11464: INFORMATION SYSTEMS SECURITY

12/5/2021

Chapter 4-2: Simplified – Data Encryption Standard

2

Data Encryption Standard

By

Mustafa Al-Fayoumi

3 Simplified – Data Encryption Standard

S-DES

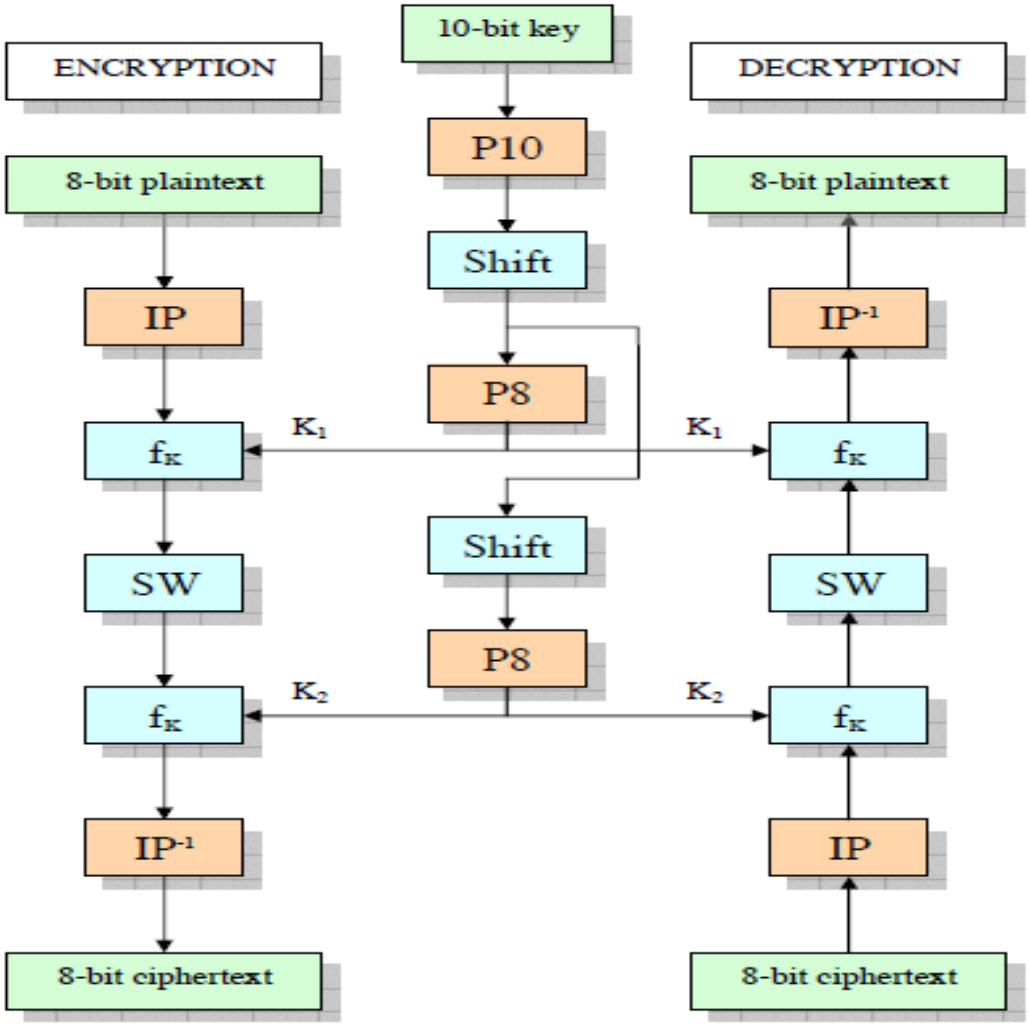
Simplified DES (S-DES)

- Cipher using principles of DES
- Developed for education (not real world use)
- Input (plaintext) block : 8-bits
- Output (ciphertext) block : 8-bits
- Key: 10 bits
- Round: 2
- Round keys generated using permutations and left shifts
- Encryption: Initial permutation, Round function, Switch halves.
- Decryption: Same as encryption, except round key used in opposite order

From DES to S-DES key

- From DES to S-DES key
  - S-DES
    - 10-bit key is used
    - From which two 8-bit keys are calculated
  - DES
    - 56-bit key is used
    - From which 16 -48-bit keys are calculated

S-DES Algorithm



S-DES Operations

- P10 (permutate)

Input:

1	2	3	4	5	6	7	8	9	10

Output:

3	5	2	7	4	10	1	9	8	6

- P8 (select and permutate)

Input:

1	2	3	4	5	6	7	8	9	10

Output:

6	3	7	4	8	5	10	9

- P4 (permutate)

Input:

1	2	3	4

Output:

2	4	3	1

S-DES Operations

- EP (Expand and permutate)

Input:

1	2	3	4

Output:

4	1	2	3	2	3	4	1

- IP (Initial permutate)

Input:

1	2	3	4	5	6	7	8

Output:

2	6	3	1	4	8	5	7

- IP^{-1} (Inverse pf IP)

Input:

1	2	3	4	5	6	7	8

Output:

4	1	3	5	7	2	8	6

S-DES Operations

- LS-1 (Left Shift 1 Position)

Input:	1	2	3	4	5	6	7	8	9	10
Output:	2	3	4	5	1	7	8	9	10	6

- LS-2 (Left Shift 2 Position)

Input:	1	2	3	4	5	6	7	8	9	10
Output:	3	4	5	1	2	8	9	10	6	7

S-DES

- DES = Data Encryption Standard.
  - Two Phases:
    - Key Generation. 10-bit key
    - Encryption / Decryption. 8-bit block.

Sub- Key Generation

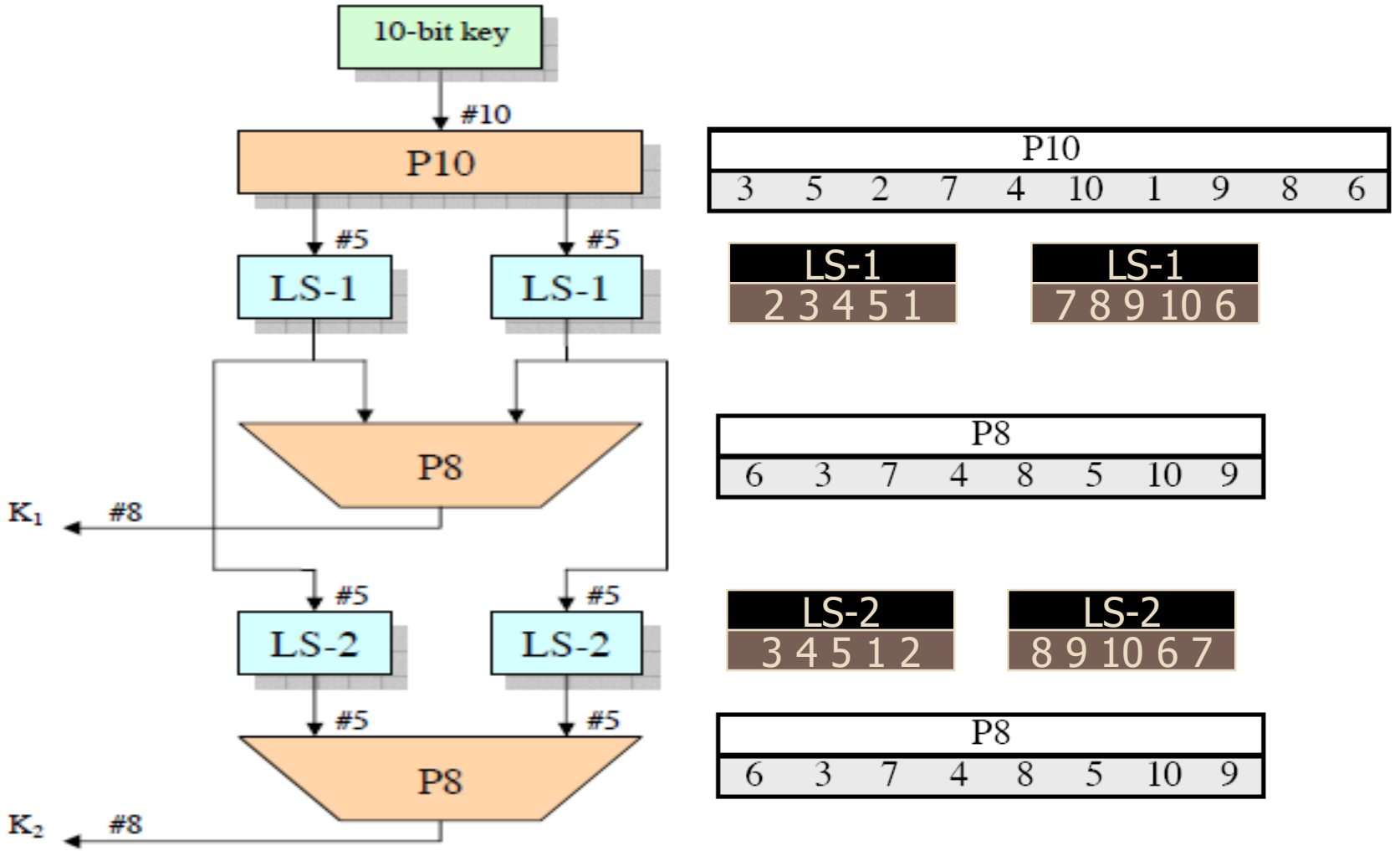


Figure 2: Key Generation for Simplified DES.

Sub- Key Generation

- Apply the P10 operation on the 10 bit input
- Apply LS-1 (left shift 1) to each 5-bit group
- Apply permutation P8 $\rightarrow$ K1
- Apply LS-2 (left shift 2) to each 5-bit group.
- Apply permutation P8 $\rightarrow$ K2.

S-DES KG Example

Assume given a key to be:

K = 1010000010

Step (1):P10 → 10000 | 01100

Step (2): LS-1 → 00001 | 11000

Step (3): Apply permutation *P8*

P10									
3	5	2	7	4	10	1	9	8	6

LS-1					LS-1				
2	3	4	5	1	7	8	9	10	6

P8							
6	3	7	4	8	5	10	9

then K1 = 10100100

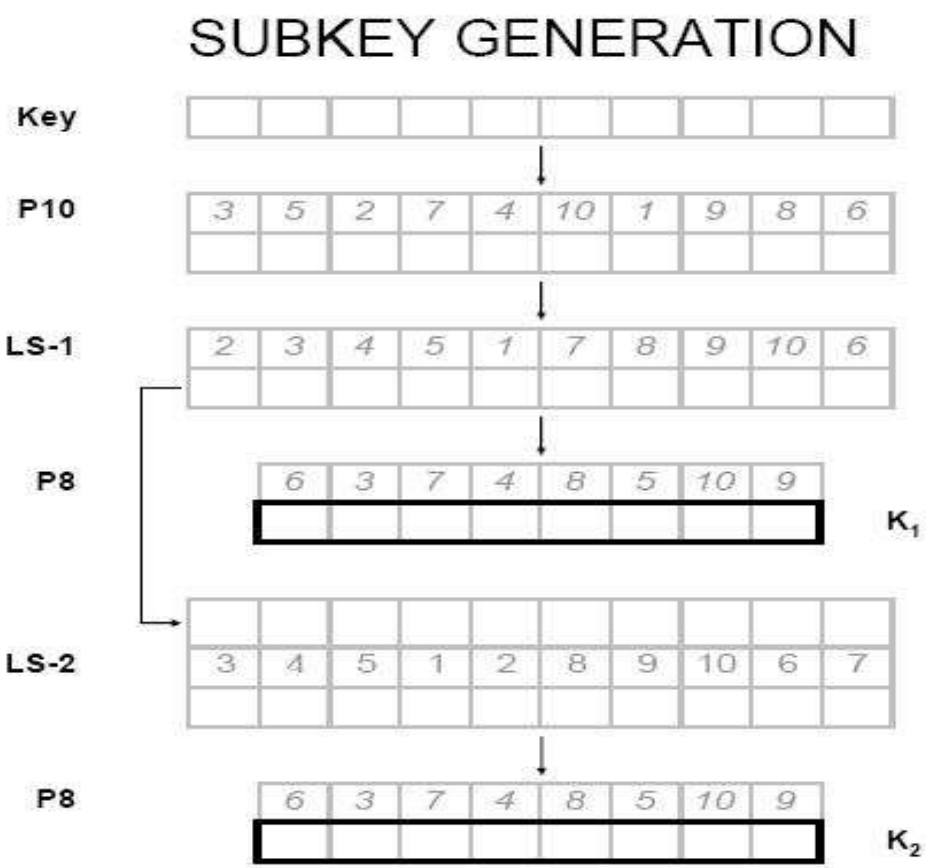
Step (4): Apply LS-2 (left shift 2)

LS-2					LS-2				
3	4	5	1	2	8	9	10	6	7

00001 | 11000 → LS2 → 00100 | 00011 → *P8*

K2 = 01000011

S-DES KG Example



Self Assessment

- Using S-DES key generation, generate the k1 and K2 using the key (0110110101), Show intermediate results after each function

S-DES KG Example

Assume given a key to be:

K = 0110110101

Step (1):P10 → 11100 | 10011

Step (2): LS-1 → 11001 | 00111

Step (3): Apply permutation *P8*

P10									
3	5	2	7	4	10	1	9	8	6

LS-1					LS-1				
2	3	4	5	1	7	8	9	10	6

P8							
6	3	7	4	8	5	10	9

then K1 = 00001111

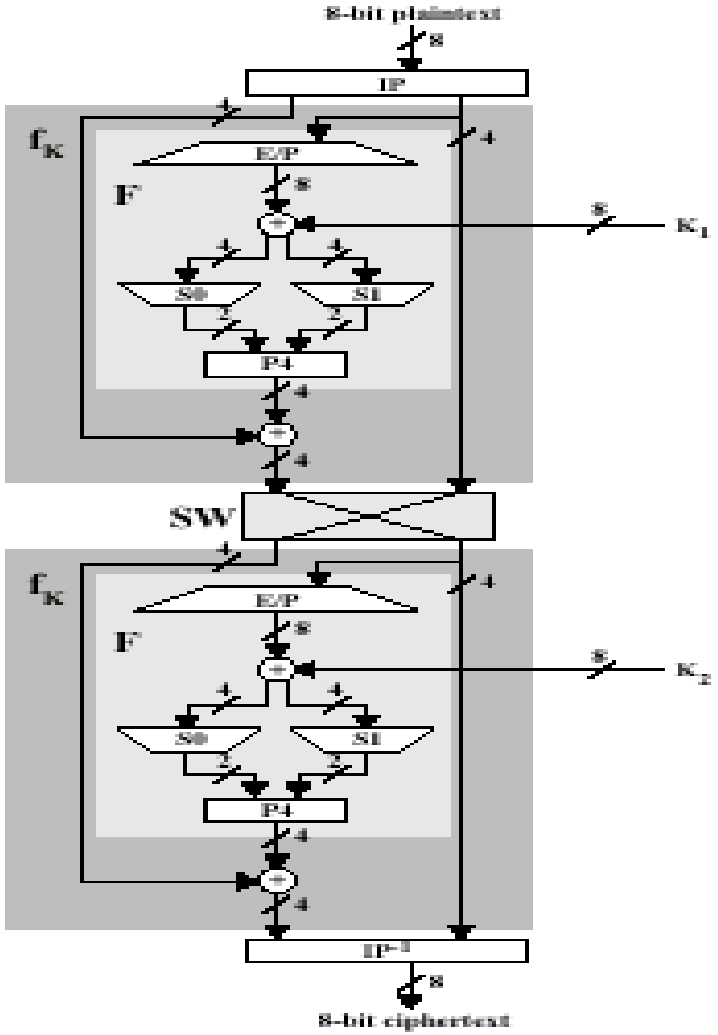
Step (4): Apply LS-2 (left shift 2)

LS-2					LS-2				
3	4	5	1	2	8	9	10	6	7

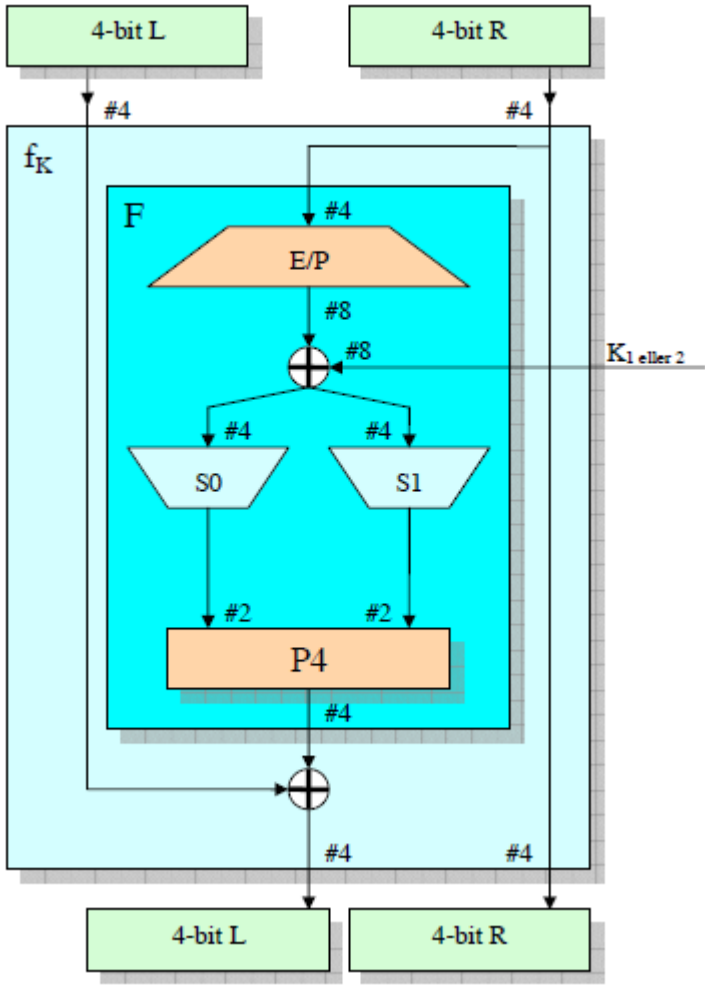
00001 | 11000 → LS2 → 00111 | 11100 → *P8*

K2 = 11111100

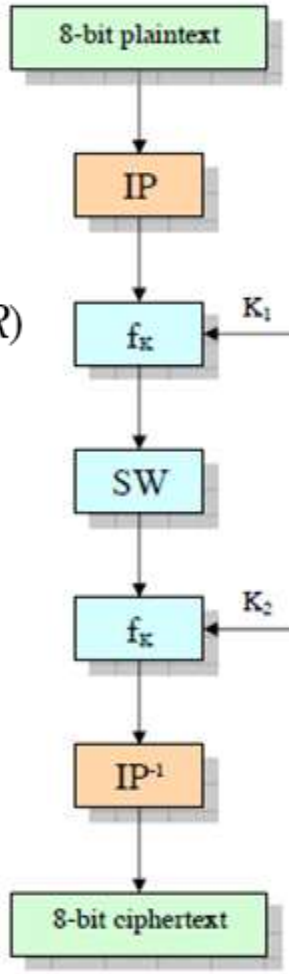
S-DES Encryption Details



S-DES Encryption Details



$$f_K(L, R) = (L \oplus \mathrm{F}(R, SK), R)$$



S-DES S-Boxes

- S-DES (and DES) perform substitutions using S-Boxes
- S-Box considered as a matrix: input used to select row/column; selected elements is output.
- 4 bit input: bit_1, bit_2, bit_3, bit_4
- Bit_1 bit_4 specifies row (0, 1, 2, 3 in decimal)
- Bit_2 bit_3 specifies column
- 2 bit output

S_0		C_0	C_1	C_2	C_3
	R_0	1	0	3	2
	R_1	3	2	1	0
	R_2	0	2	1	3
	R_3	3	1	3	2

S_1		C_0	C_1	C_2	C_3
	R_0	0	1	2	3
	R_1	2	0	1	3
	R_2	3	0	1	0
	R_3	2	1	0	3

S-DES S-Boxes Operations

1. **First and fourth bits give row number.**
2. **Second and third bits give column number.**
3. **Look up number in specified row and column.**
4. **Convert to binary.**

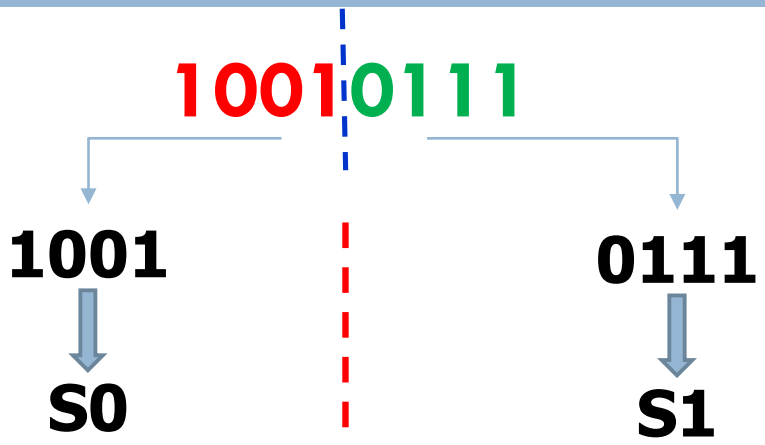
S-Boxes Operations Example – 4 bits

1001

$$R_{14} \rightarrow 11 \rightarrow R_3$$

$$C_{23} \rightarrow 00 \rightarrow C_0$$

S-Boxes Operations Example – 8 bits



$R_{14} \rightarrow 11 \rightarrow R_3$
$C_{23} \rightarrow 00 \rightarrow C_0$
From $S_0 \rightarrow R_3$ & C_0

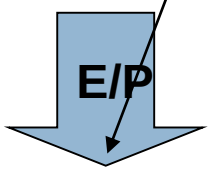
$R_{14} \rightarrow 01 \rightarrow R_1$
$C_{23} \rightarrow 11 \rightarrow C_3$
From $S_1 \rightarrow R_1$ & C_3

S-DES Example

Let plaintext: 01101101

$IP = (2,6,3,1,4,8,5,7)$

1110 | 0110



Apply expansion/permutation E/P to right 4 bits of above result,
= 4 1 2 3 2 3 4 1

00111100

S-DES Example

⊕	0	1
0	0	1
1	1	0

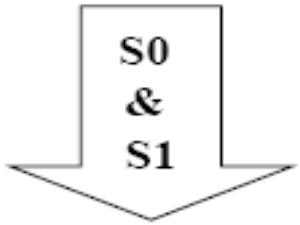
XOR

Perform binary XOR operation with sub key K1: 10100100

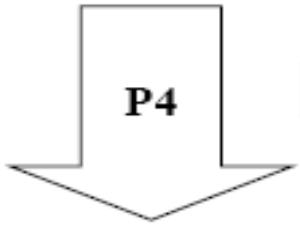
1001 | 1000

From above:
For the row, combine bits 1 and 4 and convert to decimal.
For the column, combine bits 2 and 3 and convert to decimal.

Left Side:
bits 1 & 4 → 11 → Row: 3
bits 2 & 3 → 00 → Col: 0
therefore, get from S_0 R3 & C0 → 3 → 11
Right Side:
bits 1 & 4 → 10 → Row: 2
bits 2 & 3 → 00 → Col: 0
therefore, get from S1 R2 & C0 → 3 → 11



1111



P4 = (2,4,3,1)

1111

Perform binary XOR operation, combining it with the left 4-bits of our first result (application of IP to original plaintext input, blue cell above).

Result:

0001

Rewrite that first result with its left half replaced.

$$0001 \mid 0110$$

Swap the two 4-bit halves of the above result.

$$0110 \mid 0001$$

To right 4 bits of above, apply E/P

$$10000010$$

Upon above result, perform binary XOR operation with sub-key K2: 01000011

$$11000001$$

1100 | 0001

From above:
For the row, combine bits 1 and 4 and convert to decimal.
For the column, combine bits 2 and 3 and convert to decimal.

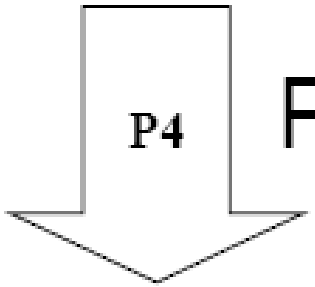
Left Side:

bits 1 & 4 → 10 → Row: 2
bits 2 & 3 → 10 → Col: 2
therefore, get from S_0 R2 & C2 → 1 → 01

Right Side:

bits 1 & 4 → 01 → Row: 1
bits 2 & 3 → 00 → Col: 0
therefore, get from S_1 R1 & C0 → 2 → 10

0110



P4 = (2,4,3,1)

1010

Perform binary XOR operation with the left 4-bits of the earlier swap result (0110).

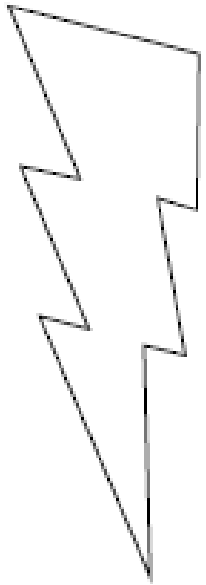
1100

Rewrite that first result with its left half replaced.

11000001

11000001

To above result, apply reverse of initial permutation IP, which is IP^{-1} =(4,1,3,5,7,2,8,6).



Ciphertext is

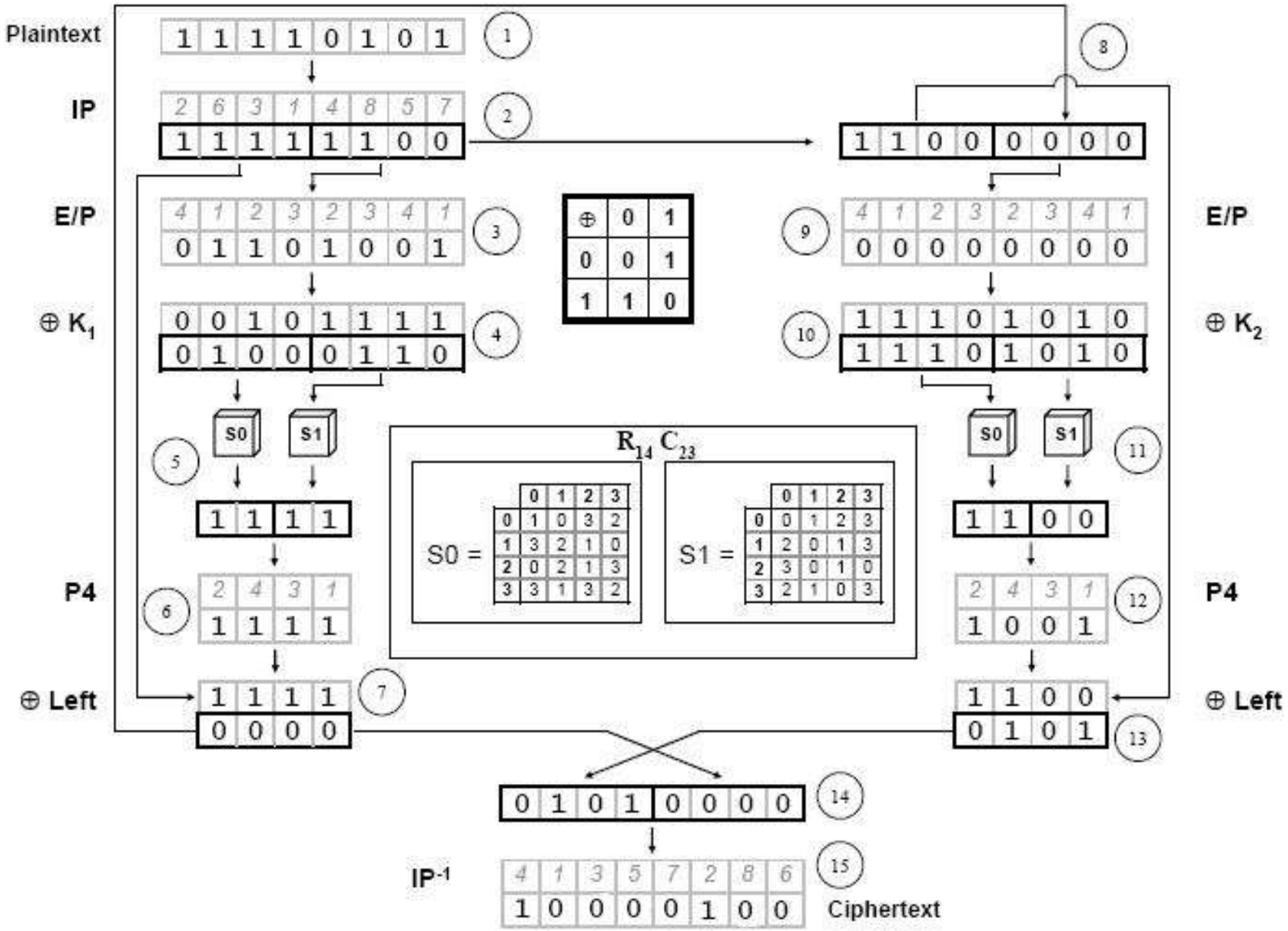
01000110

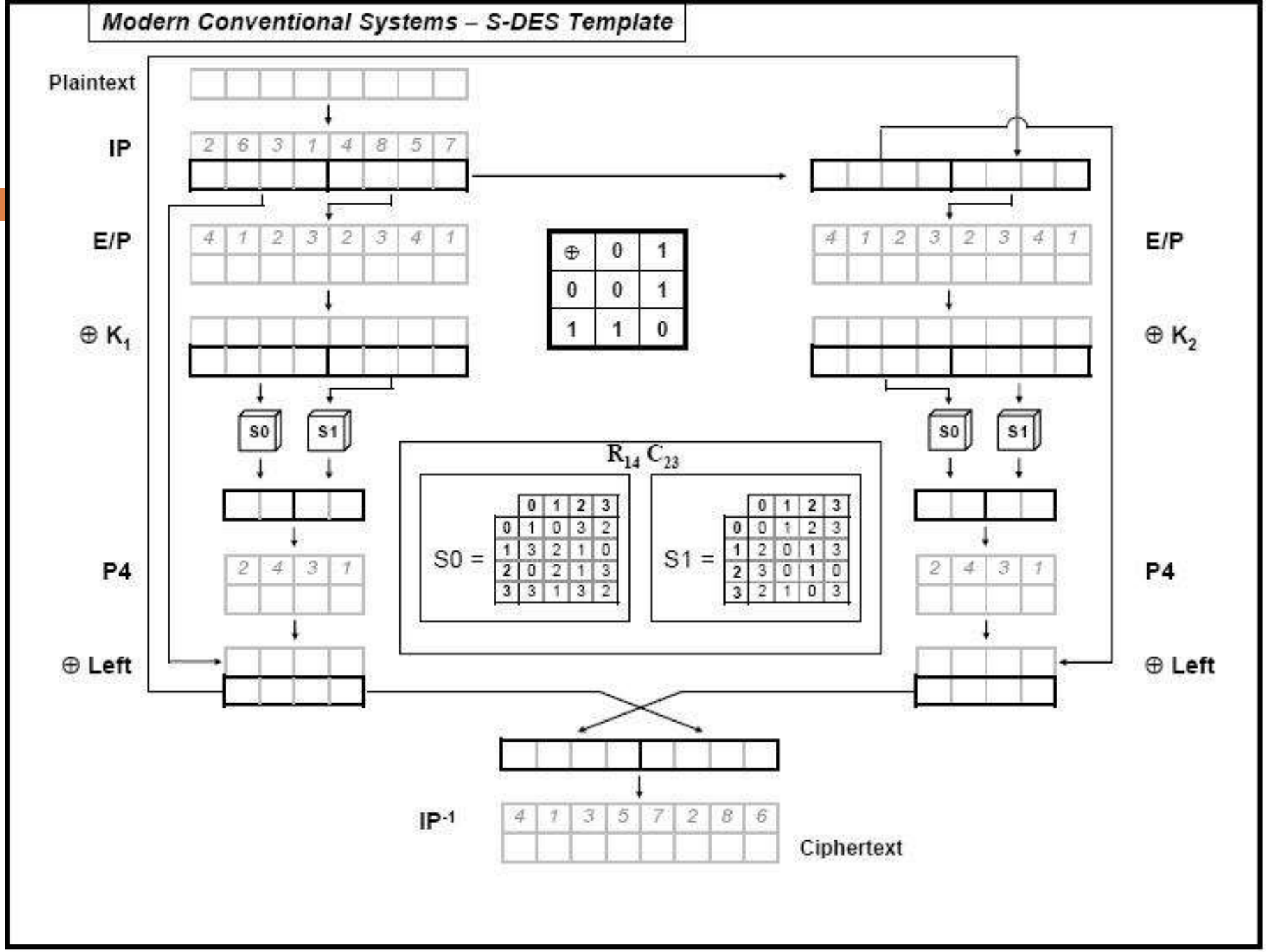
S-DES Example 1

Encrypt the following plaintext with the given key using the Simplified DES algorithm:

Plaintext: 11110101

Key: 0010010111

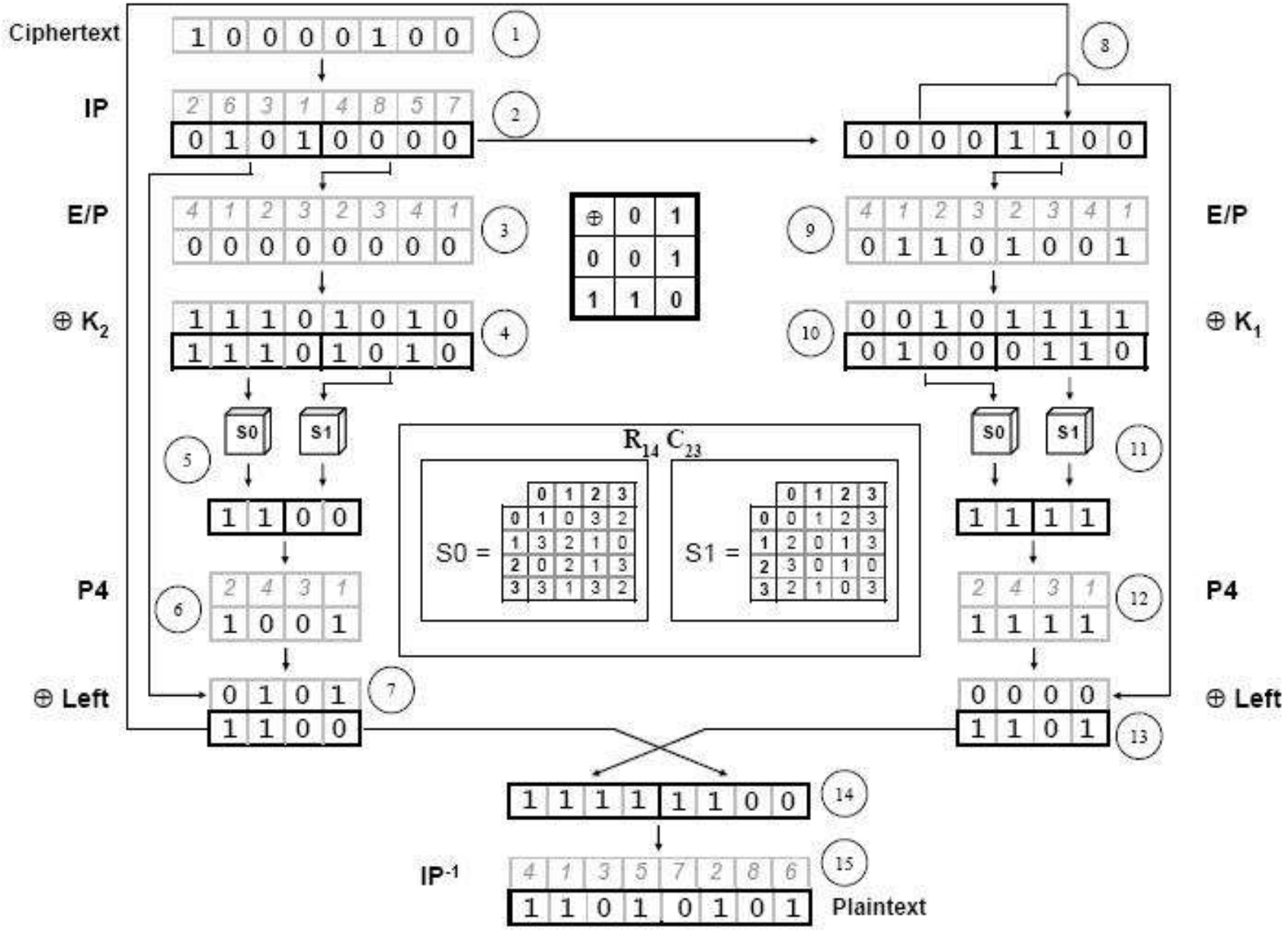

Plaintext
1 1 1 1 0 1 0 1
1
IP
2 6 3 1 4 8 5 7
1 1 1 1 1 1 0 0
2
E/P
4 1 2 3 2 3 4 1
0 1 1 0 1 0 0 1
3
⊕ K1
0 0 1 0 1 1 1 1
0 1 0 0 0 1 1 0
4
S0
S1
5
1 1 1 1
P4
2 4 3 1
1 1 1 1
6
⊕ Left
1 1 1 1
0 0 0 0
7
⊕ 0 1
0 0 1
1 1 0
R14 C23
S0 =
0 1 2 3
0 1 0 3 2
1 3 2 1 0
2 0 2 1 3
3 3 1 3 2
S1 =
0 1 2 3
0 0 1 2 3
1 2 0 1 3
2 3 0 1 0
3 2 1 0 3
8
1 1 0 0 0 0 0 0
9
E/P
4 1 2 3 2 3 4 1
0 0 0 0 0 0 0 0
10
⊕ K2
1 1 1 0 1 0 1 0
1 1 1 0 1 0 1 0
S0
S1
11
1 1 0 0
P4
2 4 3 1
1 0 0 1
12
⊕ Left
1 1 0 0
0 1 0 1
13
0 1 0 1 0 0 0 0
14
IP-1
4 1 3 5 7 2 8 6
1 0 0 0 0 1 0 0
15
Ciphertext

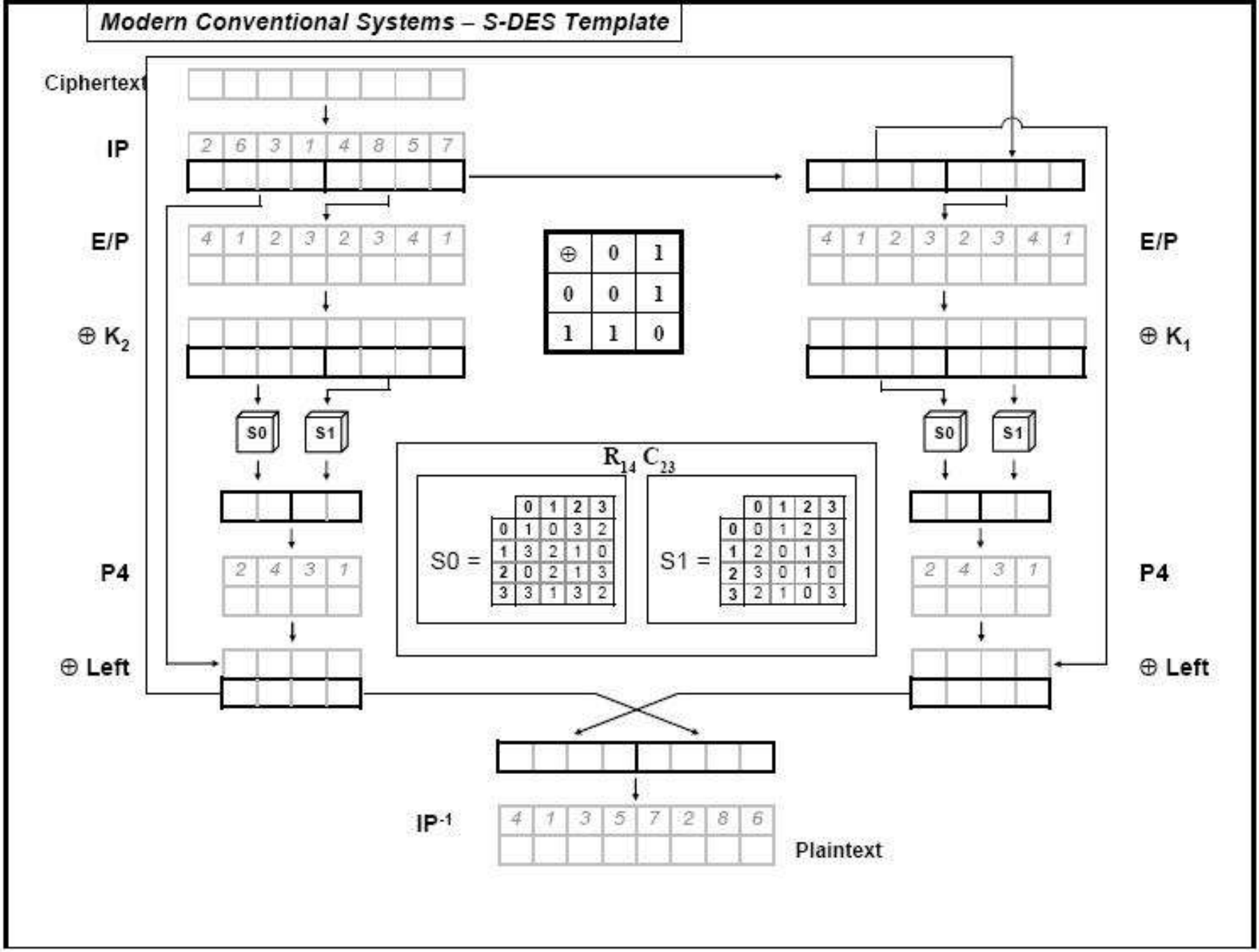

Modern Conventional Systems – S-DES Template
Plaintext
IP
2 6 3 1 4 8 5 7
E/P
4 1 2 3 2 3 4 1
⊕ K1
S0
S1
P4
2 4 3 1
⊕ Left
⊕ 0 1
0 0 1
1 1 0
R14 C23
S0 =
0 1 2 3
0 1 0 3 2
1 3 2 1 0
2 0 2 1 3
3 3 1 3 2
S1 =
0 1 2 3
0 0 1 2 3
1 2 0 1 3
2 3 0 1 0
3 2 1 0 3
E/P
⊕ K2
S0
S1
P4
⊕ Left
IP-1
4 1 3 5 7 2 8 6
Ciphertext

Self Assessment

- Let the plaintext be the string 0010 1000, Let the 10 bit key be 1100011110. Using S-DES key generation, generate the k_1 and K_2, and Find (L_1, R_1, L_2 and R_2) and then the ciphertext, Show intermediate results after each function

S-DES Decryption


Ciphertext
1 0 0 0 0 1 0 0
1
IP
2 6 3 1 4 8 5 7
0 1 0 1 0 0 0 0
2
E/P
4 1 2 3 2 3 4 1
0 0 0 0 0 0 0 0
3
⊕ K2
1 1 1 0 1 0 1 0
1 1 1 0 1 0 1 0
4
S0
S1
5
1 1 0 0
P4
2 4 3 1
1 0 0 1
6
⊕ Left
0 1 0 1
1 1 0 0
7
⊕ 0 1
0 0 1
1 1 0
8
0 0 0 0 1 1 0 0
9
E/P
4 1 2 3 2 3 4 1
0 1 1 0 1 0 0 1
10
⊕ K1
0 0 1 0 1 1 1 1
0 1 0 0 0 1 1 0
S0
S1
11
1 1 1 1
P4
2 4 3 1
1 1 1 1
12
⊕ Left
0 0 0 0
1 1 0 1
13
R14 C23
S0 =
0 1 2 3
0 1 0 3 2
1 3 2 1 0
2 0 2 1 3
3 3 1 3 2
S1 =
0 1 2 3
0 0 1 2 3
1 2 0 1 3
2 3 0 1 0
3 2 1 0 3
1 1 1 1 1 1 0 0
14
IP-1
4 1 3 5 7 2 8 6
1 1 0 1 0 1 0 1
15
Plaintext


Modern Conventional Systems – S-DES Template
Ciphertext
IP
2 6 3 1 4 8 5 7
E/P
4 1 2 3 2 3 4 1
⊕ K2
S0
S1
P4
2 4 3 1
⊕ Left
⊕ 0 1
0 0 1
1 1 0
R14 C23
S0 =
0 1 2 3
0 1 0 3 2
1 3 2 1 0
2 0 2 1 3
3 3 1 3 2
S1 =
0 1 2 3
0 0 1 2 3
1 2 0 1 3
2 3 0 1 0
3 2 1 0 3
E/P
4 1 2 3 2 3 4 1
⊕ K1
S0
S1
P4
2 4 3 1
⊕ Left
IP-1
4 1 3 5 7 2 8 6
Plaintext