The Islamic University
College of Technical Engineering
Department of Computer Technical Engineering

Fourth Stage

Security

Lecture 15

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objective

The student will recognize the following Contents:

- **Data Encryption Standard (DES).**
  - **Example.**

Example

Find the ciphertext for the plaintext below for the first round by using **Data Encryption Standard (DES)**.

P = 0 1 2 3 4 5 6 7 8 9 A B C D E F

K = 0 1 2 3 4 5 6 7 8 9 A B C D E F

Ans:-

First we have to prepare the encryption key for the **first** round.

1. Key Generation

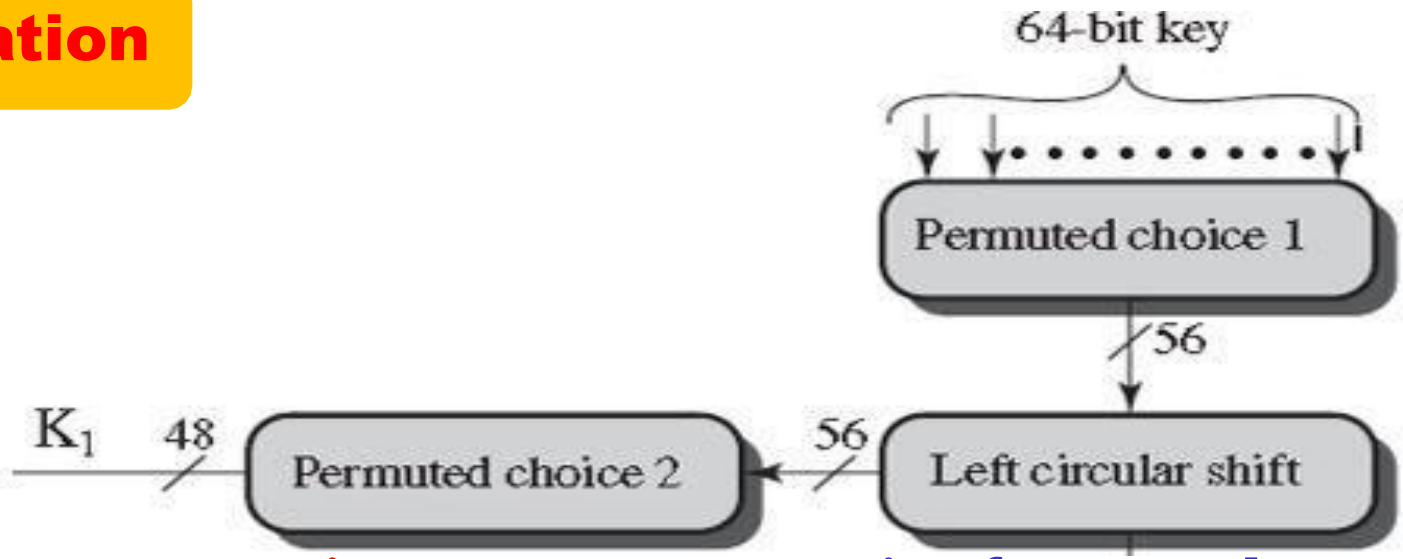


Figure 1: Key generation for Round 1.

1. distribute a 64 bit key K = 0 1 2 3 4 5 6 7 8 9 A B C D E F

Key (Hex)	Key (Binary)
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Table 1: Input Key.

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

1. Key Generation

1 0	2 0	3 0	4 0	5 0	6 0	7 0	8 1
9 0	10 0	11 1	12 0	13 0	14 0	15 1	16 1
17 0	18 1	19 0	20 0	21 0	22 1	23 0	24 1
25 0	26 1	27 1	28 0	29 0	30 1	31 1	32 1
33 1	34 0	35 0	36 0	37 1	38 0	39 0	40 1
41 1	42 0	43 1	44 0	45 1	46 0	47 1	48 1
49 1	50 1	51 0	52 0	53 1	54 1	55 0	56 1
57 1	58 1	59 1	60 0	61 1	62 1	63 1	64 1

2. Rearrange the 56 bit key as Permuted Choice One PC-1.

1	0	2	0	3	0	4	0	5	0	6	0	7	0	8	1
9	0	10	0	11	1	12	0	13	0	14	0	15	1	16	1
17	0	18	1	19	0	20	0	21	0	22	1	23	0	24	1
25	0	26	1	27	1	28	0	29	0	30	1	31	1	32	1
33	1	34	0	35	0	36	0	37	1	38	0	39	0	40	1
41	1	42	0	43	1	44	0	45	1	46	0	47	1	48	1
49	1	50	1	51	0	52	0	53	1	54	1	55	0	56	1
57	1	58	1	59	1	60	0	61	1	62	1	63	1	64	1

Table 2: Permuted Choice One (PC-1).

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

1	1	1	1	0	0	0
0	1	1	0	0	1	1
0	0	1	0	1	0	1
0	1	0	0	0	0	0
1	0	1	0	1	0	1
0	1	1	0	0	1	1
0	0	1	1	1	1	0
0	0	0	0	0	0	0

8 x 7
Matrix 56 bit

1	1	1	1	0	0	0
0	1	1	0	0	1	1
0	0	1	0	1	0	1
0	1	0	0	0	0	0
1	0	1	0	1	0	1
0	1	1	0	0	1	1
0	0	1	1	1	1	0
0	0	0	0	0	0	0

C_0

1	1	1	1	0	0	0
0	1	1	0	0	1	1
0	0	1	0	1	0	1
0	1	0	0	0	0	0

D_0

1	0	1	0	1	0	1
0	1	1	0	0	1	1
0	0	1	1	1	1	0
0	0	0	0	0	0	0

2. Left Shifts for Round 1.

Table 3: Number of bit shifts.

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

C_0

1	1	1	1	0	0	0
0	1	1	0	0	1	1
0	0	1	0	1	0	1
0	1	0	0	0	0	0

D_0

1	0	1	0	1	0	1
0	1	1	0	0	1	1
0	0	1	1	1	1	0
0	0	0	0	0	0	0

C_1

1	1	1	0	0	0	0
1	1	0	0	1	1	0
0	1	0	1	0	1	0
1	0	0	0	0	0	1

D_1

0	1	0	1	0	1	0
1	1	0	0	1	1	0
0	1	1	1	1	0	0
0	0	0	0	0	0	1

3. Rearrange the 48 bit key as Permuted Choice Two PC-2.

1 1	2 1	3 1	4 0	5 0	6 0	7 0
8 1	9 1	10 0	11 0	12 1	13 1	14 0
15 0	16 1	17 0	18 1	19 0	20 1	21 0
22 1	23 0	24 0	25 0	26 0	27 0	28 1
29 0	30 1	31 0	32 1	33 0	34 1	35 0
36 1	37 1	38 0	39 0	40 1	41 1	42 0
43 0	44 1	45 1	46 1	47 1	48 0	49 0
50 0	51 0	52 0	53 0	54 0	55 0	56 1

Table 4: Permuted Choice Two (PC-2).

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

0	0	0	0	1	0	1	1
0	0	0	0	0	0	1	0
0	1	1	0	0	1	1	1
1	0	0	1	1	0	1	1
0	1	0	0	1	0	0	1
1	0	1	0	0	1	0	1

Single Round of DES Algorithm

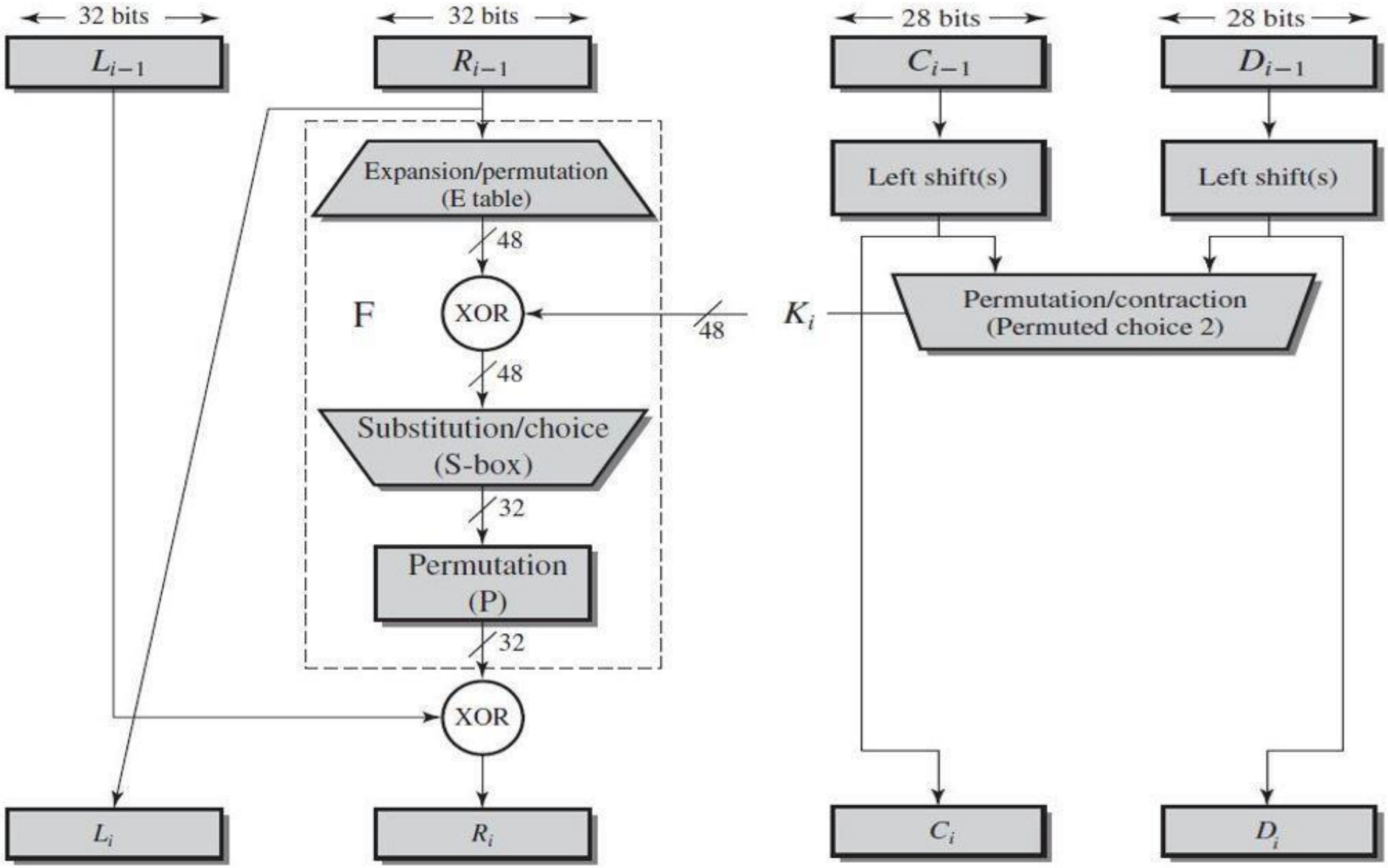


Figure 2: Single Round of DES Algorithm.

2. Plaintext

P = 0 1 2 3 4 5 6 7 8 9 A B C D EF

1. Convert the plaintext from Hexadecimal to Binary.

1 0	2 0	3 0	4 0	5 0	6 0	7 0	8 1
9 0	10 0	11 1	12 0	13 0	14 0	15 1	16 1
17 0	18 1	19 0	20 0	21 0	22 1	23 0	24 1
25 0	26 1	27 1	28 0	29 0	30 1	31 1	32 1
33 1	34 0	35 0	36 0	37 1	38 0	39 0	40 1
41 1	42 0	43 1	44 0	45 1	46 0	47 1	48 1
49 1	50 1	51 0	52 0	53 1	54 1	55 0	56 1
57 1	58 1	59 1	60 0	61 1	62 1	63 1	64 1

Key (Hex)	Key (Binary)
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

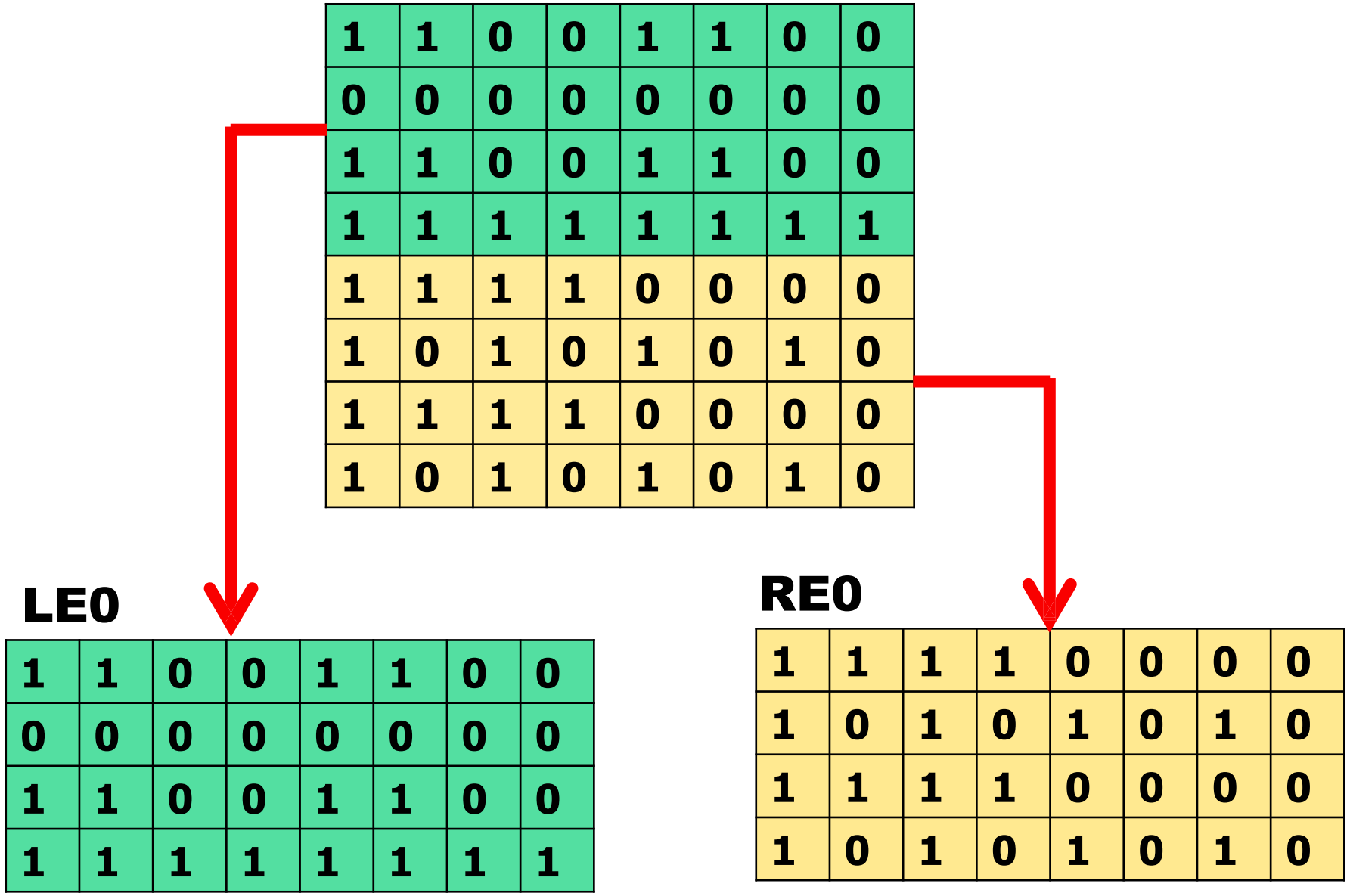
2. Apply Initial Permutation (IP).

1	0	2	0	3	0	4	0	5	0	6	0	7	0	8	1
9	0	10	0	11	1	12	0	13	0	14	0	15	1	16	1
17	0	18	1	19	0	20	0	21	0	22	1	23	0	24	1
25	0	26	1	27	1	28	0	29	0	30	1	31	1	32	1
33	1	34	0	35	0	36	0	37	1	38	0	39	0	40	1
41	1	42	0	43	1	44	0	45	1	46	0	47	1	48	1
49	1	50	1	51	0	52	0	53	1	54	1	55	0	56	1
57	1	58	1	59	1	60	0	61	1	62	1	63	1	64	1

Table 5: Initial Permutation (IP).

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

1	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0
1	1	0	0	1	1	0	0
1	1	1	1	1	1	1	1
1	1	1	1	0	0	0	0
1	0	1	0	1	0	1	0
1	1	1	1	0	0	0	0
1	0	1	0	1	0	1	0


1 1 0 0 1 1 0 0
0 0 0 0 0 0 0 0
1 1 0 0 1 1 0 0
1 1 1 1 1 1 1 1
1 1 1 1 0 0 0 0
1 0 1 0 1 0 1 0
1 1 1 1 0 0 0 0
1 0 1 0 1 0 1 0
LE0
1 1 0 0 1 1 0 0
0 0 0 0 0 0 0 0
1 1 0 0 1 1 0 0
1 1 1 1 1 1 1 1
RE0
1 1 1 1 0 0 0 0
1 0 1 0 1 0 1 0
1 1 1 1 0 0 0 0
1 0 1 0 1 0 1 0

3. Select right and left side then put the right into E-Table.

Table 6: Expansion P-box Table.

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

RE0

1 1	1 2	1 3	1 4	0 5	0 6	0 7	0 8
1 9	0 10	1 11	0 12	1 13	0 14	1 15	0 16
1 17	1 18	1 19	1 20	0 21	0 22	0 23	0 24
1 25	0 26	1 27	0 28	1 29	0 30	1 31	0 32

0	1	1	1	1	0
1	0	0	0	0	1
0	1	0	1	0	1
0	1	0	1	0	1
0	1	1	1	1	0
1	0	0	0	0	1
0	1	0	1	0	1
0	1	0	1	0	1

4. XOR the 48 bit from the E-Table and the 48 bit key.

Expansion P-box Table

0	1	1	1	1	0
1	0	0	0	0	1
0	1	0	1	0	1
0	1	0	1	0	1
0	1	1	1	1	0
1	0	0	0	0	1
0	1	0	1	0	1
0	1	0	1	0	1

⊕

0	0	0	0	1	0
1	1	0	0	0	0
0	0	1	0	0	1
1	0	0	1	1	1
1	0	0	1	1	0
1	1	0	1	0	0
1	0	0	1	1	0
1	0	0	1	0	1

48 bit key

0	1	1	1	0	0
0	1	0	0	0	1
0	1	1	1	0	0
1	1	0	0	1	0
1	1	1	0	0	0
0	1	0	1	0	1
1	1	0	0	1	1
1	1	0	0	0	0

5. Process the output through S-box.

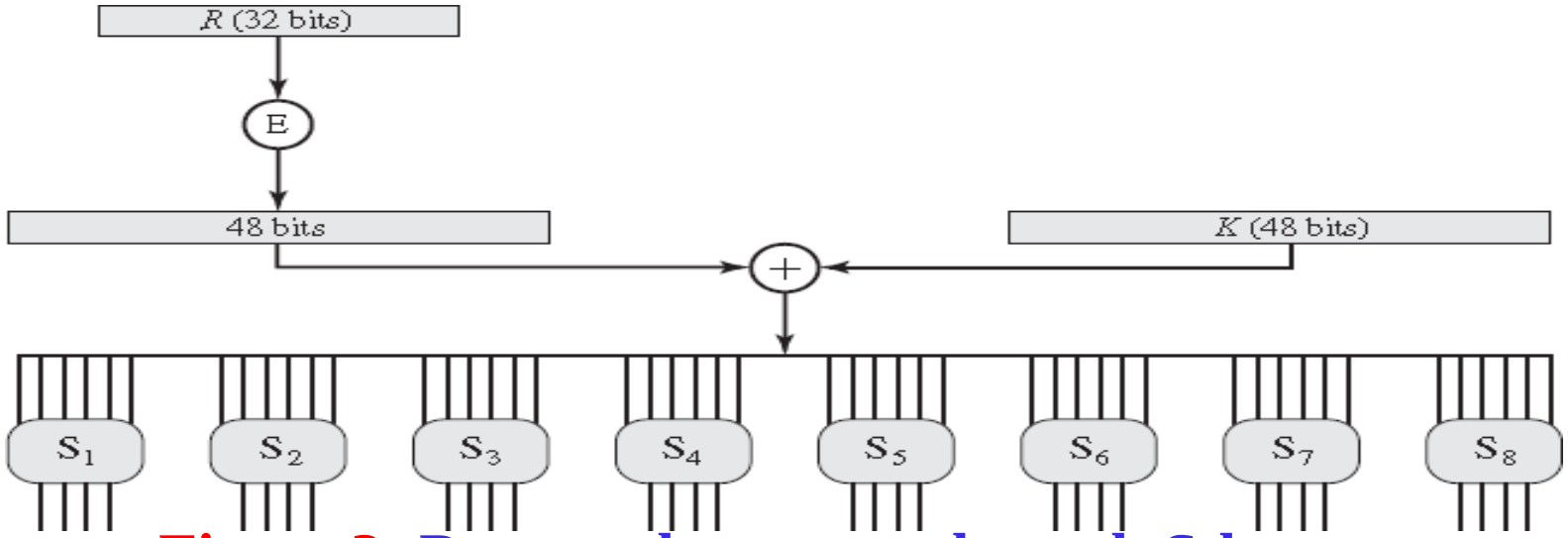


Figure 3: Process the output through S-box.

0	1	1	1	0	0
0	1	0	0	0	1
0	1	1	1	0	0
1	1	0	0	1	0
1	1	1	0	0	0
0	1	0	1	0	1
1	1	0	0	1	1
1	1	0	0	0	0

S1= 011100, R = 00, C = 1110 = 0= 0000

S2 = 010001, R = 01, C = 1000 = 12= 1100

S3 = 011100, R = 00, C = 1110 = 2 = 0010

S4 = 110010, R = 10, C = 1001= 1= 0001

S5 = 111000, R = 10, C = 1100 = 6= 0110

S6 = 010101, R= 01, C = 1010 = 13 = 1101

S7 = 110011, R = 11, C = 1001 = 5 = 0101

S8 = 110000, R = 10, C = 1000= 0 = 0000

S-Boxes

Table 7: 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

Table 8: 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

S-Boxes

Table 9: S-box 3.

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

Table 10: S-box 4.

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

S-Boxes

Table 11: S-box 5.

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

Table 12: S-box 6.

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

S-Boxes

Table 13: S-box 7.

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

Table 14: S-box 8.

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

6. Permutation Function the output bits from the S-box.

0	1	0	2	0	3	0	4
1	5	1	6	0	7	0	8
0	9	0	10	1	11	0	12
0	13	0	14	0	15	1	16
0	17	1	18	1	19	0	20
1	21	1	22	0	23	1	24
0	25	1	26	0	27	1	28
0	29	0	30	0	31	0	32

Table 15: Permutation Function (P) or Straight P-box.

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

1	0	0	1	0	0	1	0
0	0	0	1	1	1	0	0
0	0	1	0	0	0	0	0
1	0	0	1	1	1	0	0

4. Permutation Function XORLE0.

LE0

1	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0
1	1	0	0	1	1	0	0
1	1	1	1	1	1	1	1

⊕

1	0	0	1	0	0	1	0
0	0	0	1	1	1	0	0
0	0	1	0	0	0	0	0
1	0	0	1	1	1	0	0

Permutation Function (P)

LE1 = RE0

1	1	1	1	0	0	0	0
1	0	1	0	1	0	1	0
1	1	1	1	0	0	0	0
1	0	1	0	1	0	1	0

RE1

0	1	0	1	1	1	1	0
0	0	0	1	1	1	0	0
1	1	1	0	1	1	0	0
0	1	1	0	0	0	1	1

Ciphertext for Round 1 → LE1 = F0AAF0AA

RE1= 5E1CEC63

Homework

Find the Ciphertext for the Plaintext below for the First Round by using Data Encryption Standard (DES).

P is: 0 1 3 2 4 A 6 7 F 9 A D C D E 1

K is: 1 A 2 D 4 6 E 7 8 9 A B C D A B