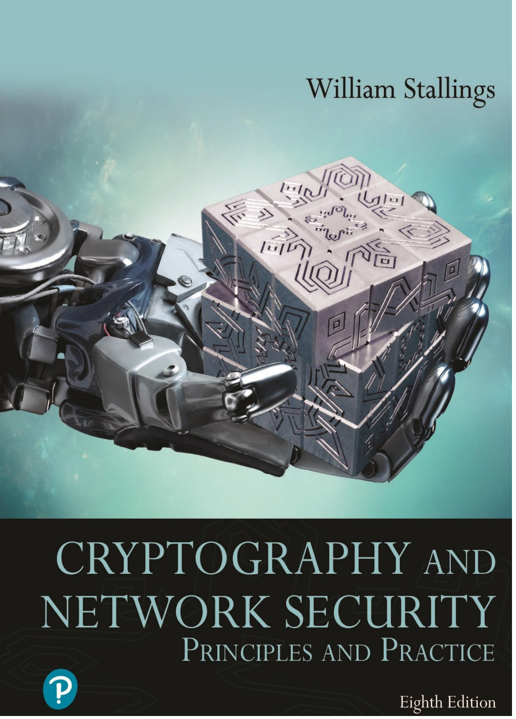


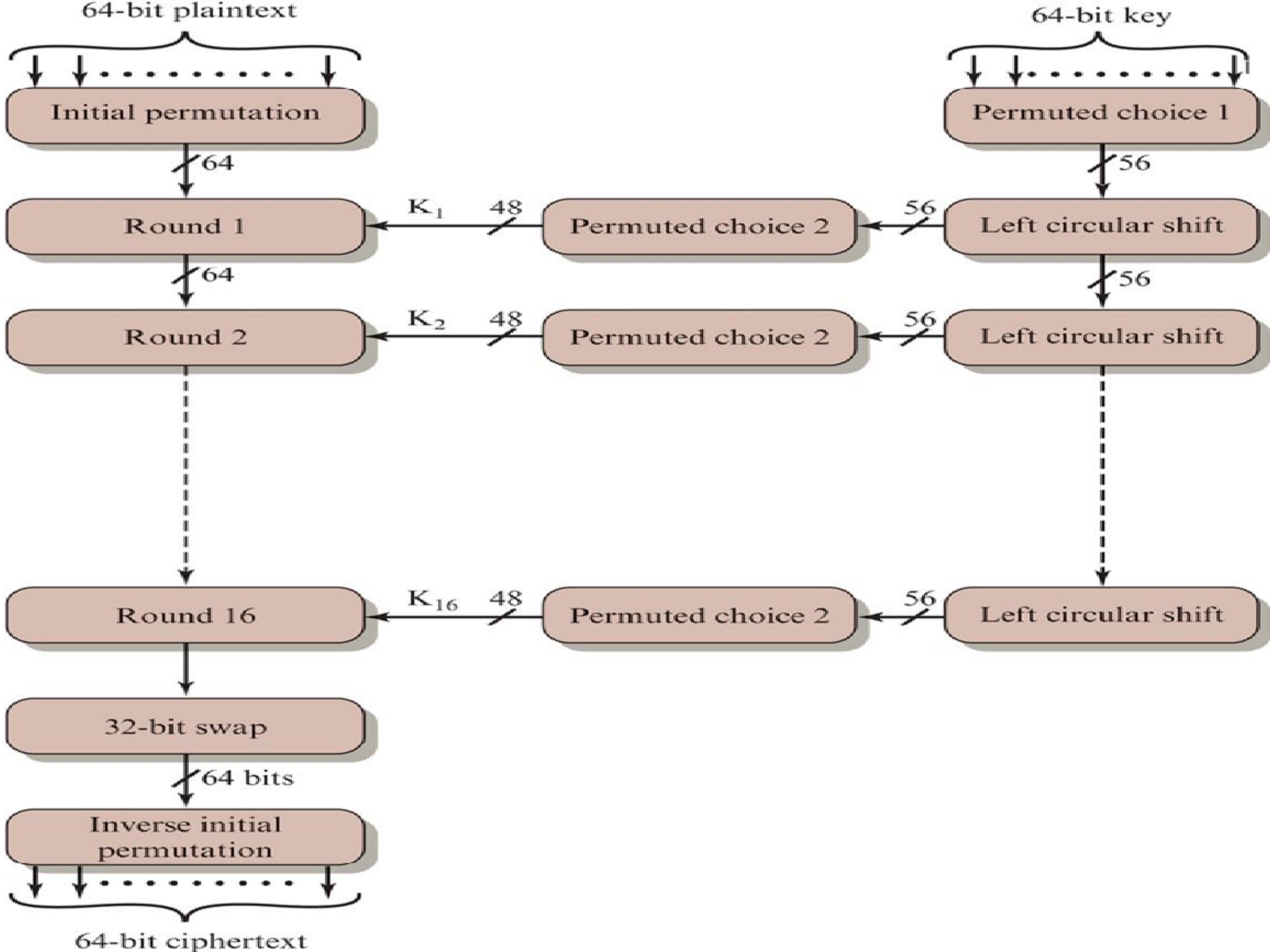
Cryptography and Network Security

Section 3

Chapter 4: Block Ciphers and the Data Encryption Standard

Syllabus

Lab	Lab Topics
1	Introduction
2	Classical Encryption techniques I
3	Classical Encryption techniques II
4	**DES**
5	block cipher operations & 3DES
6	AES
8	Public-Key Cryptography & RSA
9	Hash functions & SHA-512
10	User Authentication (Kerberos)
11	IEEE 802.11 Wireless LAN protocol

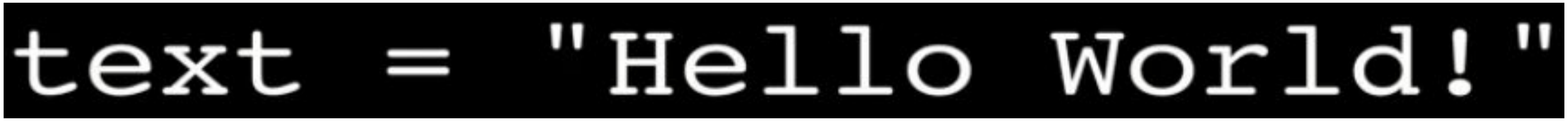

64-bit plaintext
64-bit key
Initial permutation
Permuted choice 1
64
56
K$_1$
48
Round 1
Permuted choice 2
56
Left circular shift
64
56
K$_2$
48
Round 2
Permuted choice 2
56
Left circular shift
K$_{16}$
48
Round 16
Permuted choice 2
56
Left circular shift
32-bit swap
64 bits
Inverse initial permutation
64-bit ciphertext

input 64 bit blocks

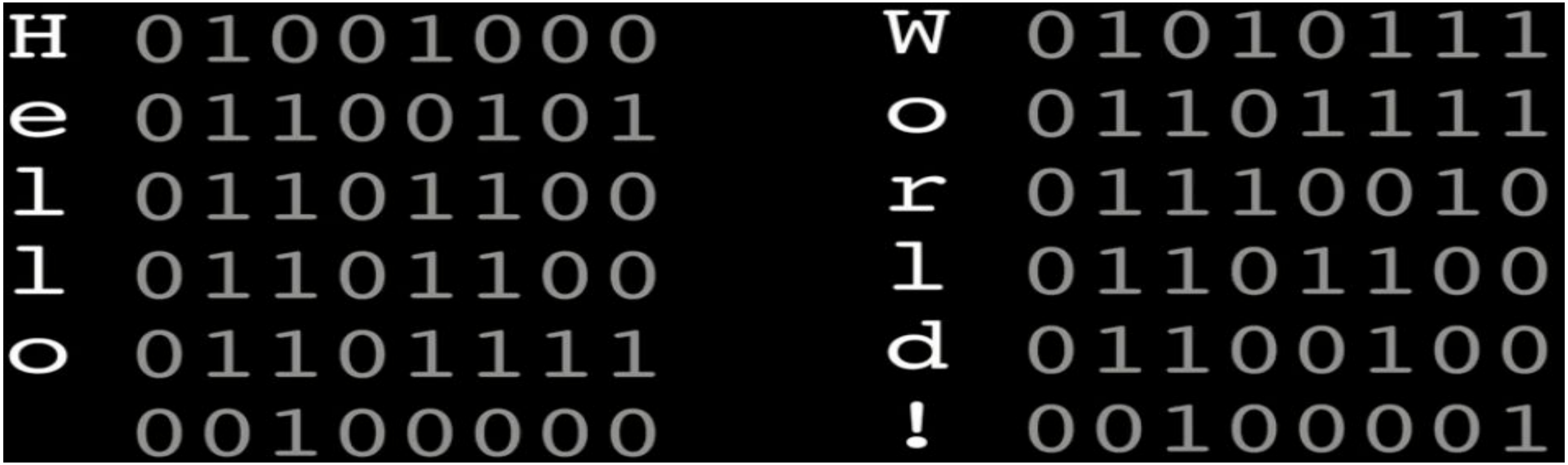
Step 1: Get Text

Step 2: Convert to Binary

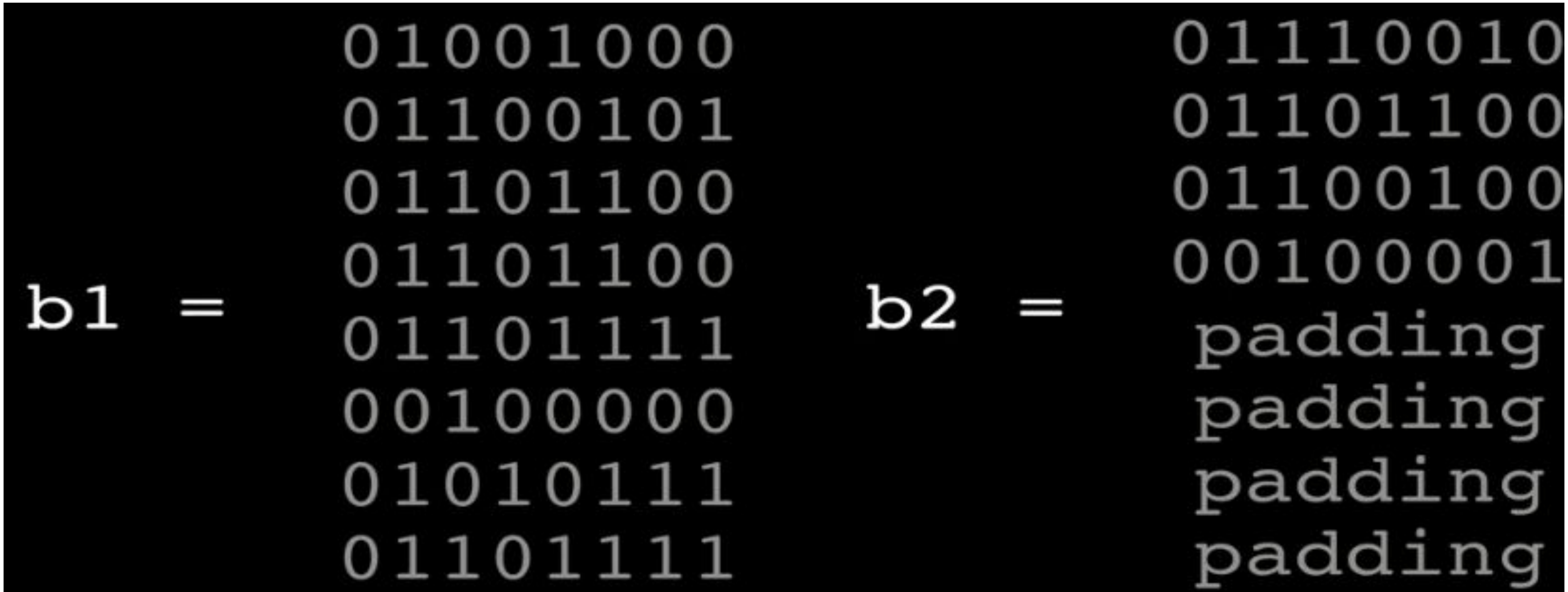
Step 3: Break into 64 bit blocks



```
text = "Hello World!"
```



```
H 01001000      W 01010111
e 01100101      o 01101111
l 01101100      r 01110010
l 01101100      l 01101100
o 01101111      d 01100100
  00100000      ! 00100001
```



```
         01001000              01110010
         01100101              01101100
         01101100              01100100
         01101100              00100001
b1 =     01101111      b2 =     padding
         00100000               padding
         01010111               padding
         01101111               padding
```

input → IP

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

input → IP

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

1	1						

input → IP

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

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

key → PC-1 = C and D

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

→

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

=

C

— — — — — — —
— — — — — — —
— — — — — — —
— — — — — — —

D

— — — — — — —
— — — — — — —
— — — — — — —
— — — — — — —

key → PC-1 = C and D

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

→

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

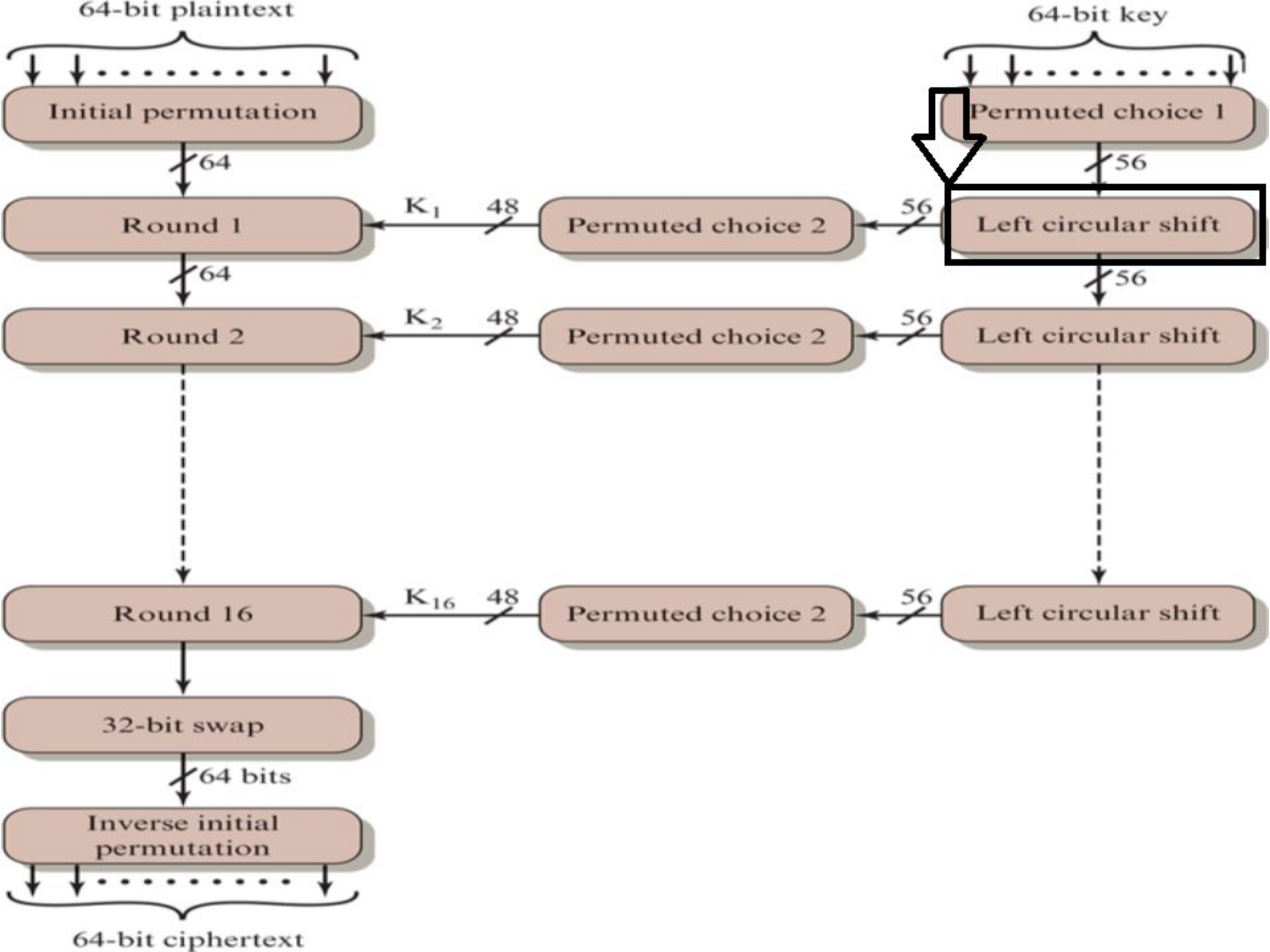
=

C

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

D

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


64-bit plaintext
64-bit key
Initial permutation
Permuted choice 1
64
56
K1
48
Round 1
Permuted choice 2
56
Left circular shift
64
56
K2
48
Round 2
Permuted choice 2
56
Left circular shift
K16
48
Round 16
Permuted choice 2
56
Left circular shift
32-bit swap
64 bits
Inverse initial permutation
64-bit ciphertext

Round 1: C

```
0 1 1 0 1 1 0
0 0 0 1 0 0 0
0 0 0 0 0 0 1
1 1 1 0 1 1 1
```

D

```
0 0 1 0 0 0 0
0 1 0 0 1 0 1
1 1 0 0 1 1 1
0 1 0 0 1 0 1
```

1. Left Circular Shift

R#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
# shifts	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

C

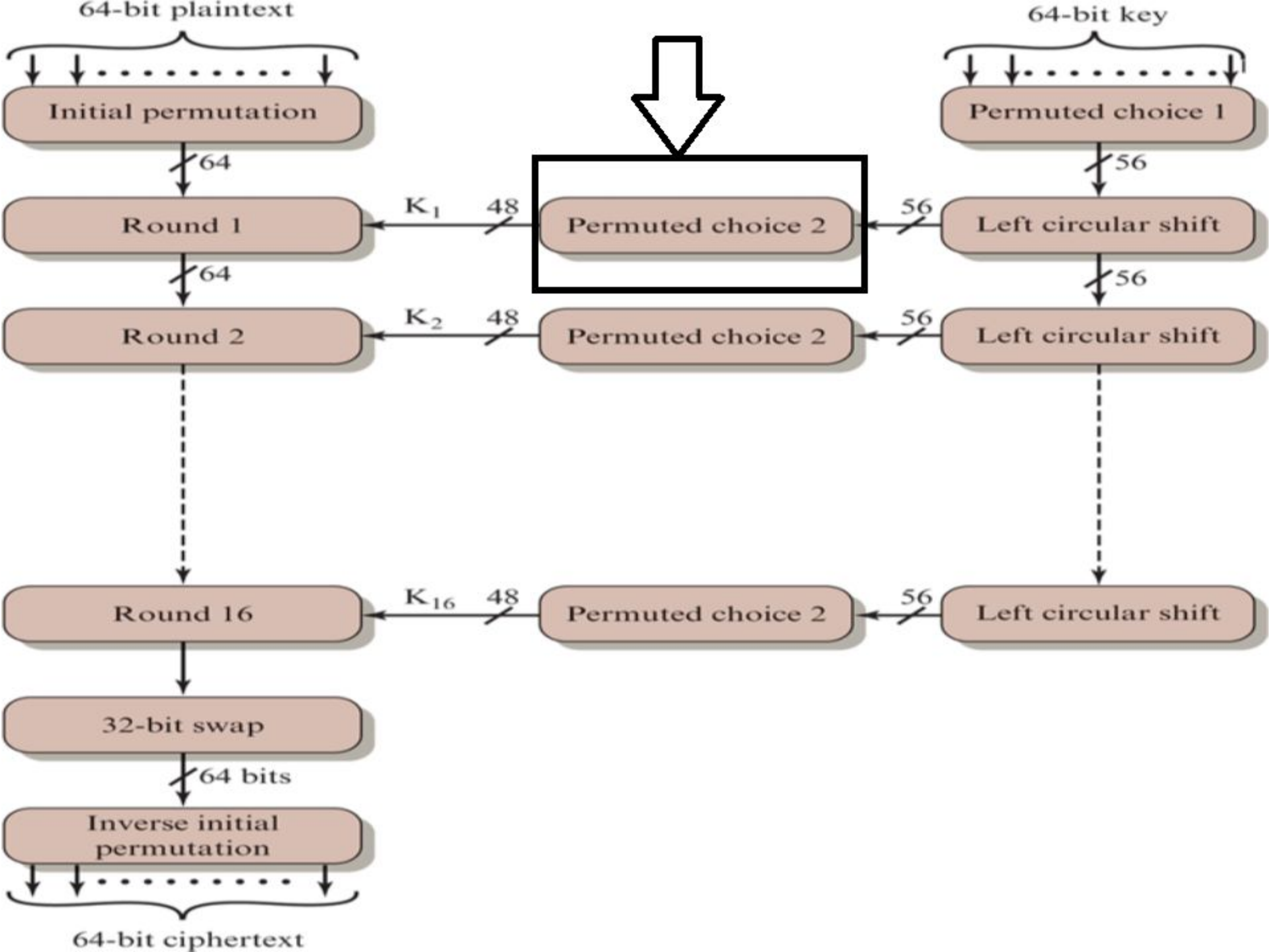
```
0 1 1 0 1 1 0        1 1 0 1 1 0 0
0 0 0 1 0 0 0   →    0 0 1 0 0 0 0
0 0 0 0 0 0 1        0 0 0 0 0 1 1
1 1 1 0 1 1 1        1 1 0 1 1 1 0
```

C_s

D

```
0 0 1 0 0 0 0        0 1 0 0 0 0 0
0 1 0 0 1 0 1   →    1 0 0 1 0 1 1
1 1 0 0 1 1 1        1 0 0 1 1 1 0
0 1 0 0 1 0 1        1 0 0 1 0 1 0
```

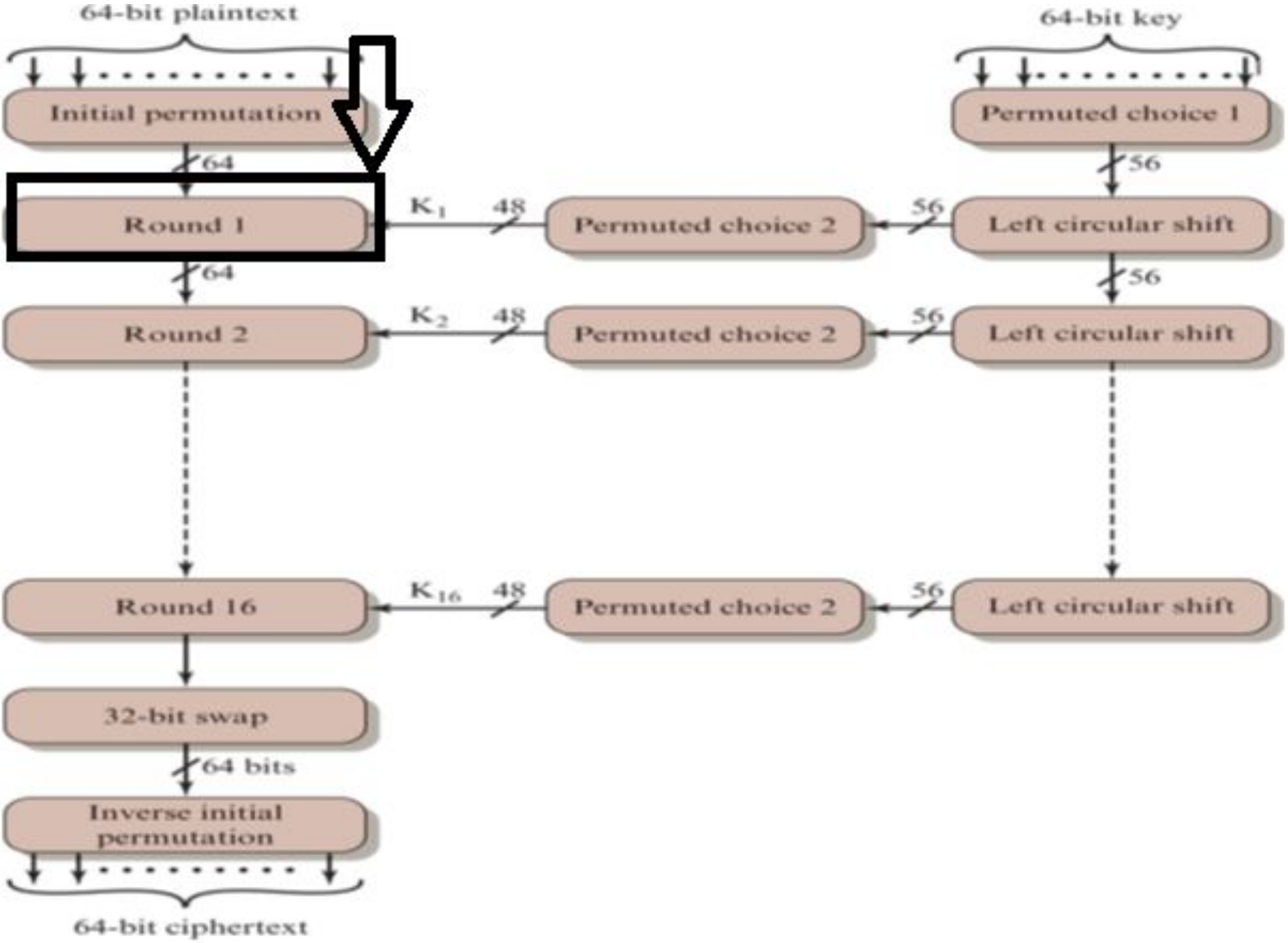
D_s


64-bit plaintext
64-bit key
Initial permutation
Permuted choice 1
64
56
K₁
48
Round 1
Permuted choice 2
56
Left circular shift
64
56
K₂
48
Round 2
Permuted choice 2
56
Left circular shift
K₁₆
48
Round 16
Permuted choice 2
56
Left circular shift
32-bit swap
64 bits
Inverse initial permutation
64-bit ciphertext

Round 1: $C_s \begin{matrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{matrix} \quad D_s \begin{matrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{matrix}$

2. PC-2

$$\begin{matrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{matrix} \rightarrow \begin{matrix} 14 & 17 & 11 & 24 & 1 & 5 \\ 3 & 28 & 15 & 6 & 21 & 10 \\ 23 & 19 & 12 & 4 & 26 & 8 \\ 16 & 7 & 27 & 20 & 13 & 2 \\ 41 & 52 & 31 & 37 & 47 & 55 \\ 30 & 40 & 51 & 45 & 33 & 48 \\ 44 & 49 & 39 & 56 & 34 & 53 \\ 46 & 42 & 50 & 36 & 29 & 32 \end{matrix} = \begin{matrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{matrix}$$


64-bit plaintext
Initial permutation
64
Round 1
K1
48
Permuted choice 2
56
Left circular shift
64
Round 2
K2
48
Permuted choice 2
56
Left circular shift
Round 16
K16
48
Permuted choice 2
56
Left circular shift
32-bit swap
64 bits
Inverse initial permutation
64-bit ciphertext
64-bit key
Permuted choice 1
56
56

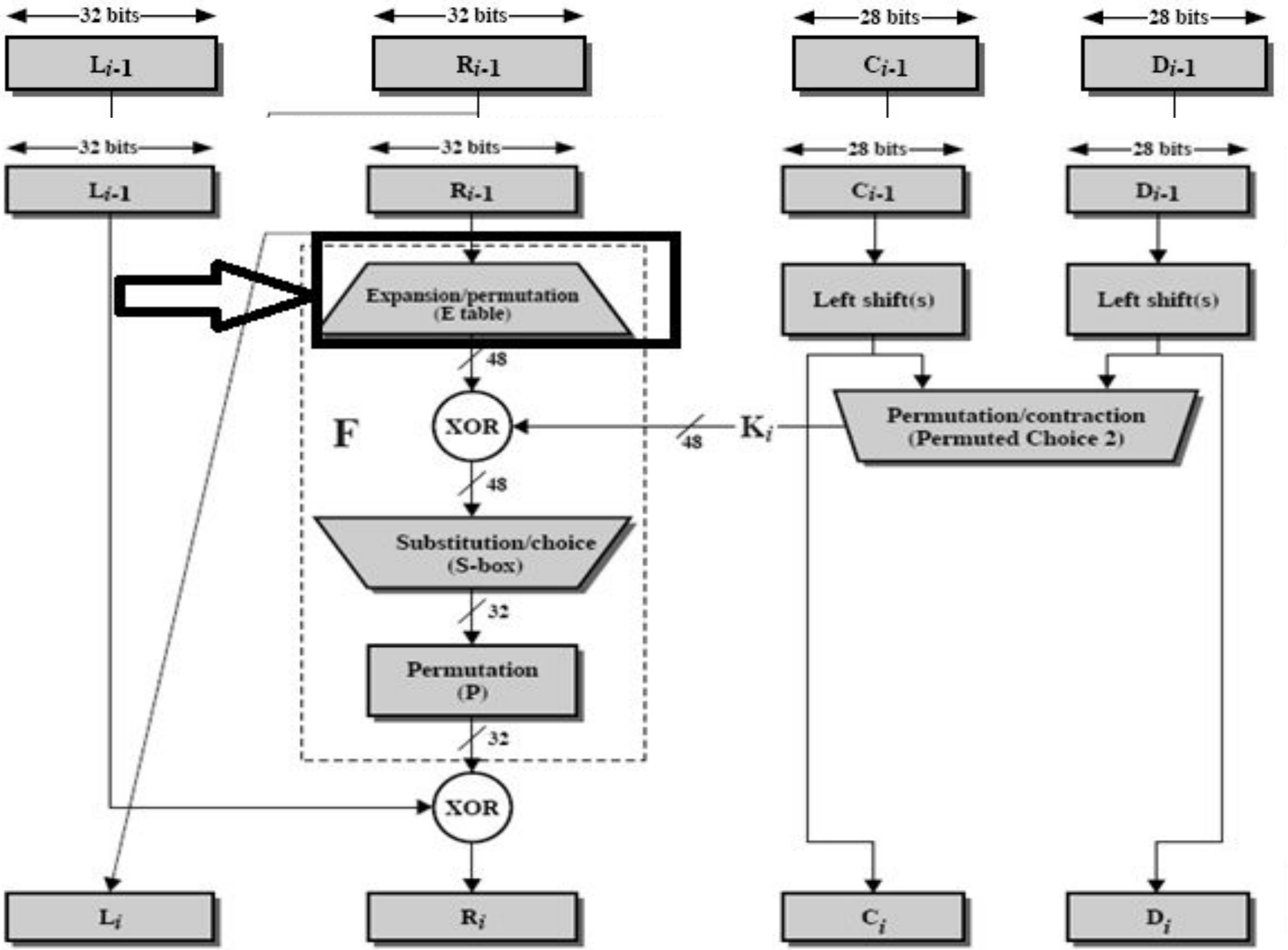


Figure 3.8 Single Round of DES Algorithm

E-bit Selection Table

2nd half input:

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

→

selection 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

=

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

48 bits

Input Key

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{matrix} \oplus \begin{matrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{matrix} = \begin{matrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{matrix}$$

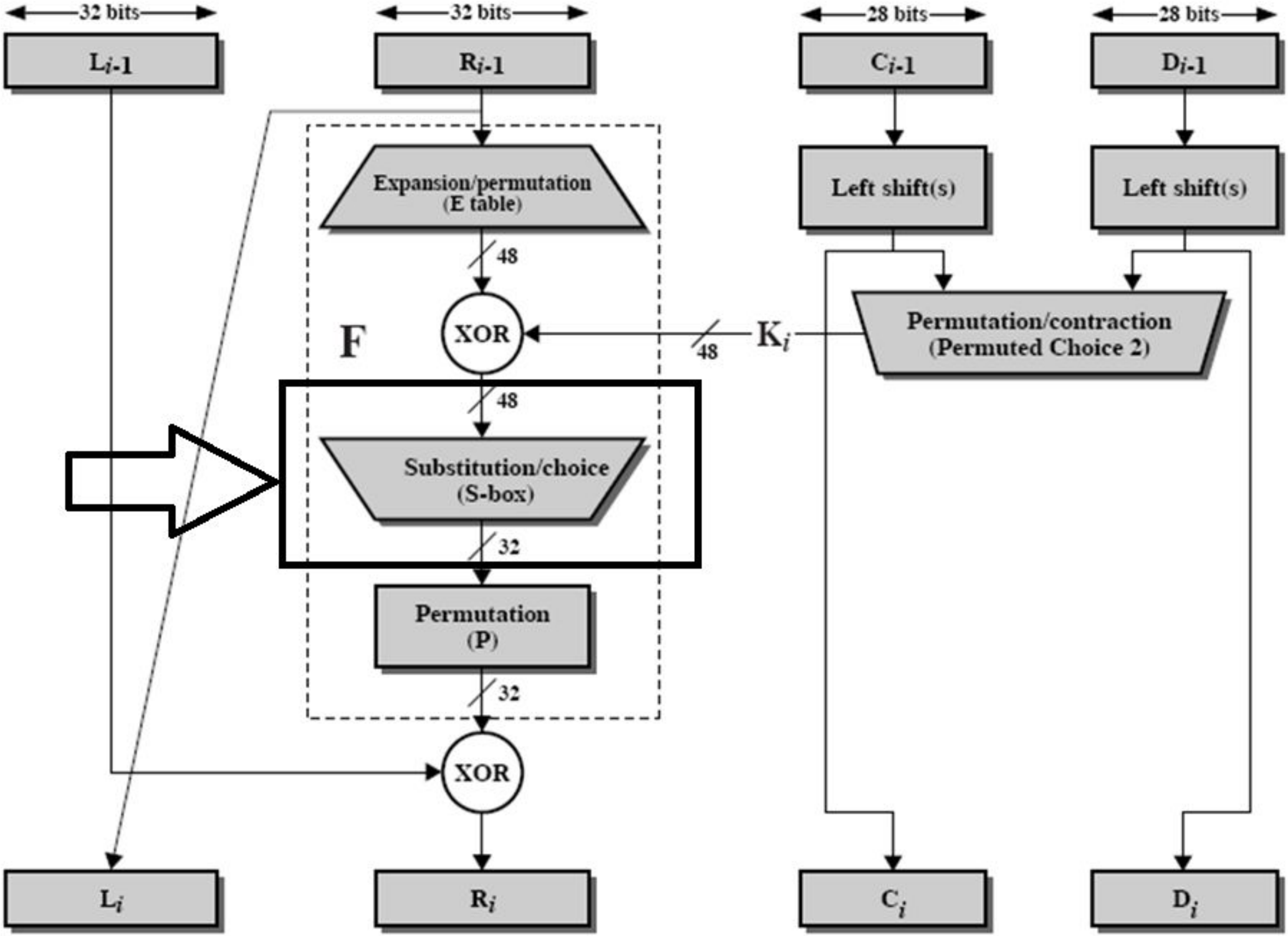
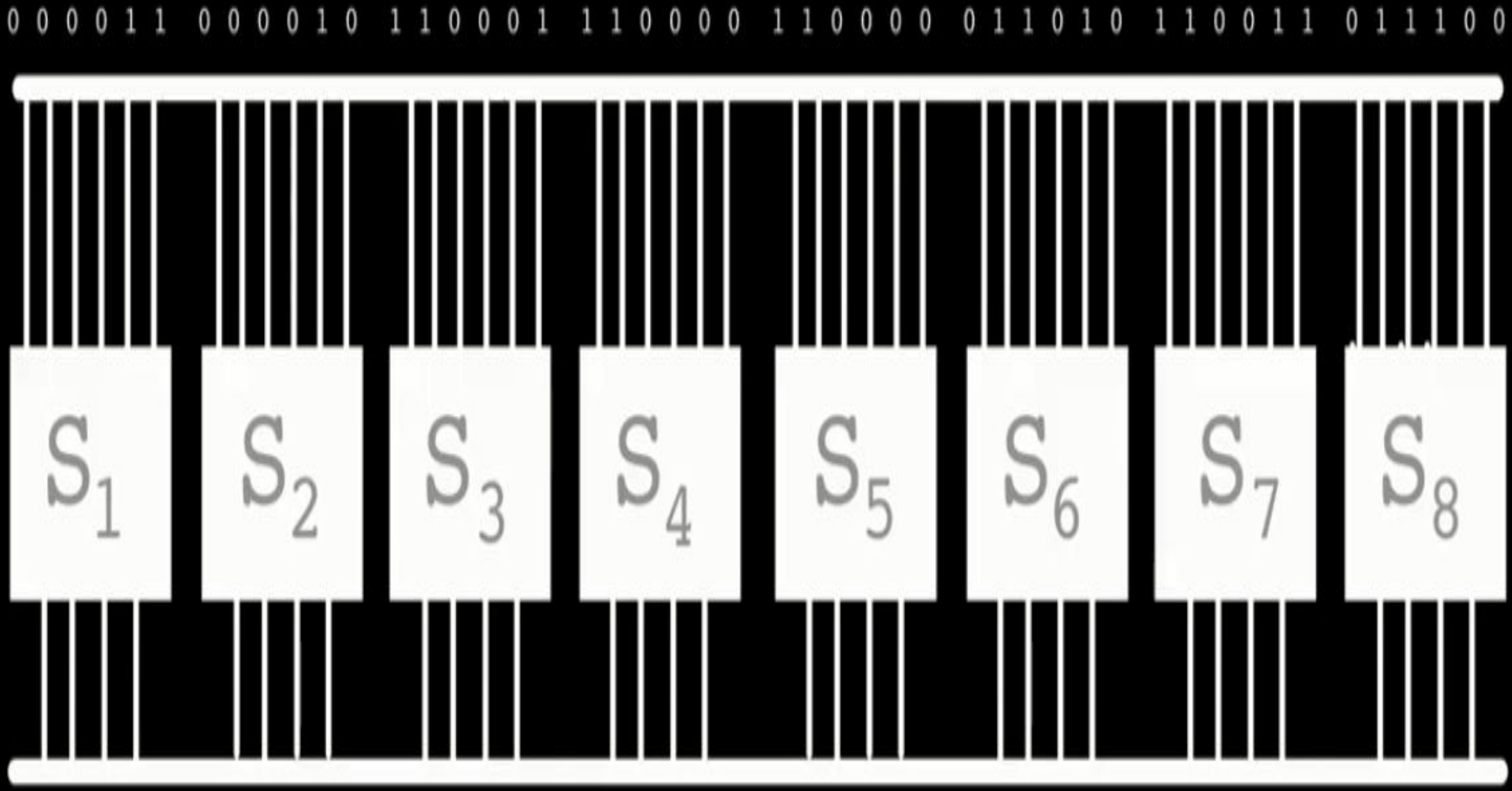


Figure 3.8 Single Round of DES Algorithm

S-boxes


000011 000010 110001 110000 110000 011010 110011 011100
S_1
S_2
S_3
S_4
S_5
S_6
S_7
S_8

The S-box: S_1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

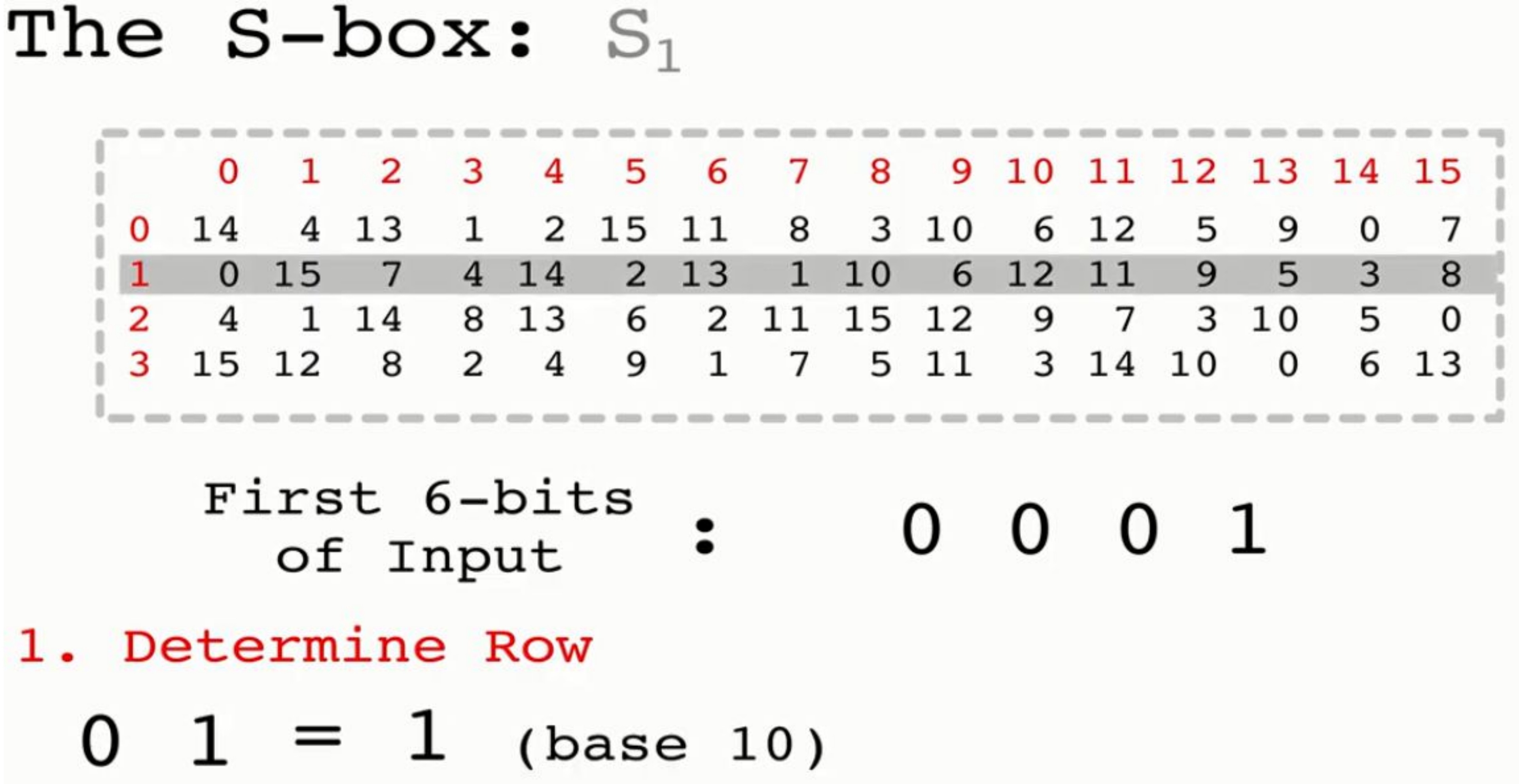
First 6-bits of Input : 0 0 0 0 1 1

The S-box: S_1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

First 6-bits of Input : $\boxed{0}$ 0 0 0 1 $\boxed{1}$

1. Determine Row



The S-box: S_1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

First 6-bits of Input : 0 0 0 1

1. Determine Row

0 1 = 1 (base 10)

The S-box: S_1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

First 6-bits of Input : 0 0 0 1

1. Determine Row

0 1 = 1 (base 10)

2. Determine Column

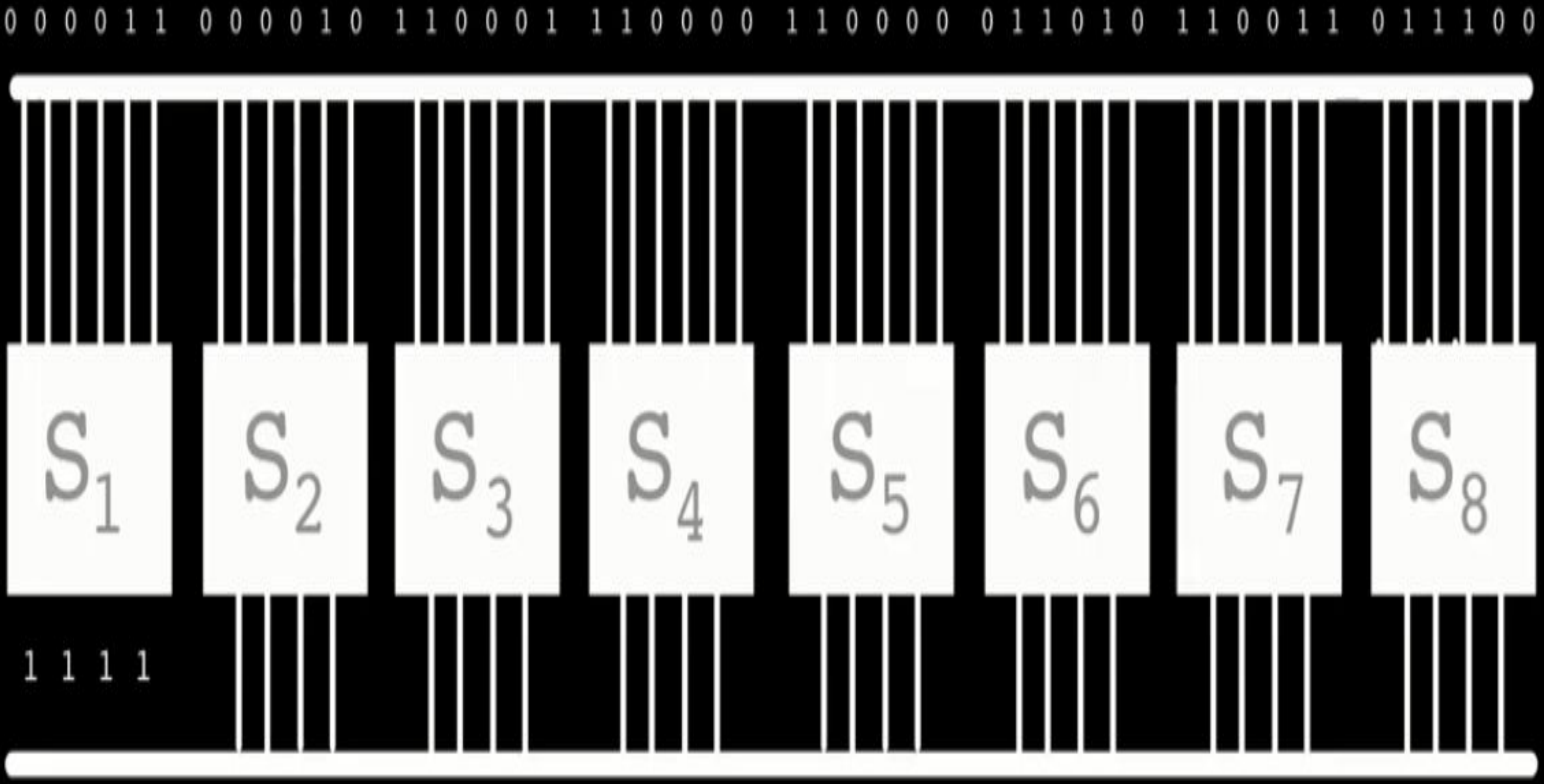
0 0 0 1 = 1 (base 10)

Output = 15

Convert Output to Binary

15 = 1 1 1 1

S-boxes


0 0 0 0 1 1
0 0 0 0 1 0
1 1 0 0 0 1
1 1 0 0 0 0
1 1 0 0 0 0
0 1 1 0 1 0
1 1 0 0 1 1
0 1 1 1 0 0
S_1
S_2
S_3
S_4
S_5
S_6
S_7
S_8
1 1 1 1

The S-box: S_2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

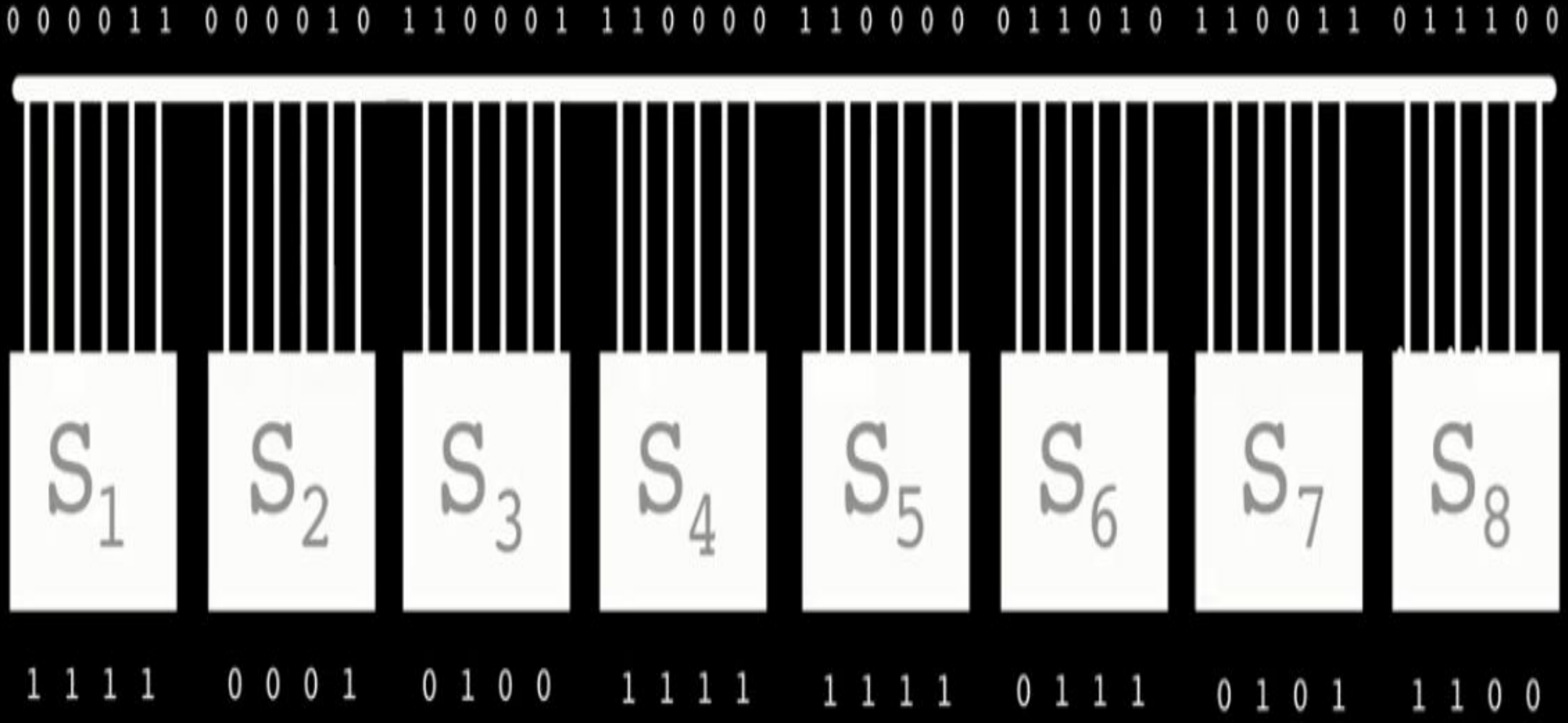
Input : 0 0 0 0 1 0

Row : 0 0 = 0

Column : 0 0 0 1 = 1

Output : 1 = 0 0 0 1

S-boxes


0 0 0 0 1 1
0 0 0 0 1 0
1 1 0 0 0 1
1 1 0 0 0 0
1 1 0 0 0 0
0 1 1 0 1 0
1 1 0 0 1 1
0 1 1 1 0 0
S_1
S_2
S_3
S_4
S_5
S_6
S_7
S_8
1 1 1 1
0 0 0 1
0 1 0 0
1 1 1 1
1 1 1 1
0 1 1 1
0 1 0 1
1 1 0 0

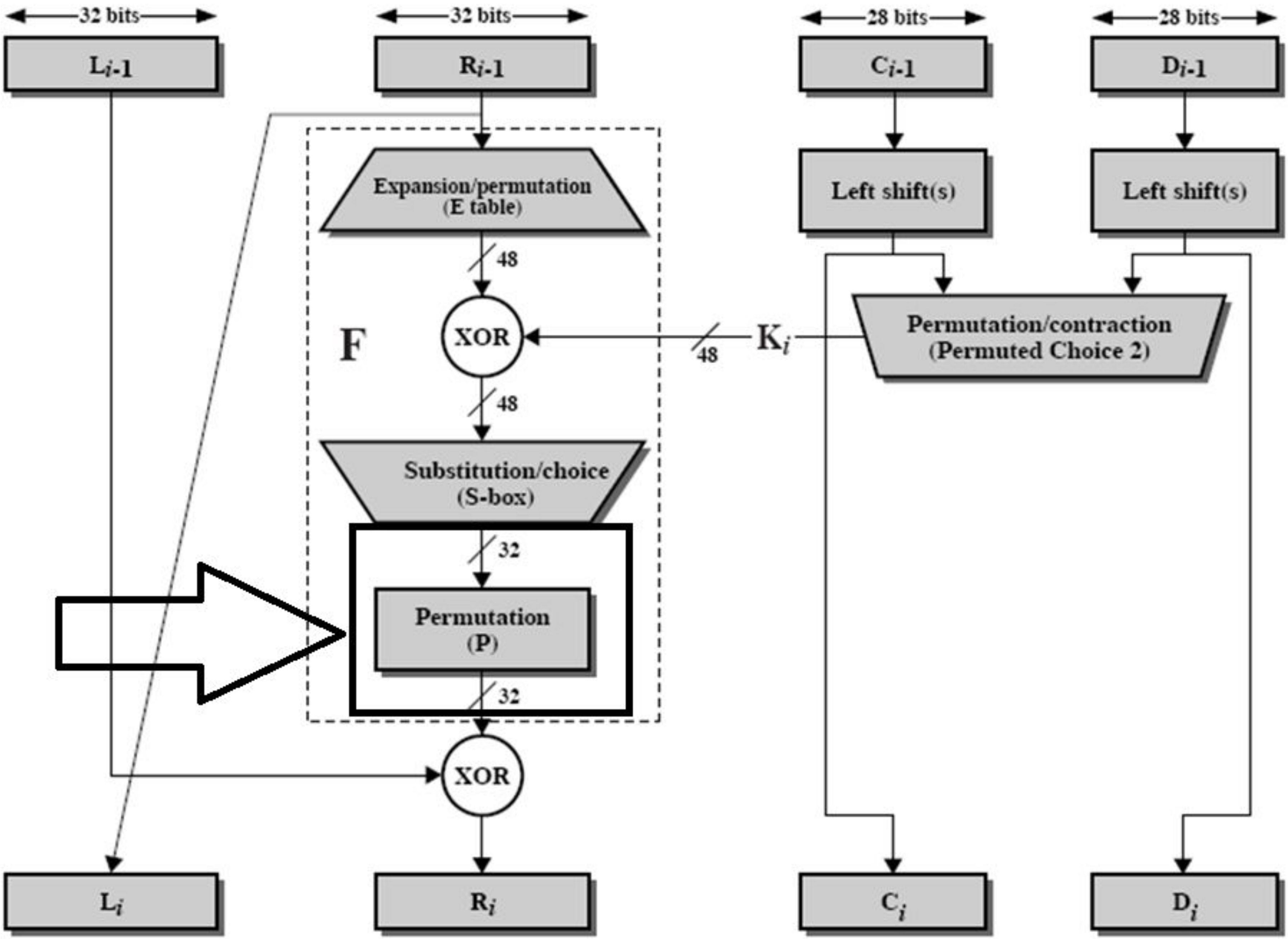
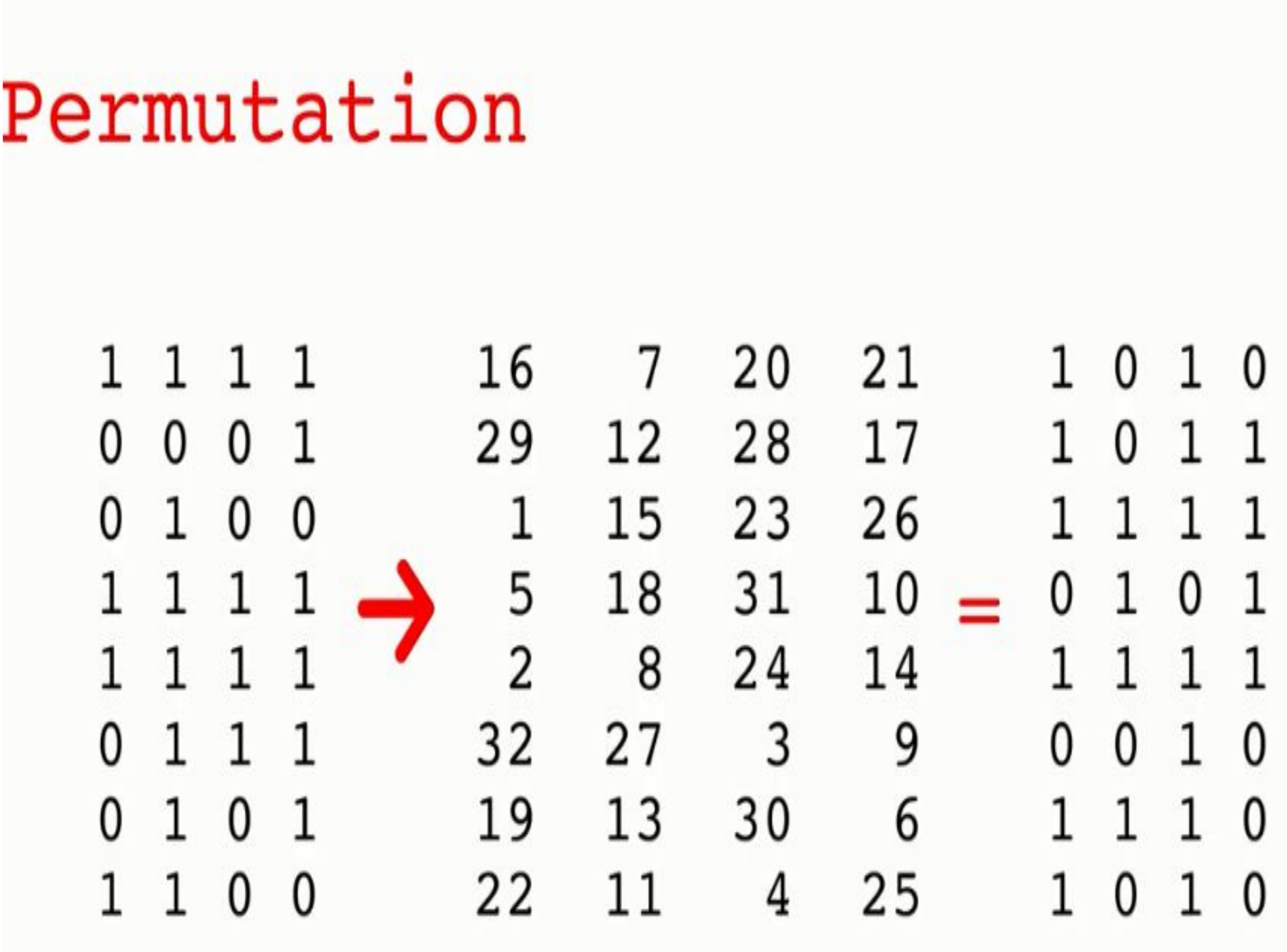


Figure 3.8 Single Round of DES Algorithm



Permutation

$$\begin{matrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{matrix} \rightarrow \begin{matrix} 16 & 7 & 20 & 21 \\ 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 \\ 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 \\ 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 \\ 22 & 11 & 4 & 25 \end{matrix} = \begin{matrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{matrix}$$

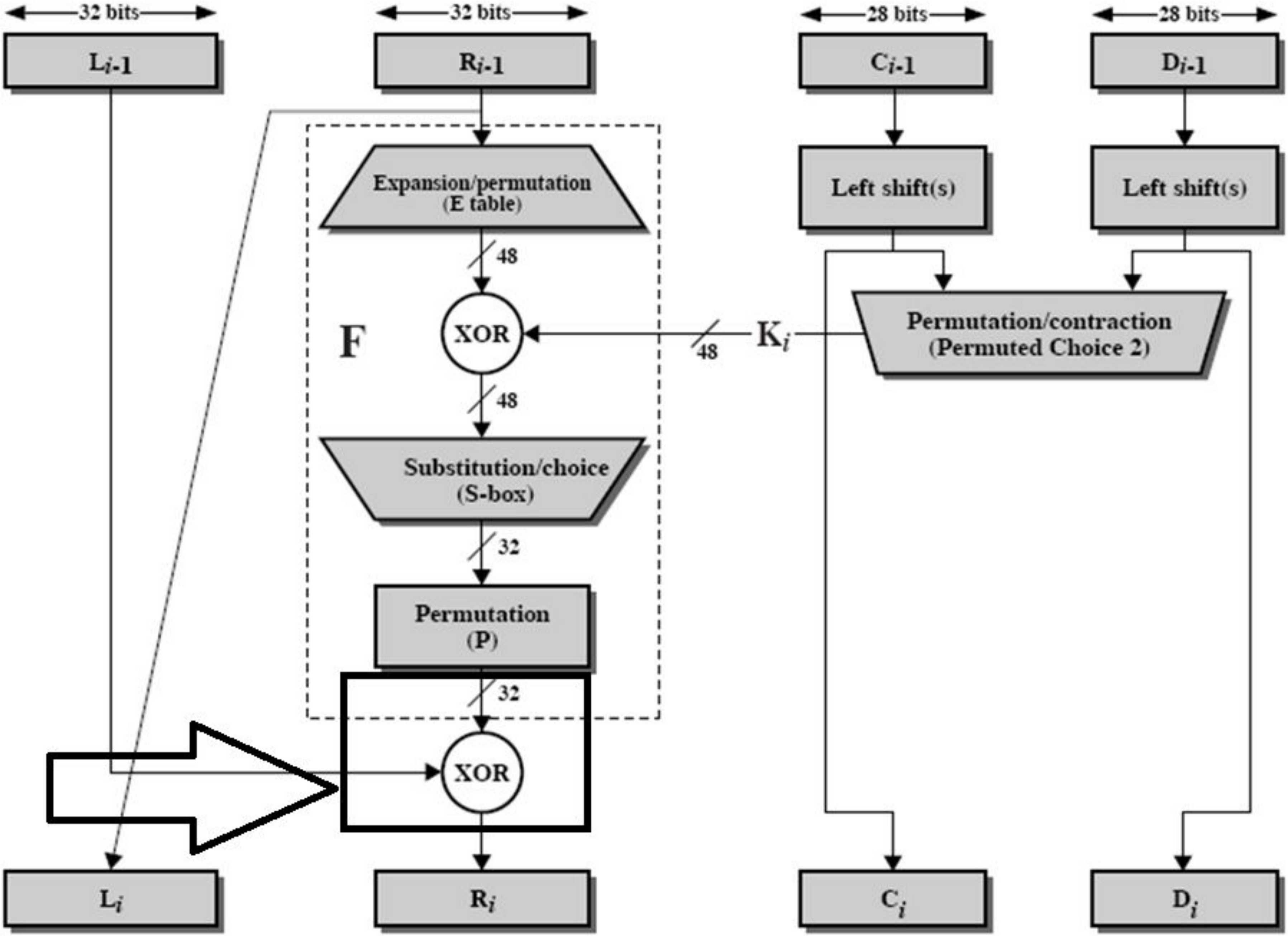
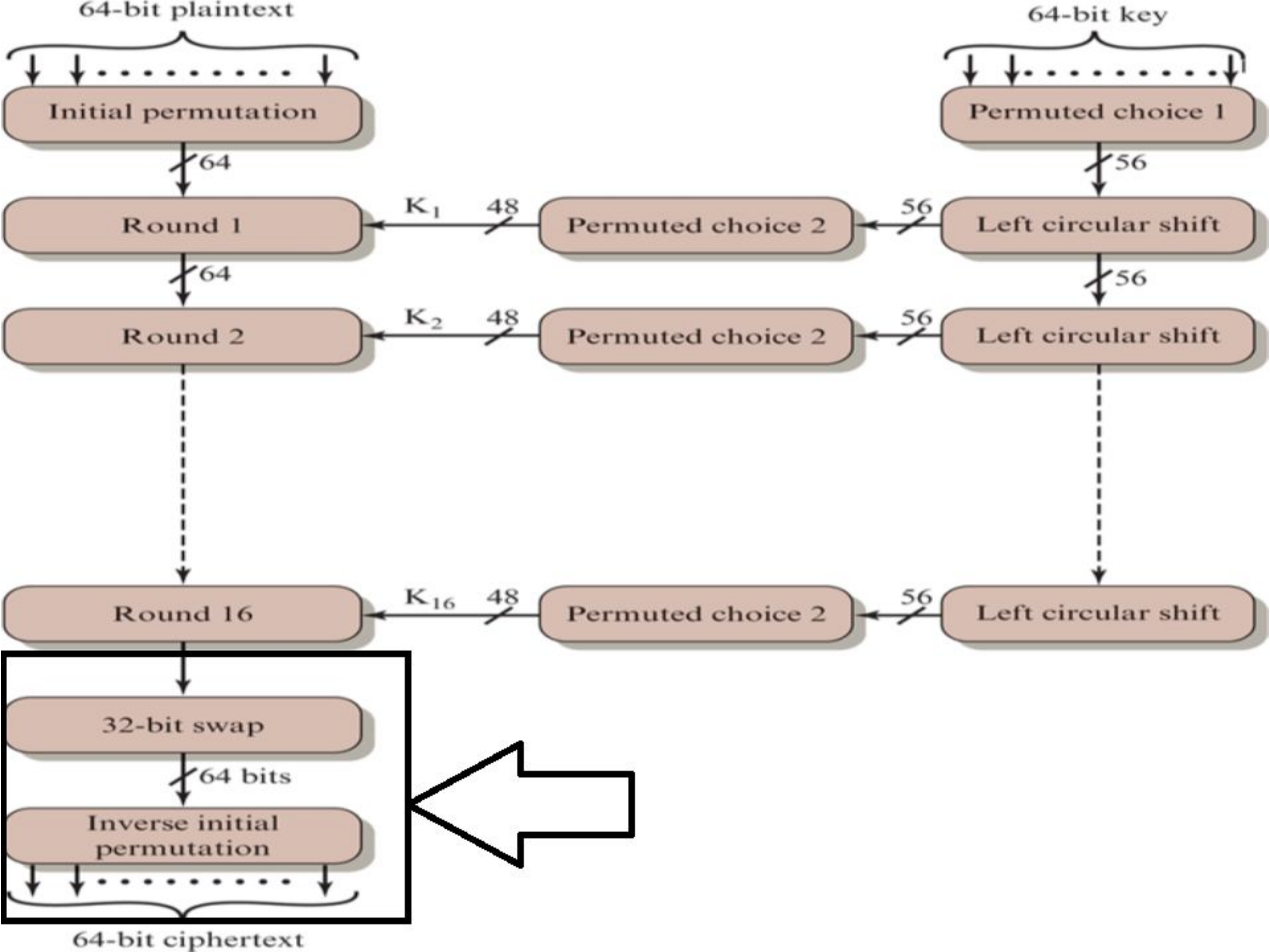
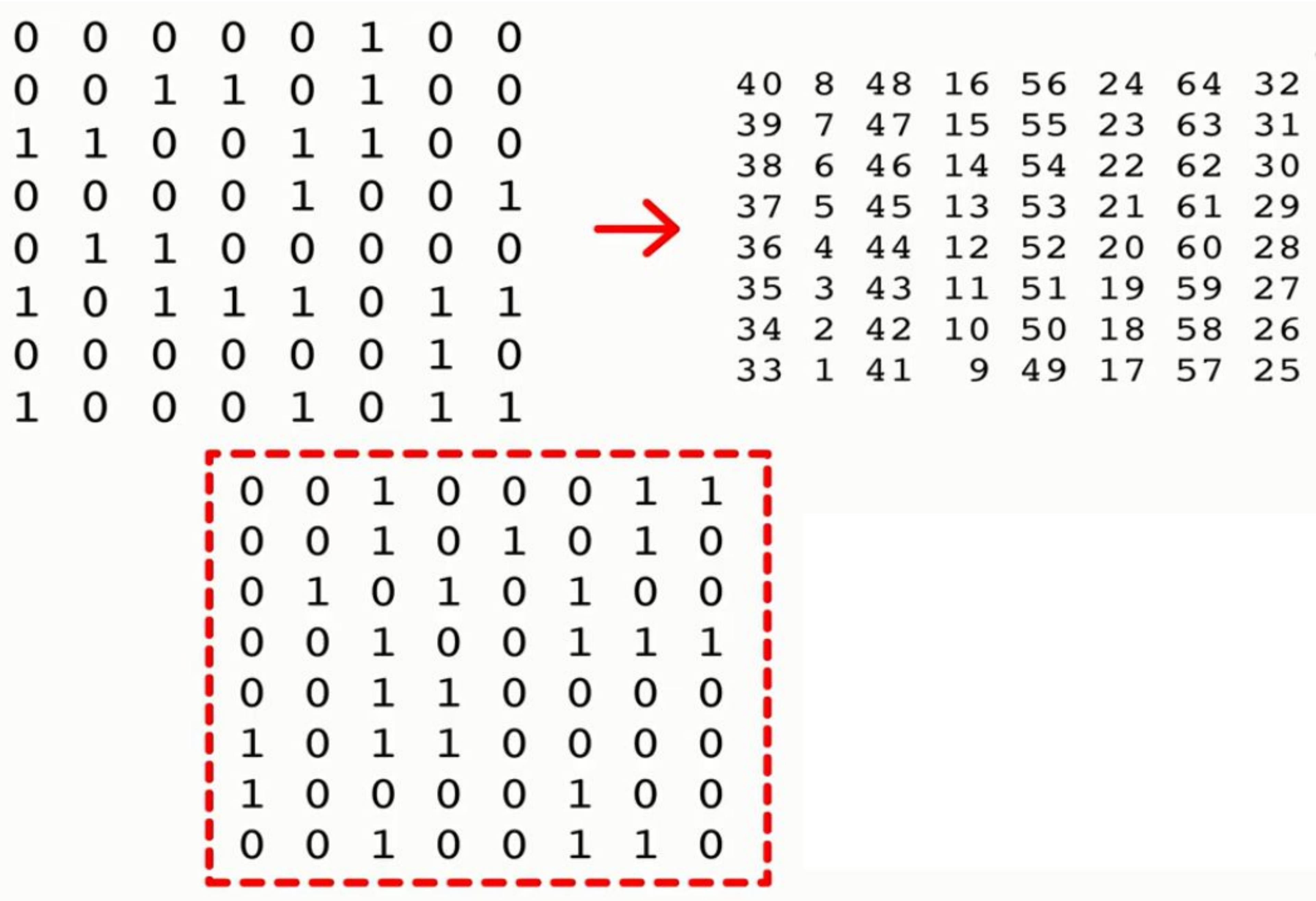


Figure 3.8 Single Round of DES Algorithm


64-bit plaintext
64-bit key
Initial permutation
Permuted choice 1
64
56
Round 1
K1
48
Permuted choice 2
56
Left circular shift
64
56
Round 2
K2
48
Permuted choice 2
56
Left circular shift
Round 16
K16
48
Permuted choice 2
56
Left circular shift
32-bit swap
64 bits
Inverse initial permutation
64-bit ciphertext

32- bit swap then inverse initial permutation

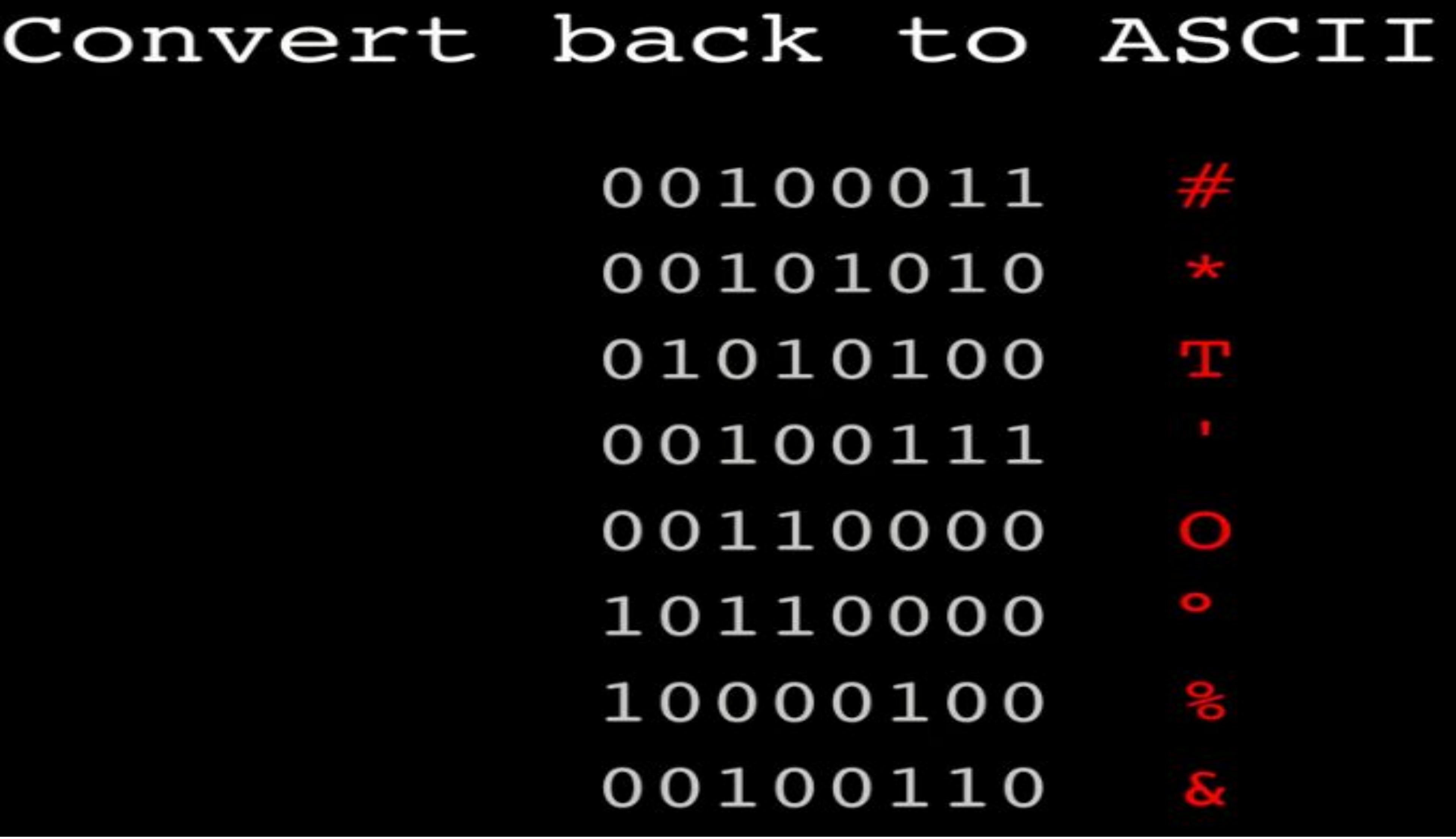


0	0	0	0	0	1	0	0
0	0	1	1	0	1	0	0
1	1	0	0	1	1	0	0
0	0	0	0	1	0	0	1
0	1	1	0	0	0	0	0
1	0	1	1	1	0	1	1
0	0	0	0	0	0	1	0
1	0	0	0	1	0	1	1

→

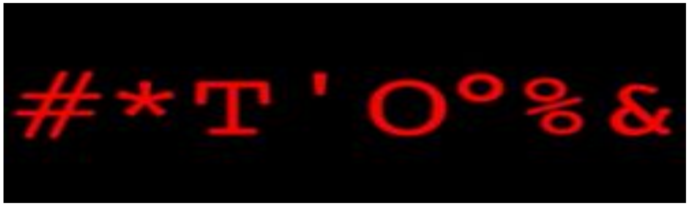
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

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



Convert back to ASCII

00100011	#
00101010	*
01010100	T
00100111	'
00110000	0
10110000	°
10000100	%
00100110	&

Cipher text = 

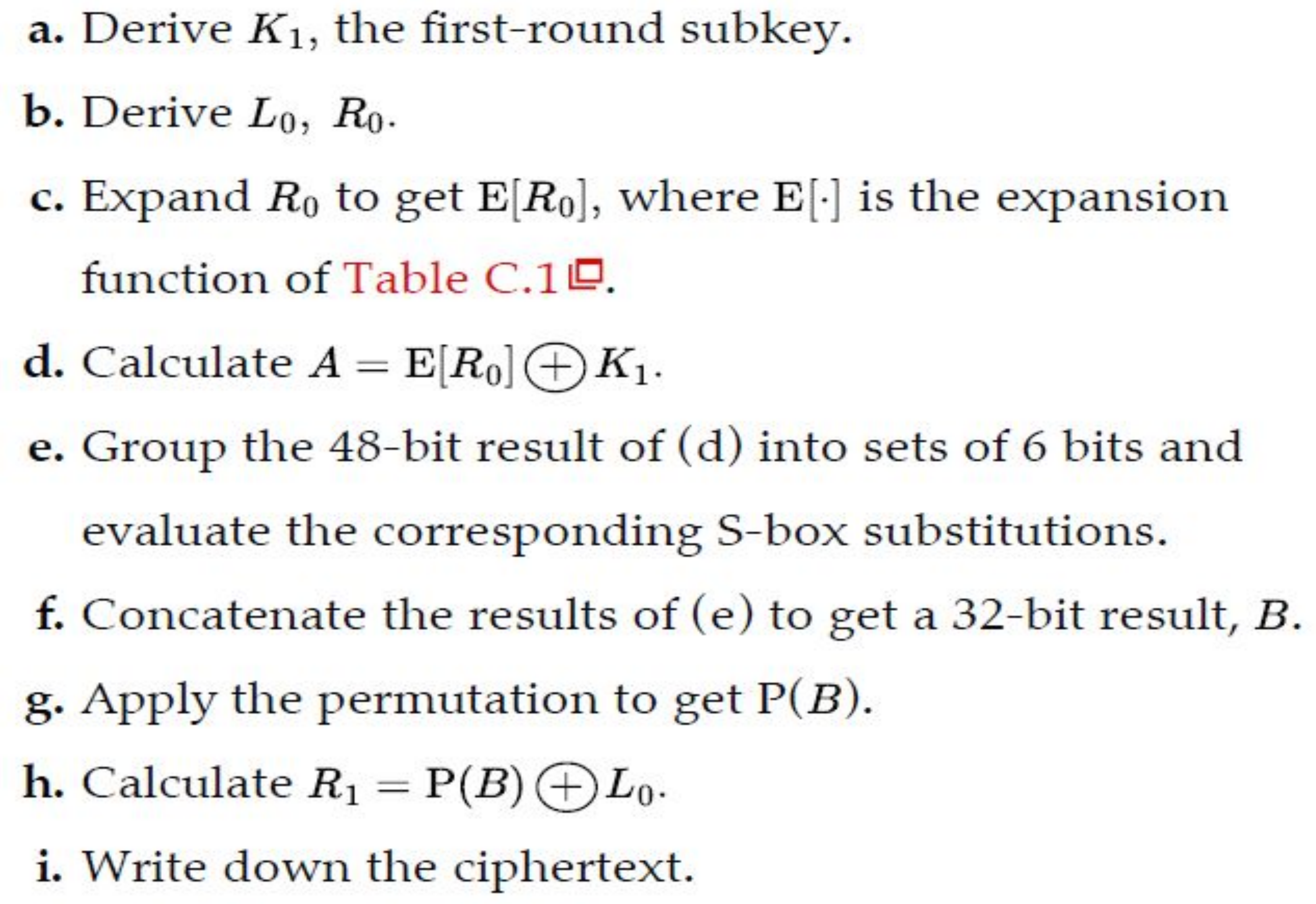
#*T'0°%&

Sheet problem

This problem provides a numerical example of encryption using a one-round version of DES. We start with the same bit pattern for the key *K* and the plaintext, namely:

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

Sheet problem(Cont.)



a. Derive K_1, the first-round subkey.

b. Derive L_0, R_0.

c. Expand R_0 to get $\mathrm{E}[R_0]$, where $\mathrm{E}[\cdot]$ is the expansion function of Table C.1.

d. Calculate $A = \mathrm{E}[R_0] \bigoplus K_1$.

e. Group the 48-bit result of (d) into sets of 6 bits and evaluate the corresponding S-box substitutions.

f. Concatenate the results of (e) to get a 32-bit result, B.

g. Apply the permutation to get $\mathrm{P}(B)$.

h. Calculate $R_1 = \mathrm{P}(B) \bigoplus L_0$.

i. Write down the ciphertext.

THANK YOU