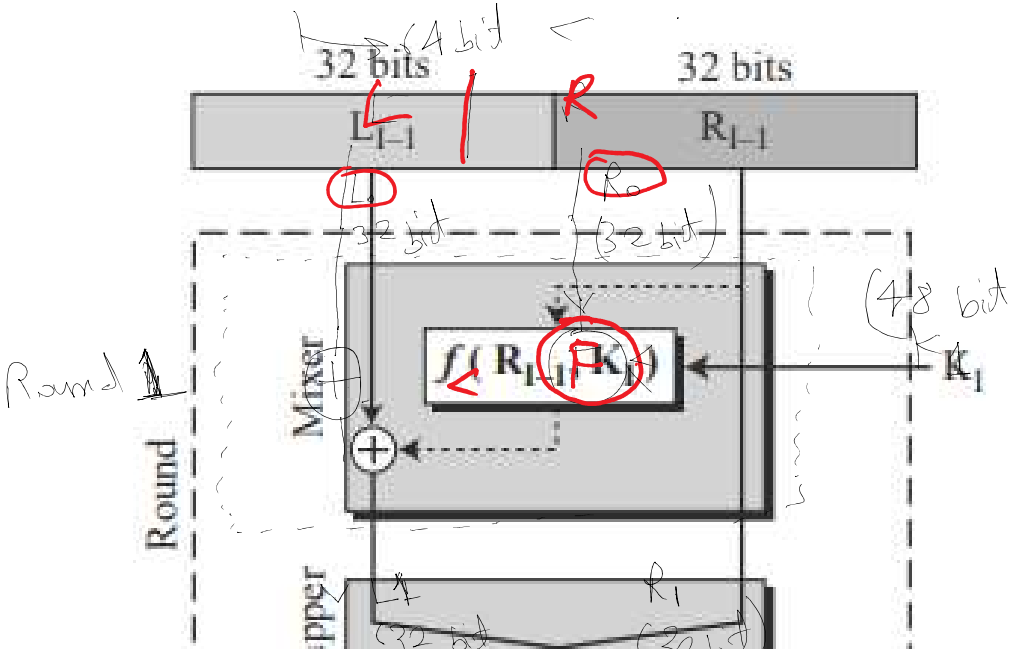
Final Permutation							
40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

Final permutation

ciphertext

64 ... 1

Functionality of Round in DES based on feistal structure



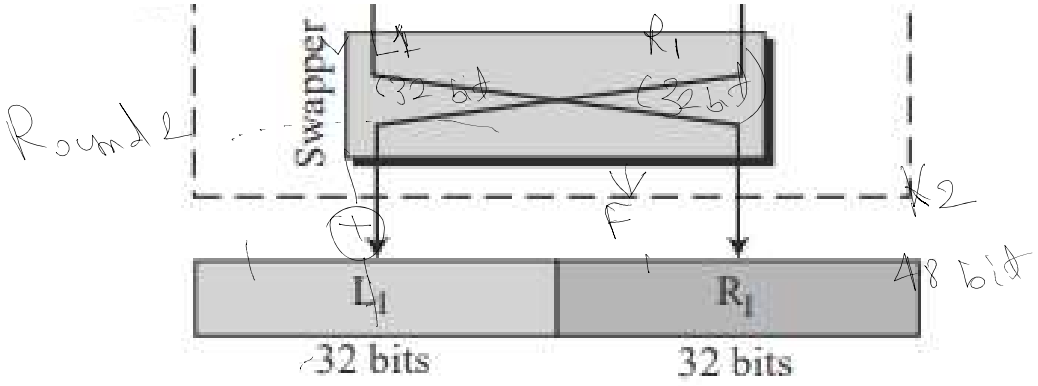
Block features

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

Round 1: Input (L_0, R_0, K_1)
output (L_1, R_1)

32 48

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



A round in DES (encryption site)

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

$L_1 = R_0$

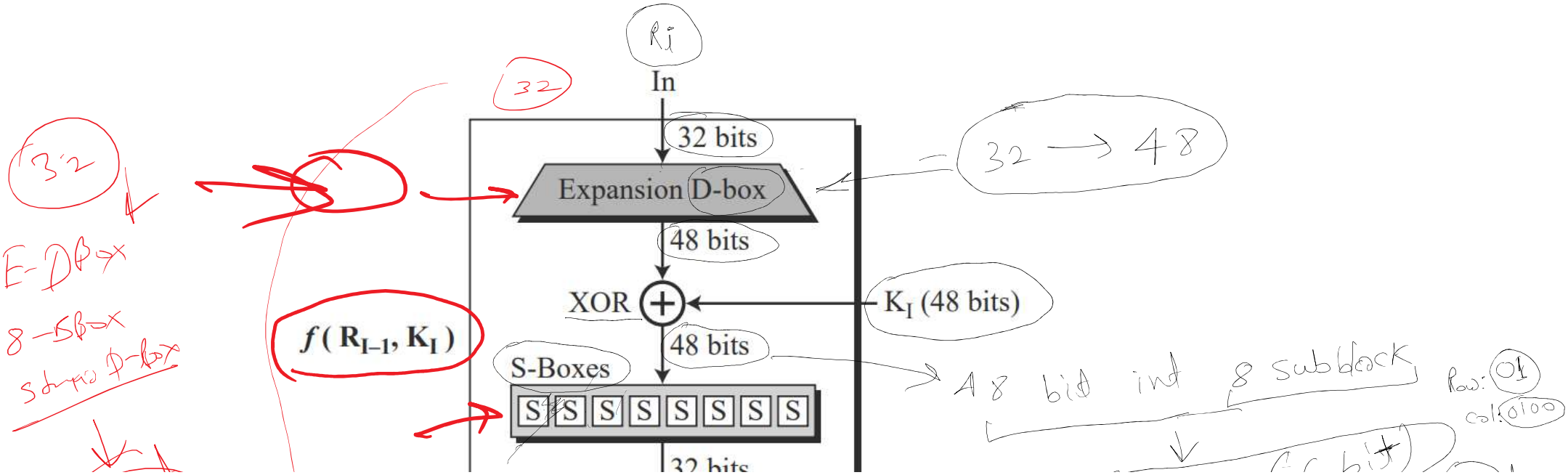
Round 2 : Input (L_1, R_1, K_2)
output (L_2, R_2)

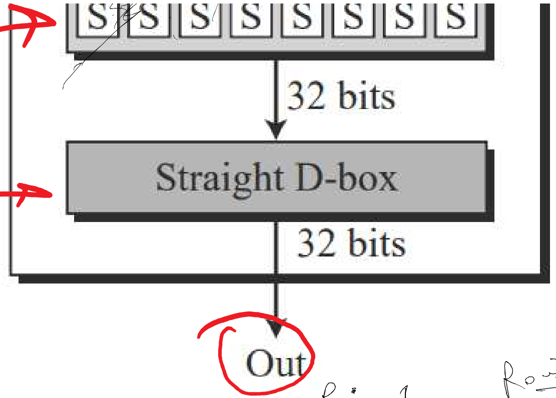
$R_2 = f(R_1, K_2) \oplus L_1$

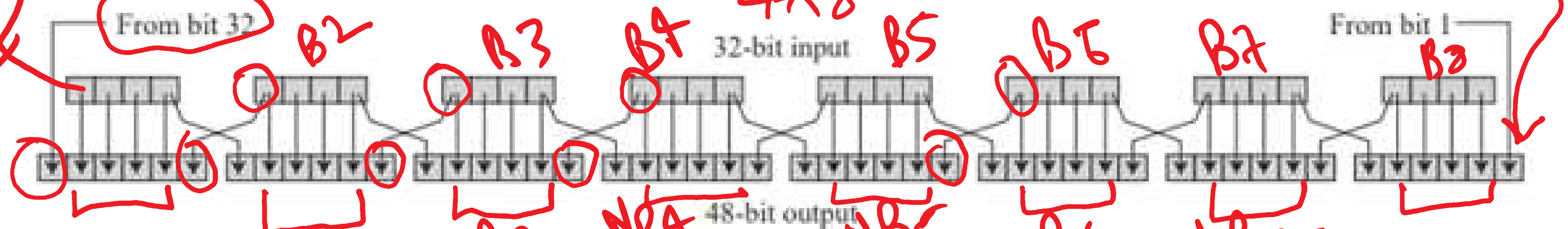
$L_2 = R_1$

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

$L_i = R_{i-1}$





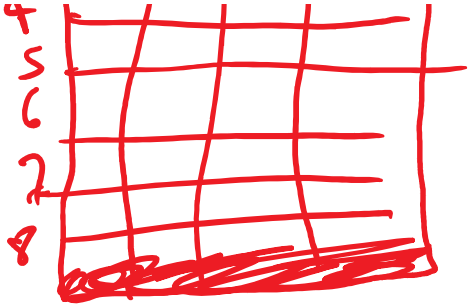


Expansion permutation

Expansion D-box table

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21

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	01

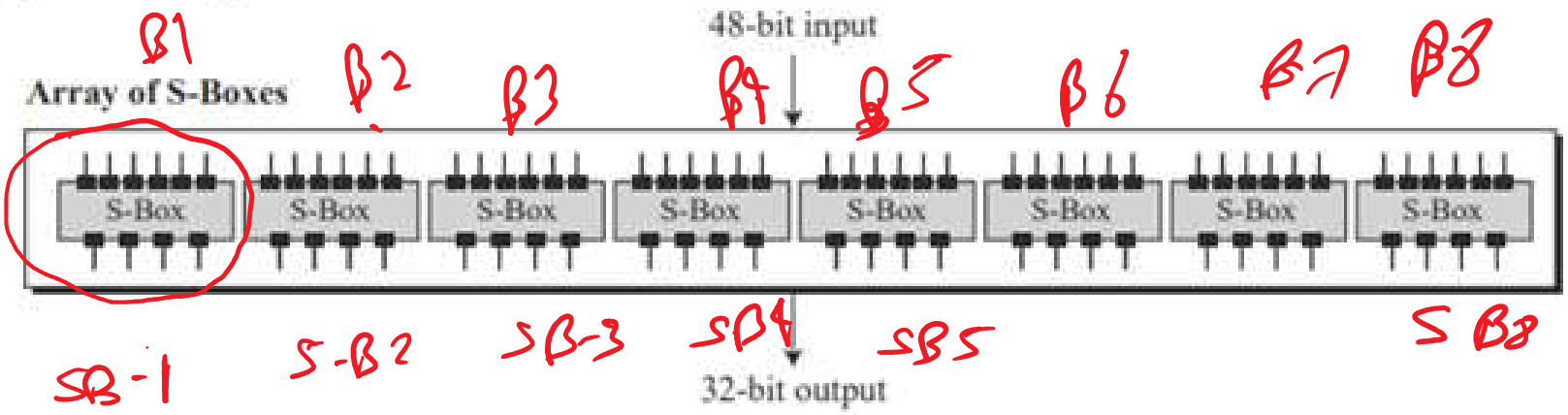


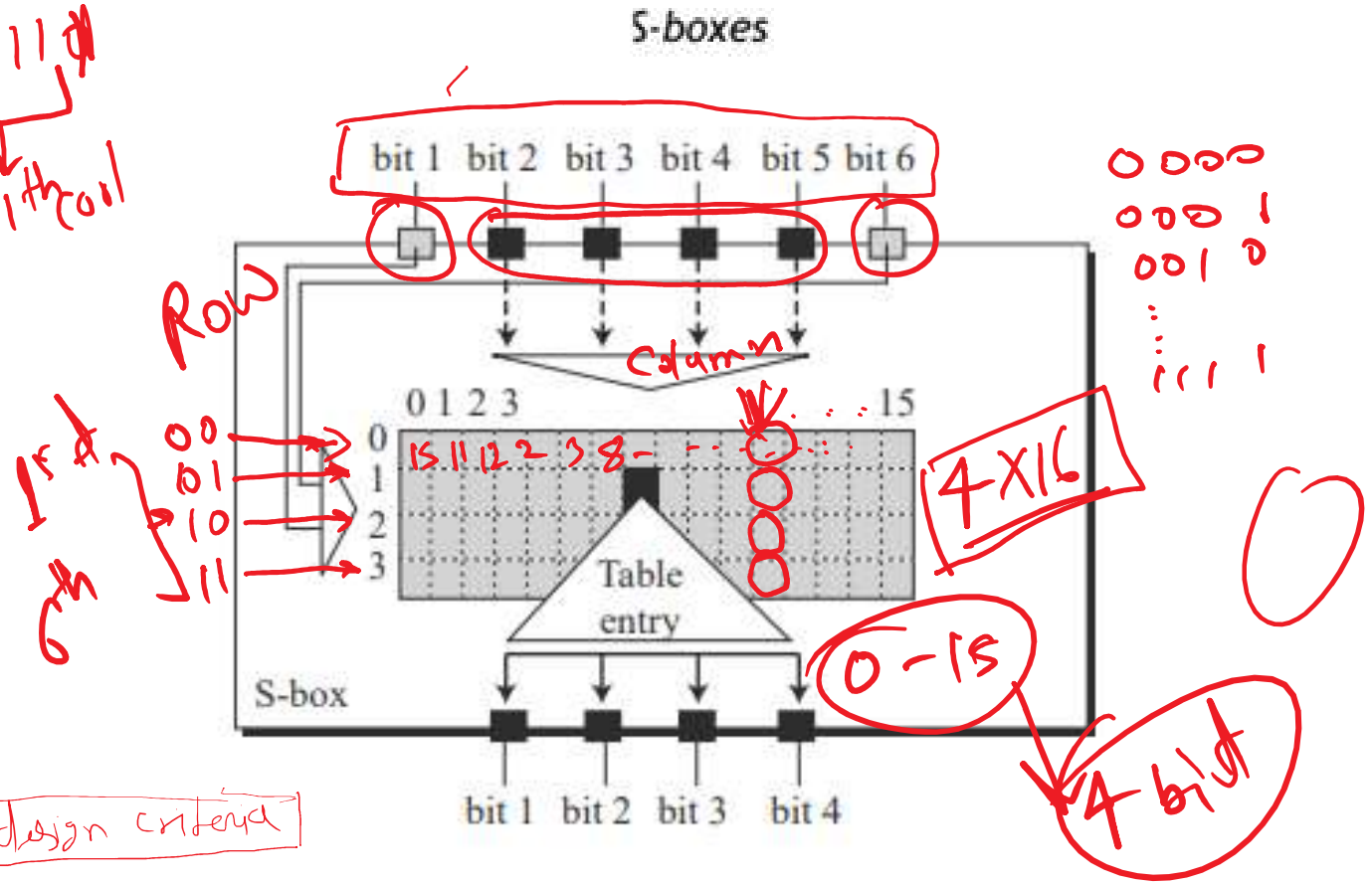
D-Box

Expansion D-Box

48 bit

6X8


48-bit input
Array of S-Boxes
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
32-bit output

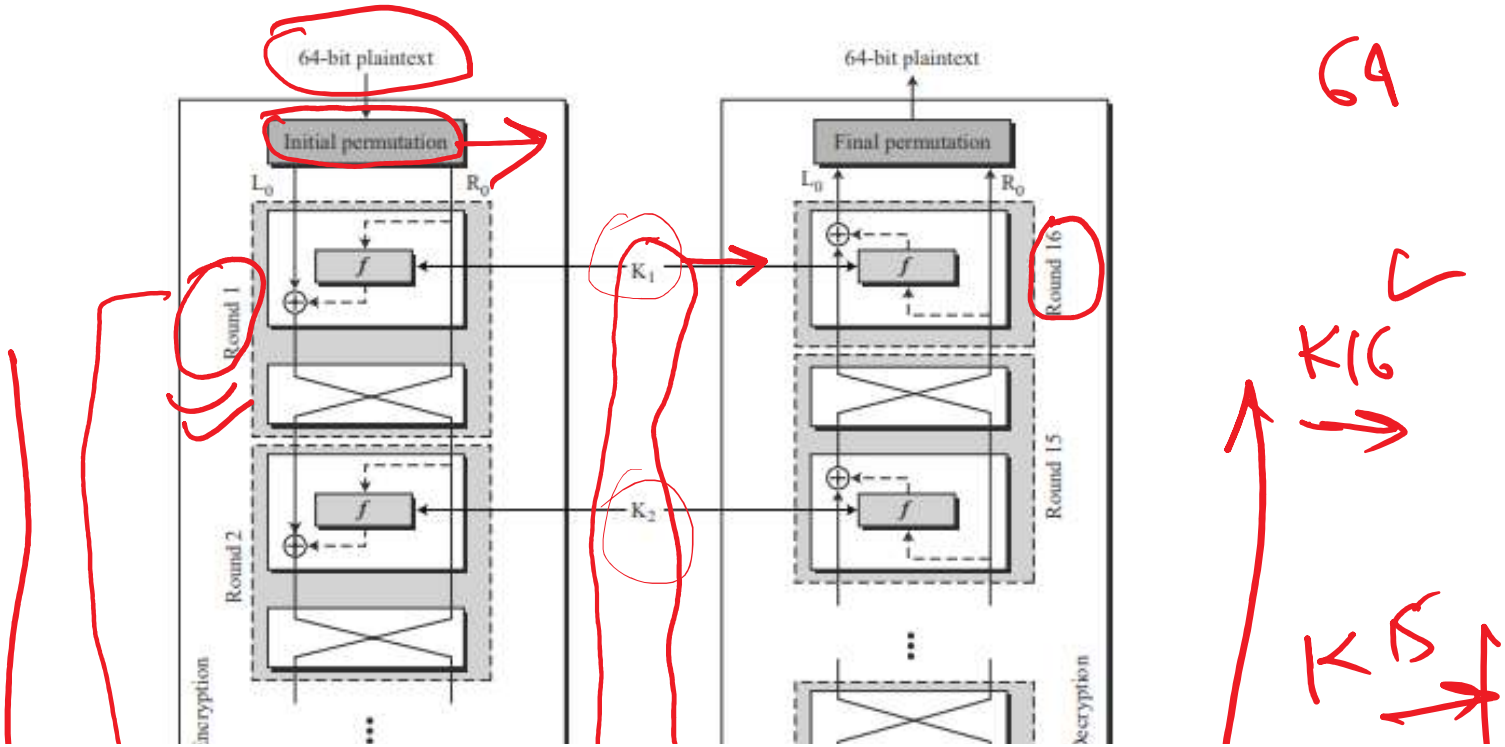

S-boxes
bit 1 bit 2 bit 3 bit 4 bit 5 bit 6
Row
Column
0 1 2 3
. . . 15
00
01
10
11
0
1
2
3
Table entry
S-box
bit 1 bit 2 bit 3 bit 4

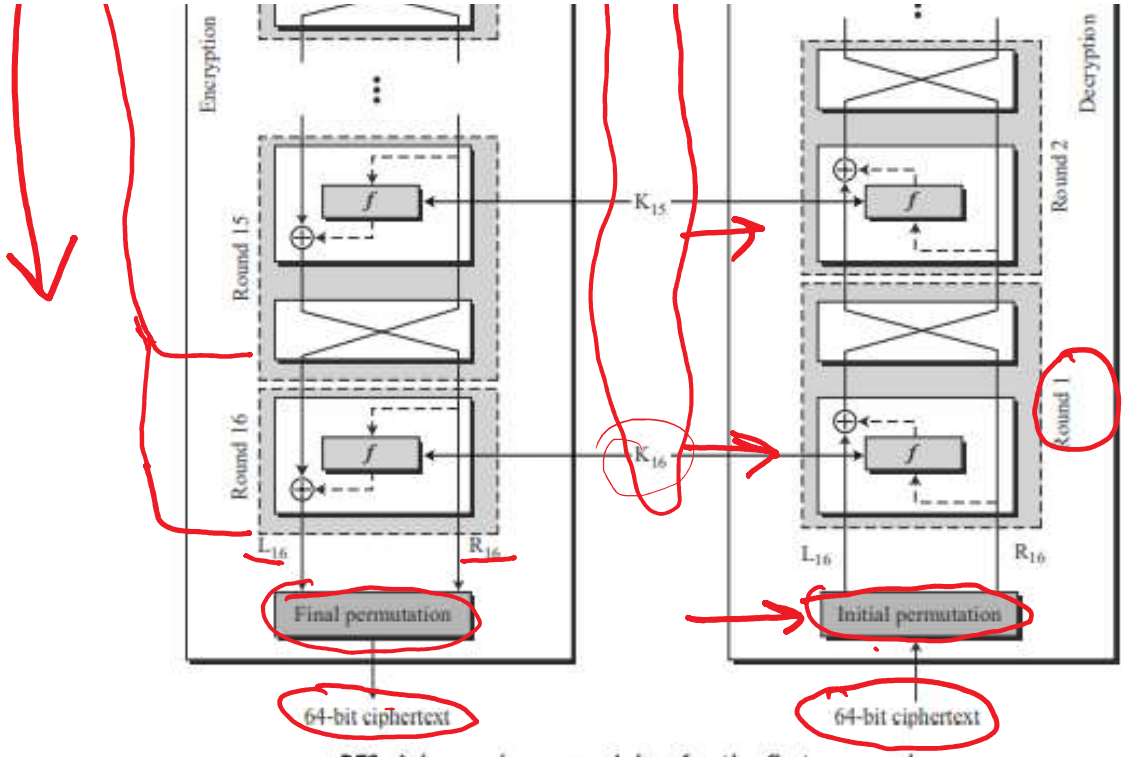
S-box 1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

S-box 2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
1	03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
2	00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
3	13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09





DES cipher and reverse cipher for the first approach

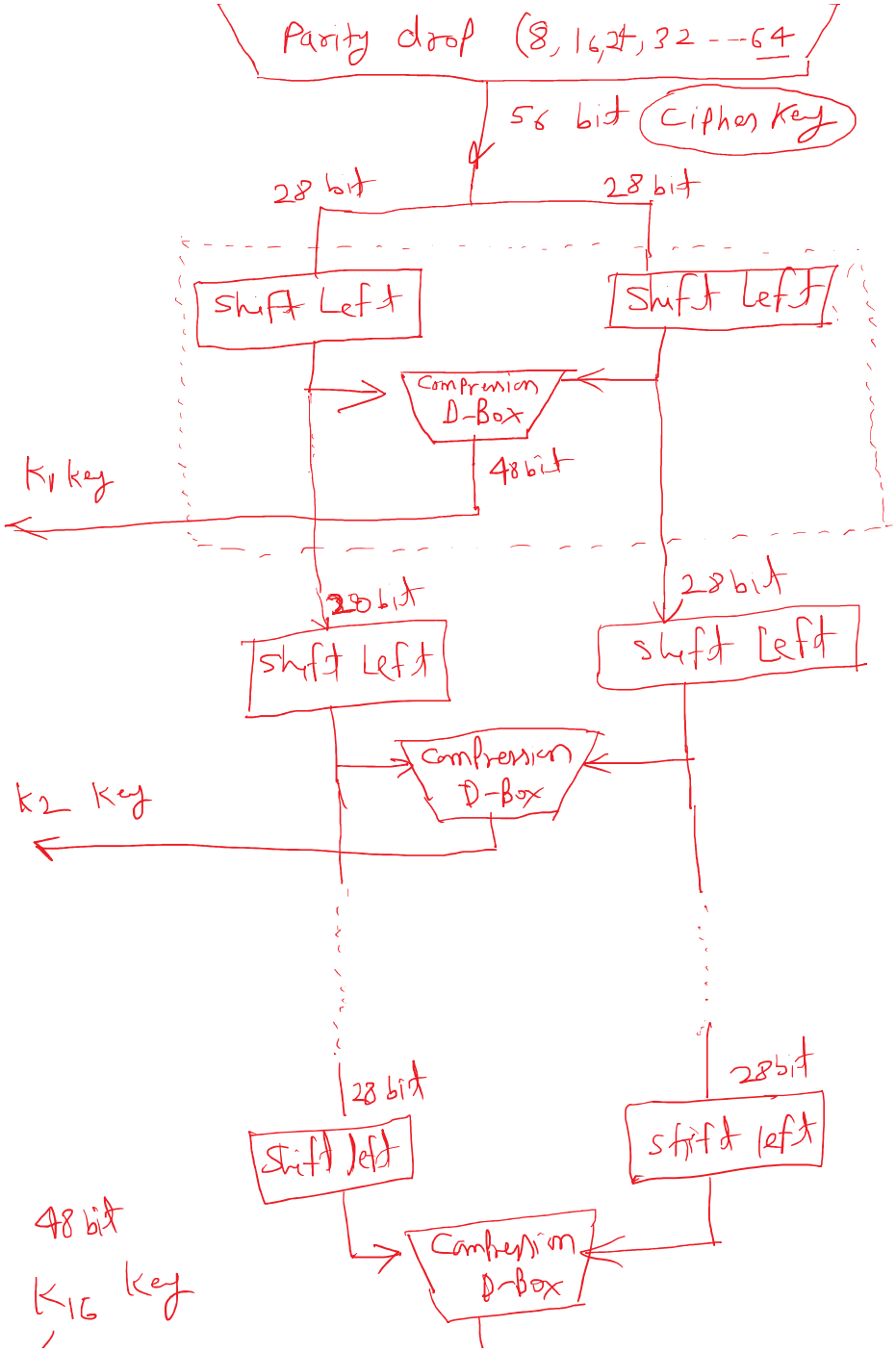
Sub-Key from K1 to K16

Key generation system (DES)

Key (64 bit)

↓ 64 bit → 8×8

Parity drop (8, 16, 24, 32 --- 64


Parity drop (8, 16, 24, 32 --- 64
56 bit
Cipher Key
28 bit
28 bit
Shift Left
Shift Left
Compression D-Box
48 bit
K1 key
28 bit
28 bit
Shift Left
Shift Left
Compression D-Box
K2 key
28 bit
28 bit
Shift left
Shift left
48 bit
Compression D-Box
K16 key

Shifting

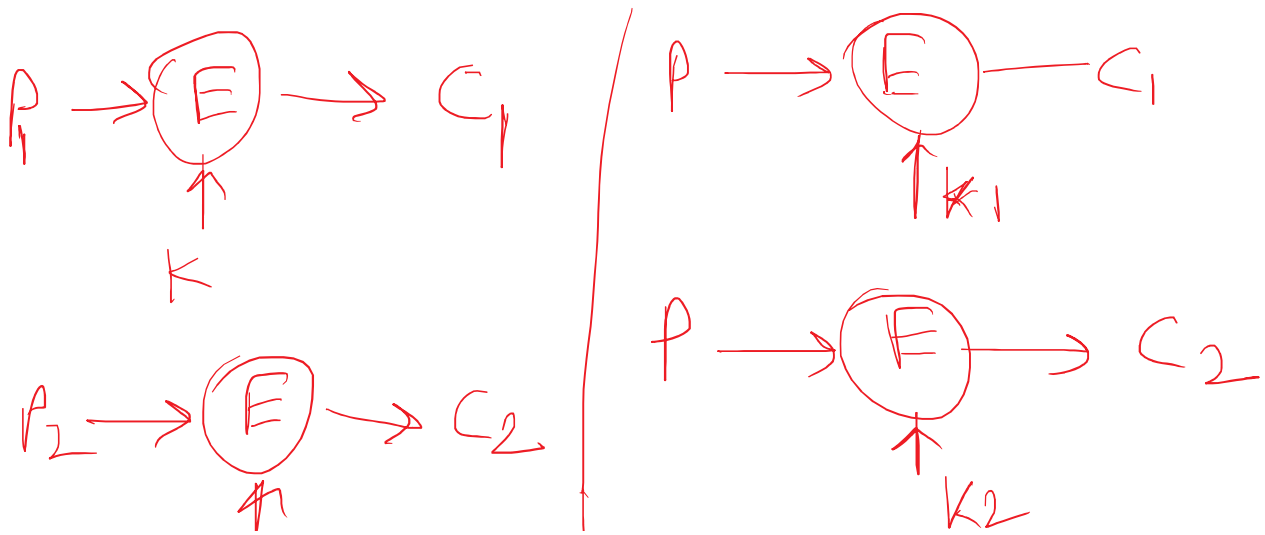
Round	Shift Left
1, 2, 9, 16	one bit
others	2 bit

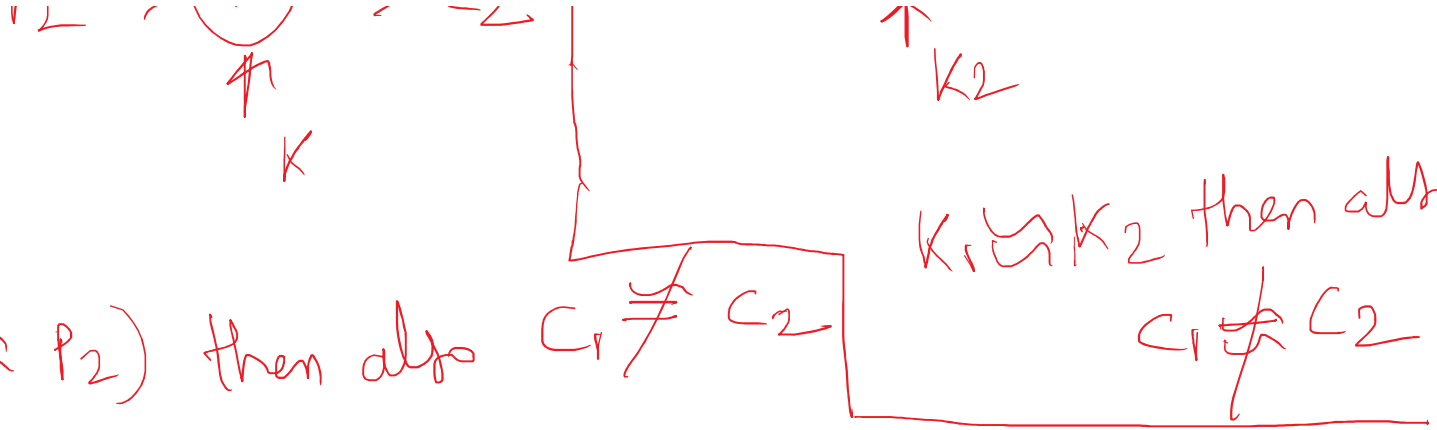
DES Analysis:

Desirable Property of block cipher

1. Avalanche effect:
2. completeness effect:

1. Avalanche effect:





It means small change in plaintext (or key) should create a significant change in the ciphertext.

Exa. Plaintext: 0000 0000 0000 0000

Key: 2223 4512 987A BB23

Cipher: 4789 FD47 6E82 A5 F1

Plaintext: 0000 0000 0000 0001

Plaintext: 0000 0000 0000 0001

key = 2223 4512 987A BB23

↳ Ciphen = 0A 4E D5 C1 5A63 FEA3

↓

.0011 (64th)

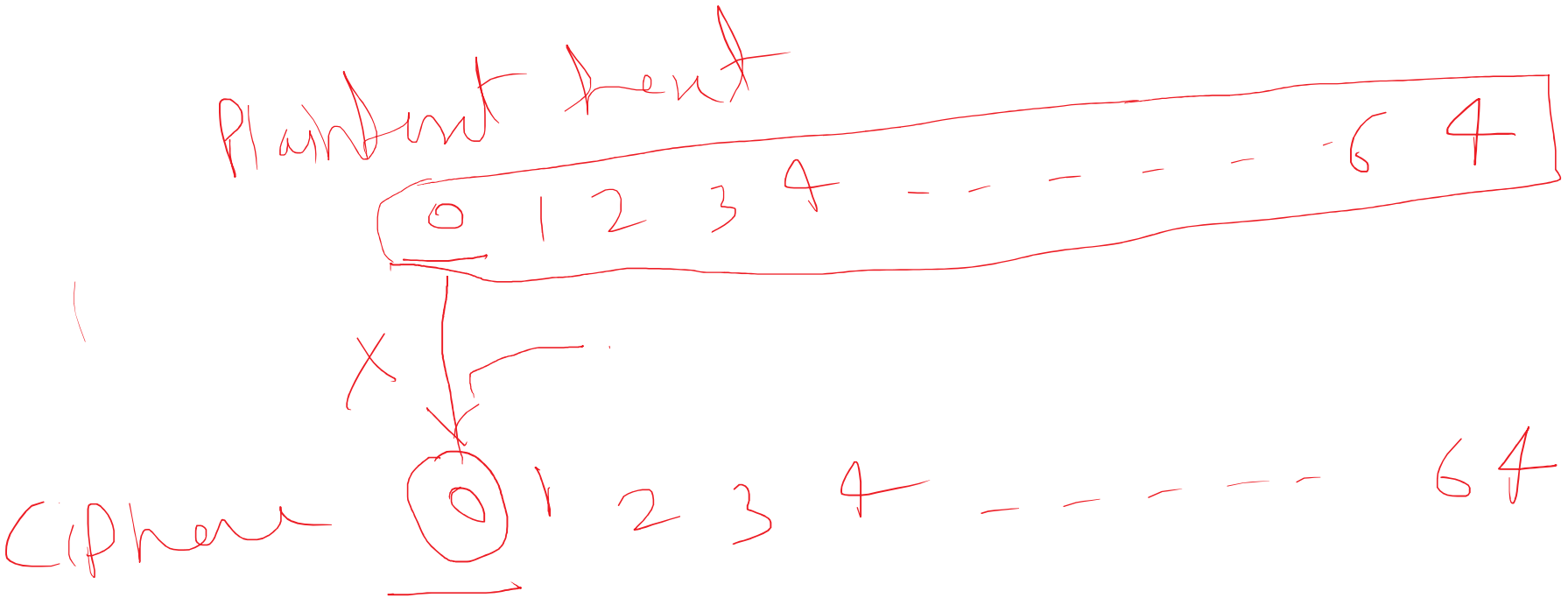
DES has been proved to be strong with regard to avalanche effect.

---

② completeness Effect:

It means that each bit of the Ciphertext need to be depend on many bits of plaintext.

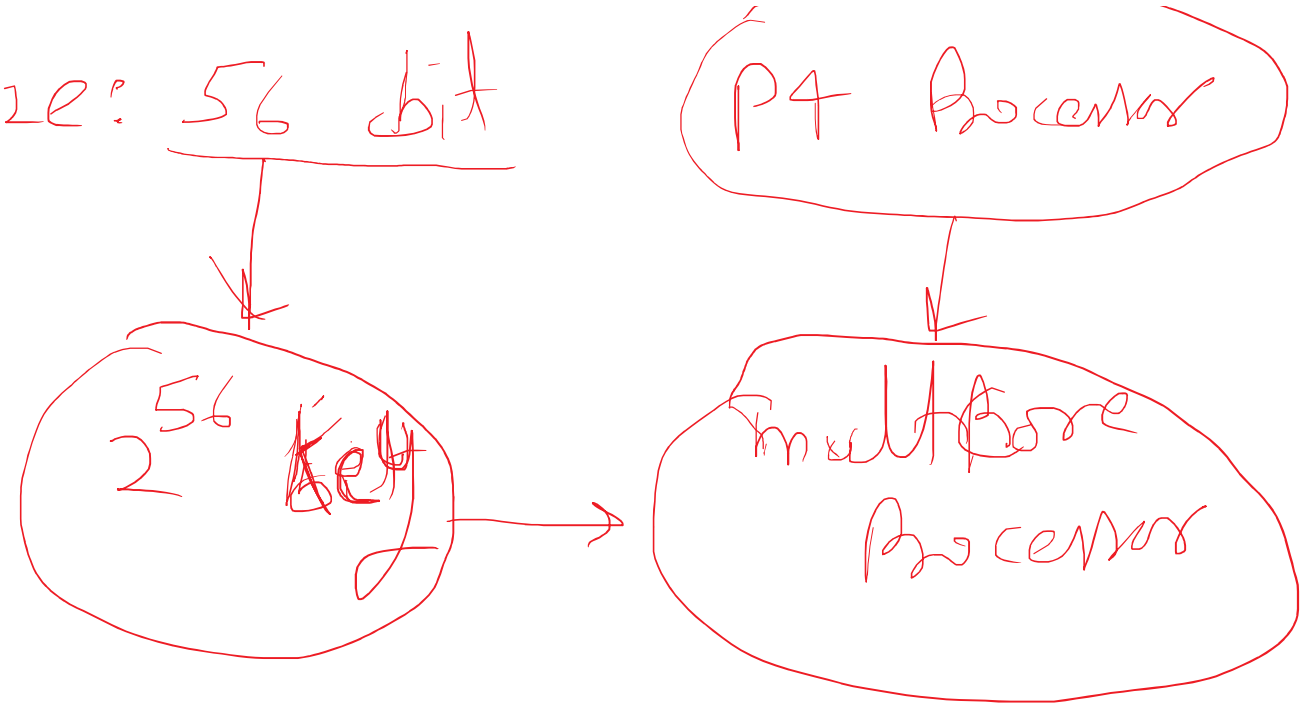
For DES this property is true. bcz of D-Box & S-Box



DES weaknesses:

(1) Key size 56 bit

① Key size: 56 bit



Many critics believe that the key size of DES that is only 56 bit long, is one of the weakness in DES.

Solve: Double DES (2 key) — (56 + 56) = (112 bit)

Triple DES (3 key) — (56 + 56 + 56) = 178 bit
(2 key)

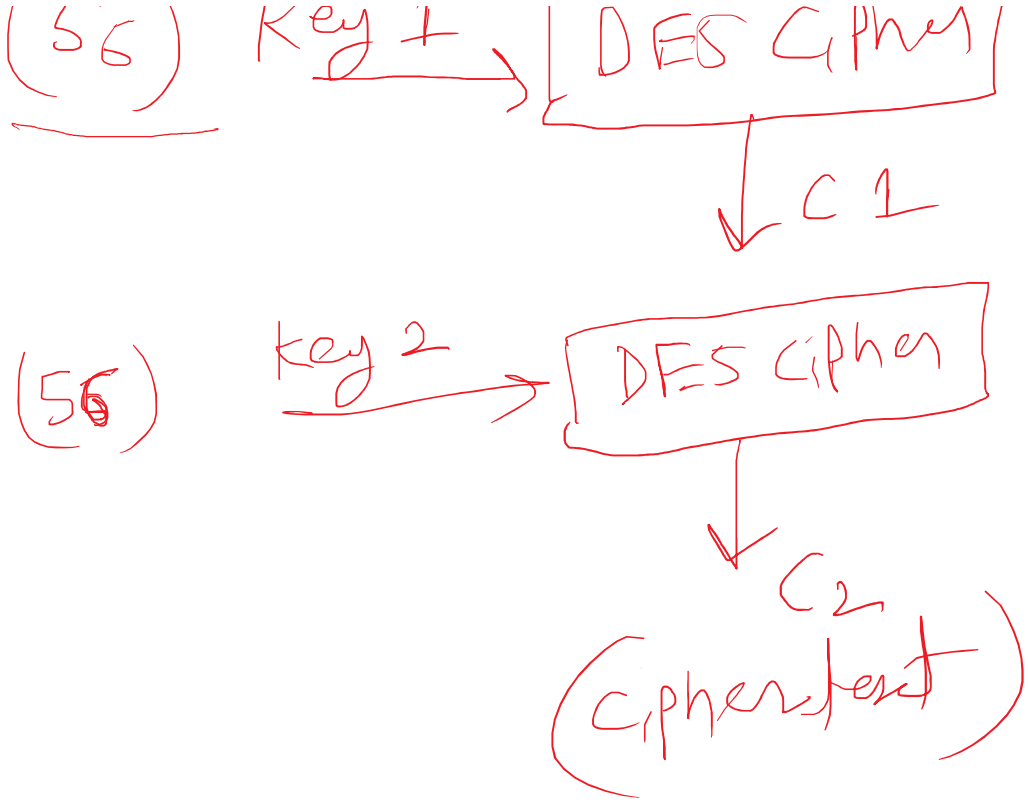
$2^{112} \approx$ Very large

Plaintext (64 bit)

↓

(56) Key 1 → [DES Cipher]

brute force



brute force

attacker

Key 1 Key 2

2^{56} * 2^{56}

difficult to crack

(2) weak Key:

(2) Weak key.

total key 2^{56}

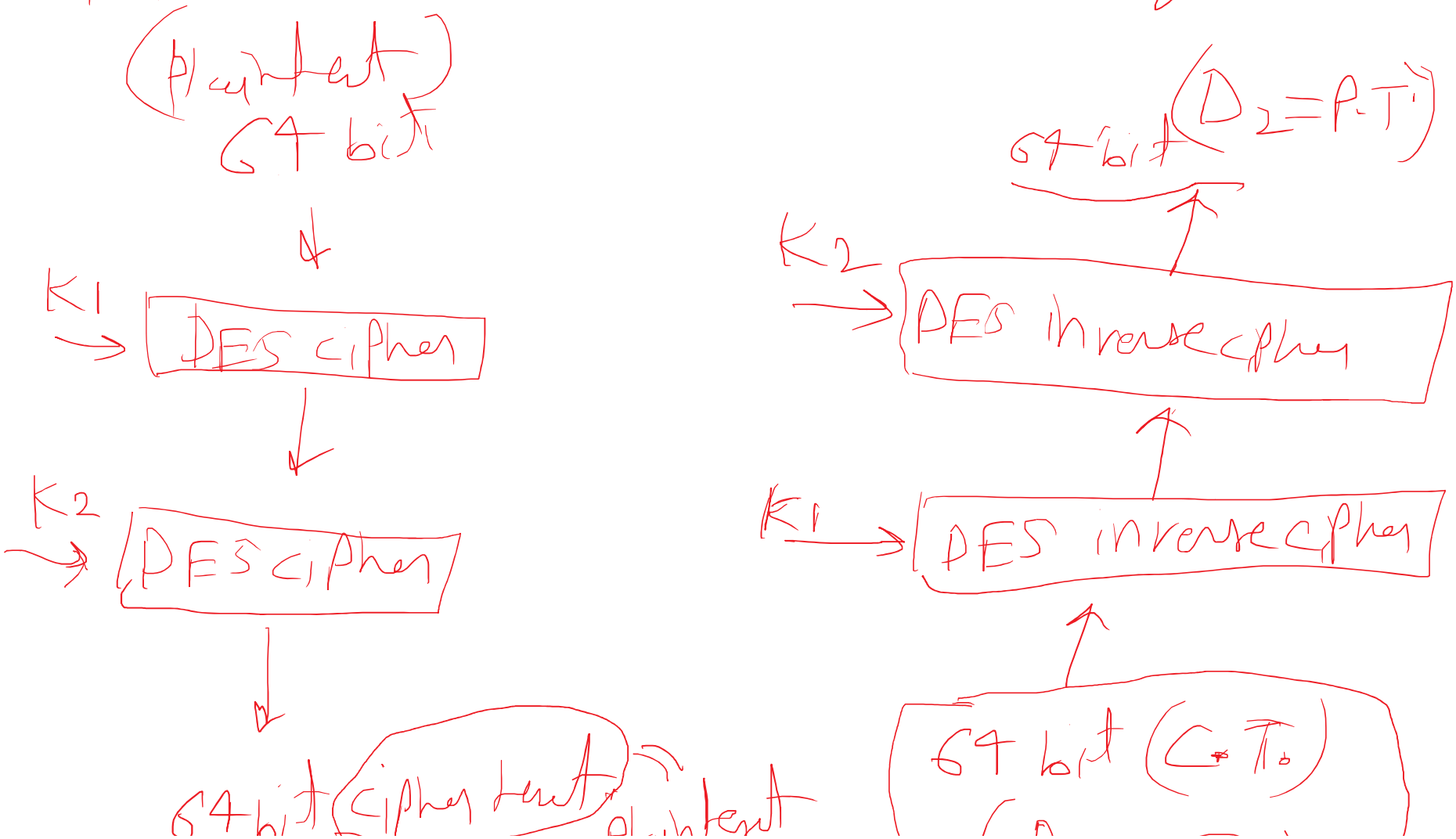
- researchers found four key as weak key.
- after the parity drop operation, a weak key is one which consists of all 0's, all 1's or half 0's and half 1's

	0 1 2 3 4 5 6	54 55
Key1:	0000000	---- 00
Key2:	1111111	---- 11
Key3:	1111111	---- 00 0000
Key4:	0 00 0000	---- 111111

Weak key

Key1 : 0 0 0 0 0 0 0 0 ---- 1 1 1 1 1 1 1 1

Disadvantage of using a weak key is:



64 bit (Ciphertext / Plaintext)

If K_1 & K_2 are weak key

then ciphertext = Plaintext

$D_1 = C \cdot T.$

if $D_1 = D_2$

then Attacker

know the key

if we encrypt a block of plaintext with weak key and subsequently encrypt the result with same key then we get

original block.

(3) Semi weak key:

researchers found 6 key pairs as semi weak key.

Semi weak key create only two diffent round keys and they each of them is repeated 8 times.

Key → K1(8), K2(8)

First key in the pair			
01FE	01FE	01FE	01FE
1FE0	1FE0	0EF1	0EF1
01E0	01E1	01F1	01F1
1FFE	1FFE	0EFE	0EFE
011F	011F	010E	010E
E0FE	E0FE	F1FE	F1FE

Round key 1	9153E54319BD	6EAC1ABCE642
Round key 2	6EAC1ABCE642	9153E54319BD
Round key 3	6EAC1ABCE642	9153E54319BD
Round key 4	6EAC1ABCE642	9153E54319BD
Round key 5	6EAC1ABCE642	9153E54319BD
Round key 6	6EAC1ABCE642	9153E54319BD
Round key 7	6EAC1ABCE642	9153E54319BD
Round key 8	6EAC1ABCE642	9153E54319BD
Round key 9	9153E54319BD	6EAC1ABCE642
Round key 10	9153E54319BD	6EAC1ABCE642
Round key 11	9153E54319BD	6EAC1ABCE642
Round key 12	9153E54319BD	6EAC1ABCE642
Round key 13	9153E54319BD	6EAC1ABCE642
Round key 14	9153E54319BD	6EAC1ABCE642
Round key 15	9153E54319BD	6EAC1ABCE642
Round key 16	6EAC1ABCE642	9153E54319BD

K1 → 9153E54319BD 6EAC1ABCE642

K2 → 6EAC1ABCE642 9153E54319BD (×8)

K1 → 9153E54319BD 6EAC1ABCE642 (×8)

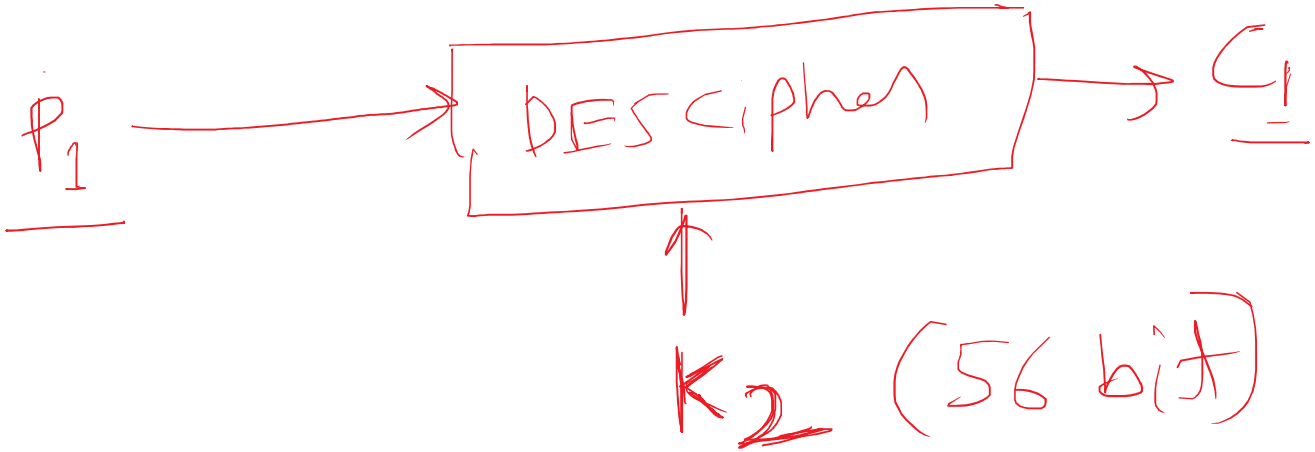
K2 → 6EAC1ABCE642 9153E54319BD

④ Possible weak key:

researchers found 48 key as possible weak key

that keys create only 4 distinct round key. means the 16 Round key are divided into 4 groups and each group is made of 4 equal keys.

(5) Key clustering :



$\therefore K_1 \neq K_2$

① Double DES → Man in middle attack

② Triple DES