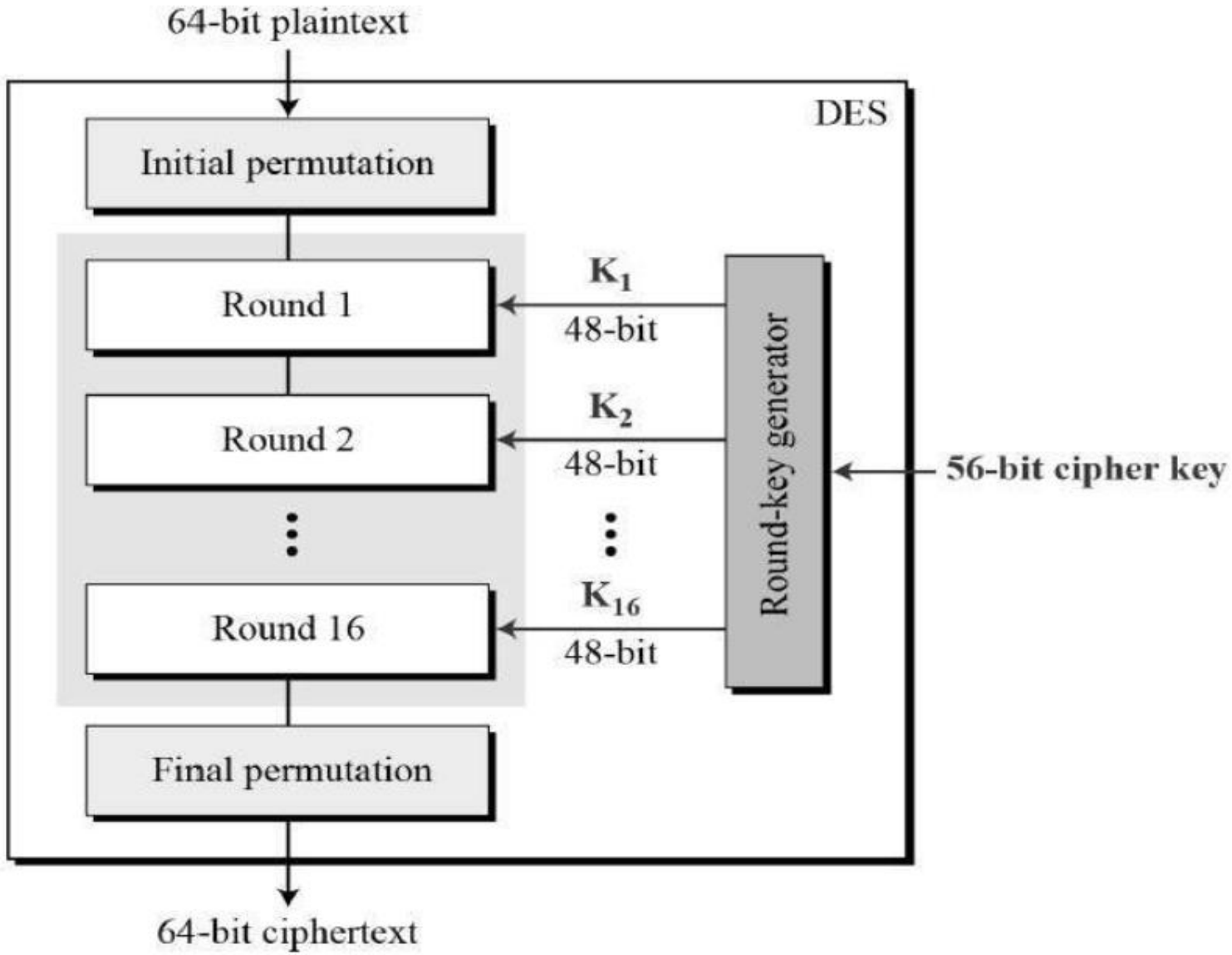
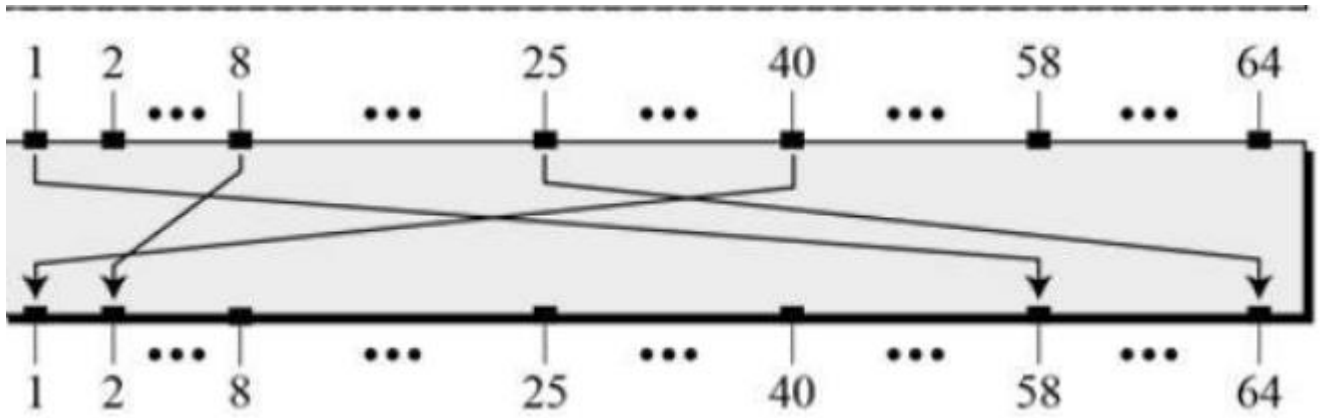
# Data Encryption Standard



# Initial permutation

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 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 |




| *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 |

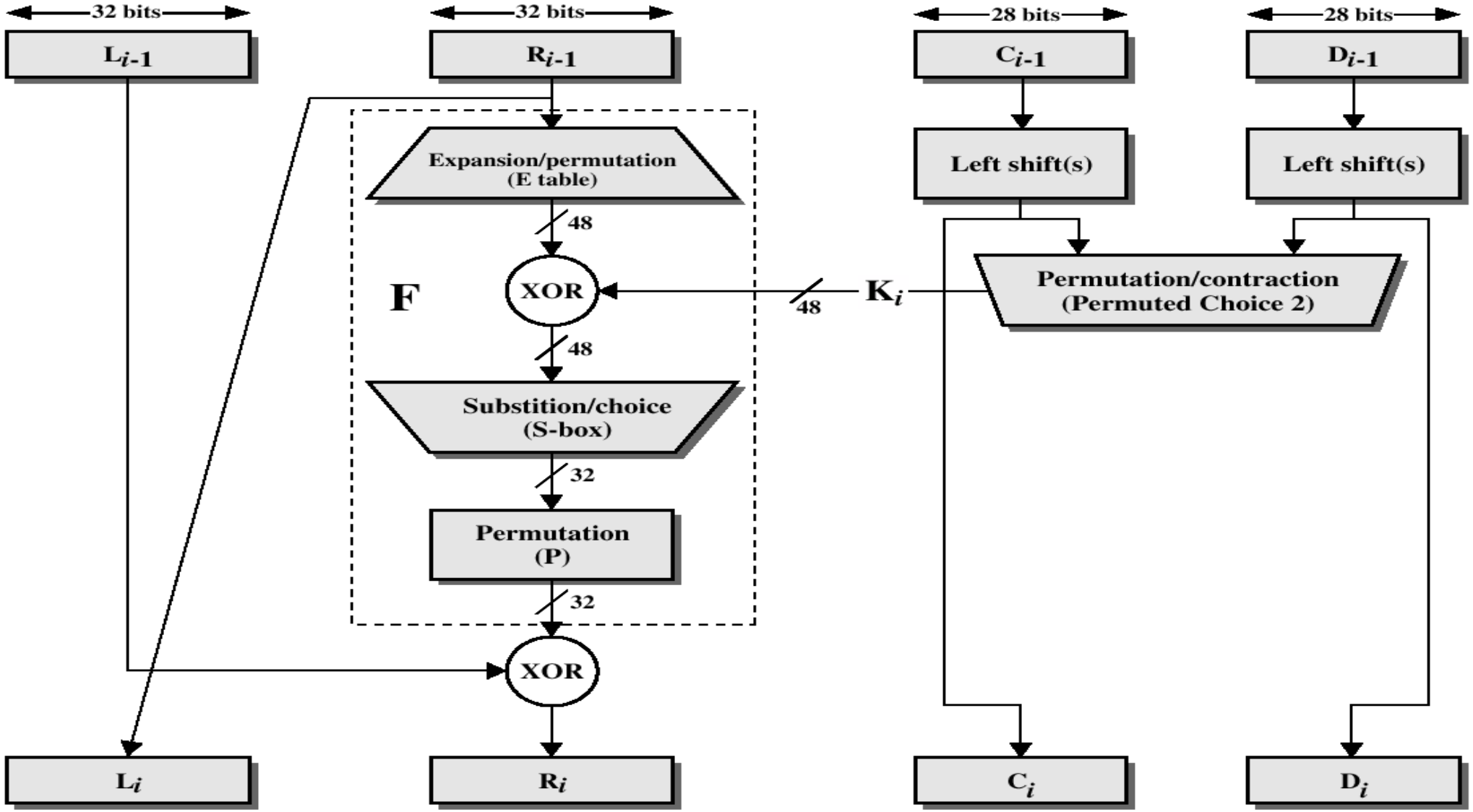
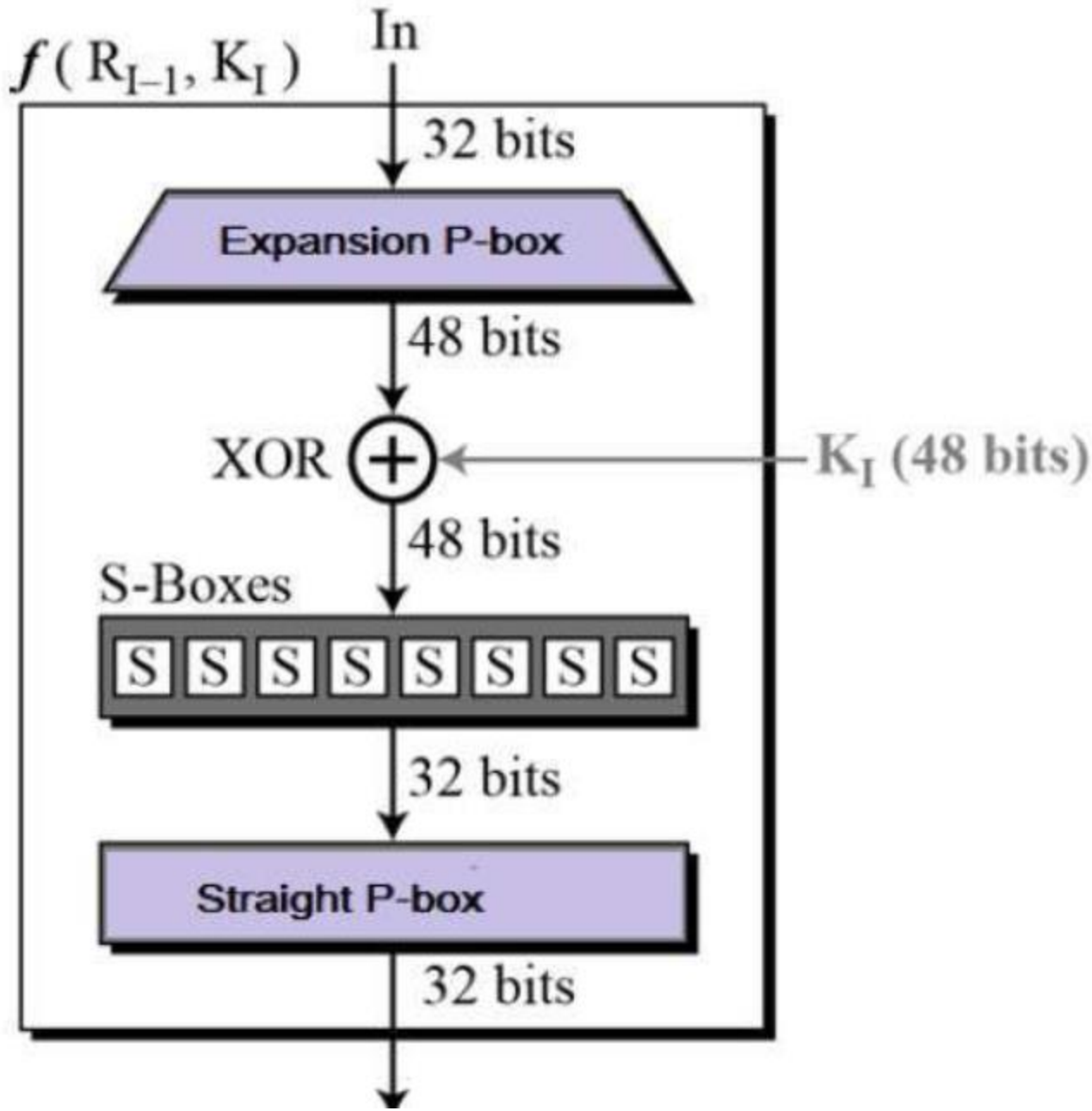
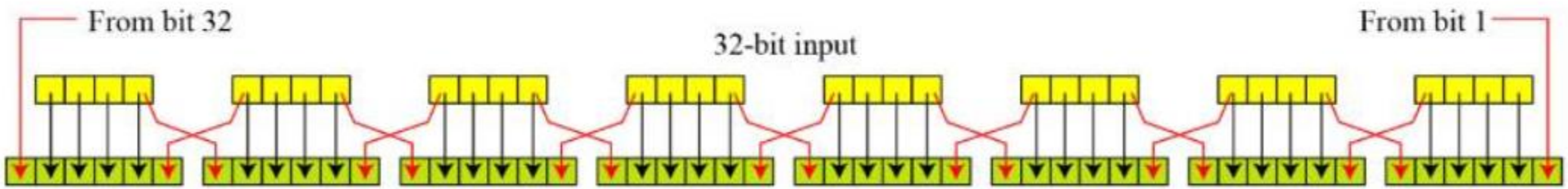
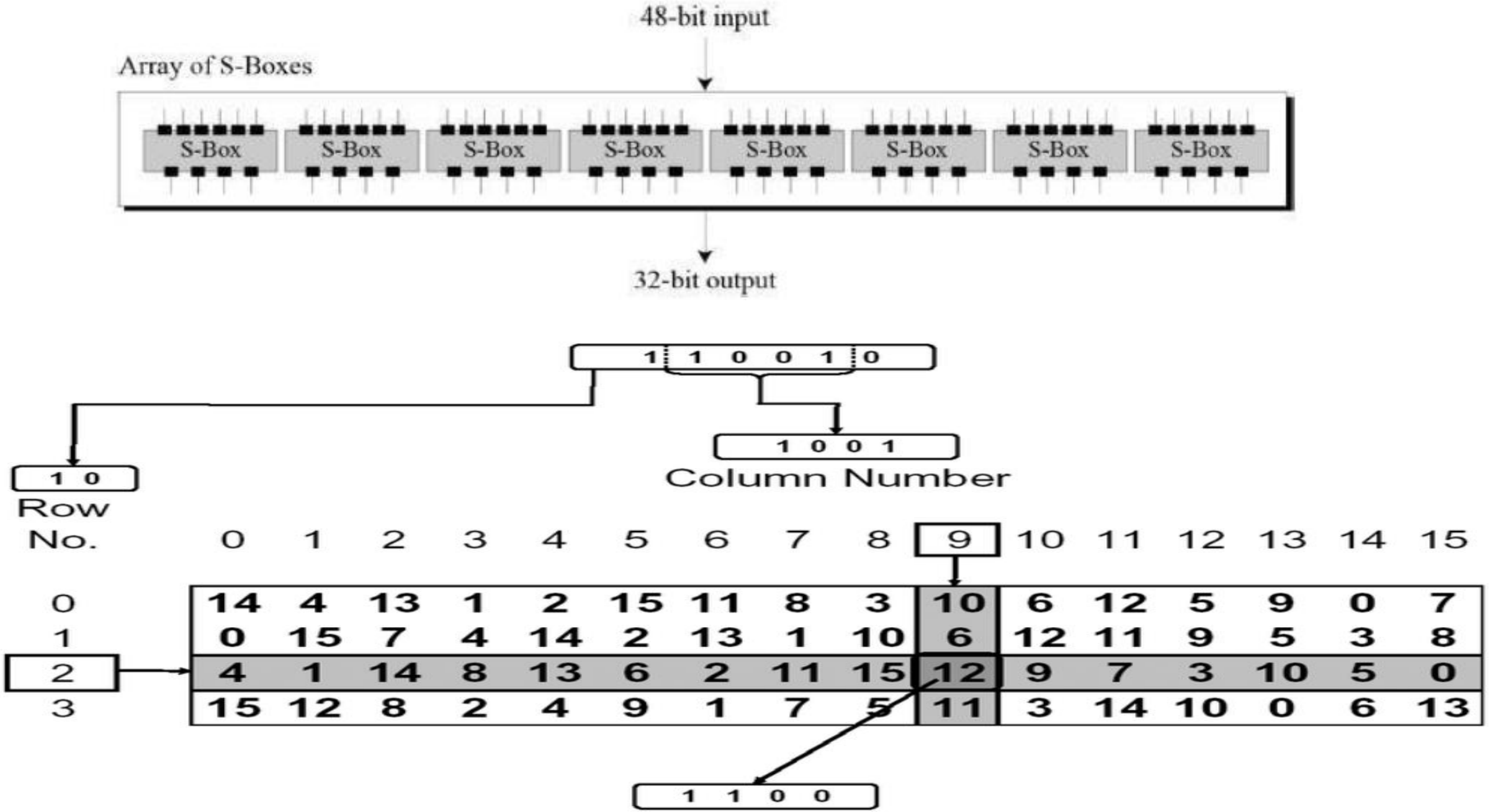


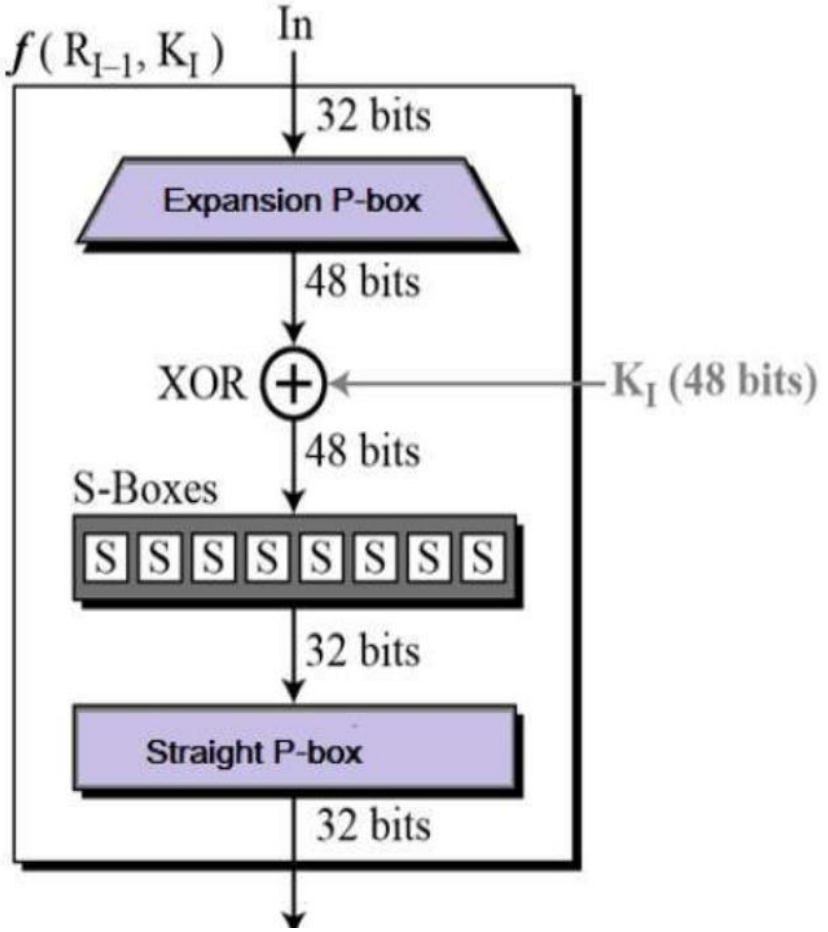

**Figure 2.4 Single Round of DES Algorithm**


$f(R_{I-1}, K_I)$
In
32 bits
Expansion P-box
48 bits
XOR
$K_I$ (48 bits)
48 bits
S-Boxes
S S S S S S S S
32 bits
Straight P-box
32 bits

## *Expansion permutation*




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
1 1 0 0 1 0
1 0 0 1
Column Number
1 0
Row
No. 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
1 1 0 0



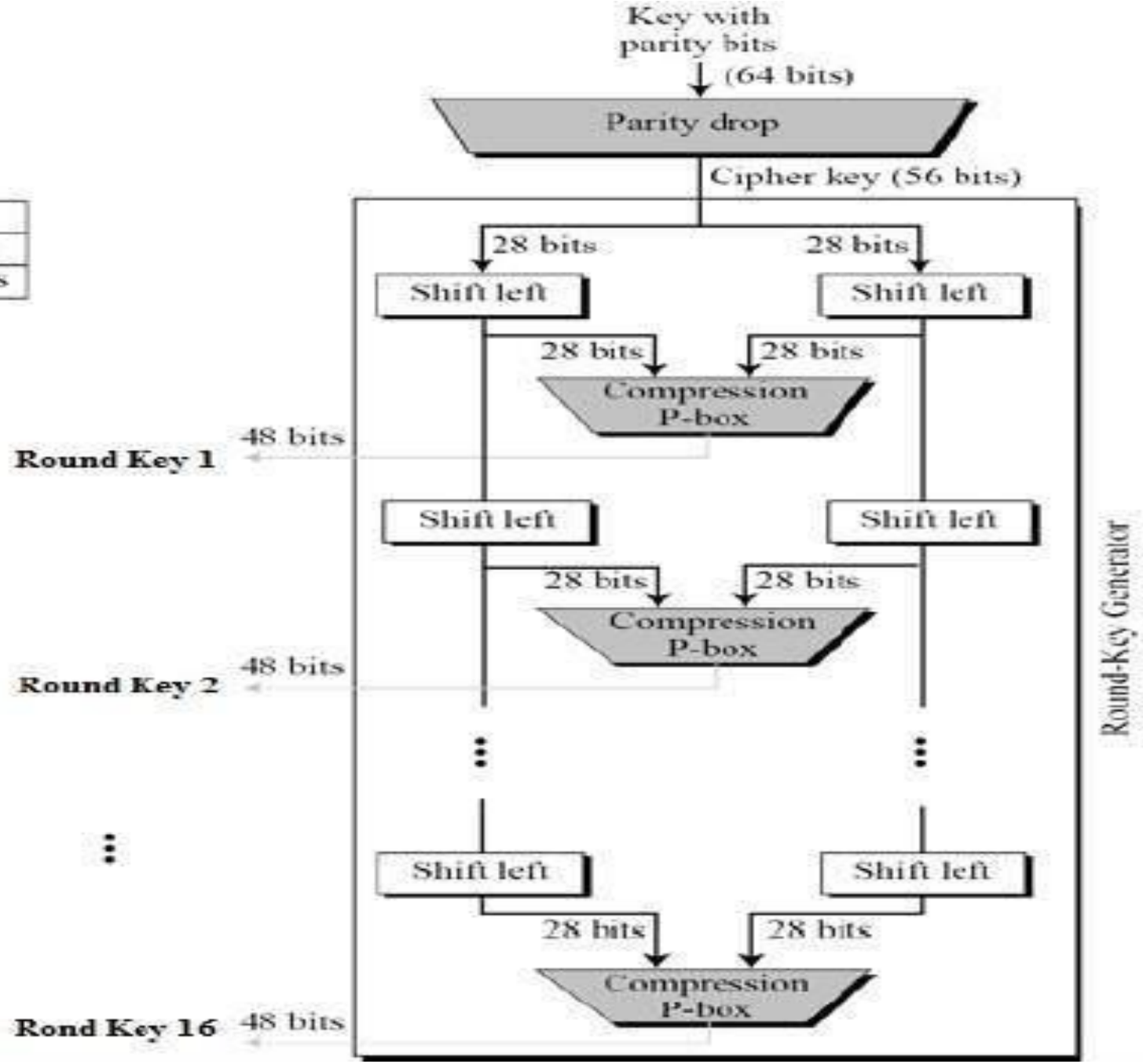

## Straight Permutation

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 07 | 20 | 21 | 29 | 12 | 28 | 17 |
| 01 | 15 | 23 | 26 | 05 | 18 | 31 | 10 |
| 02 | 08 | 24 | 14 | 32 | 27 | 03 | 09 |
| 19 | 13 | 30 | 06 | 22 | 11 | 04 | 25 |

# Key Generation

Shifting

| Rounds | Shift |
|---|---|
| 1, 2, 9, 16 | one bit |
| Others | two bits |



## DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

**Avalanche effect** − A small change in plaintext results in a very great change in the ciphertext.
**Completeness** − Each bit of ciphertext depends on many bits of plaintext.

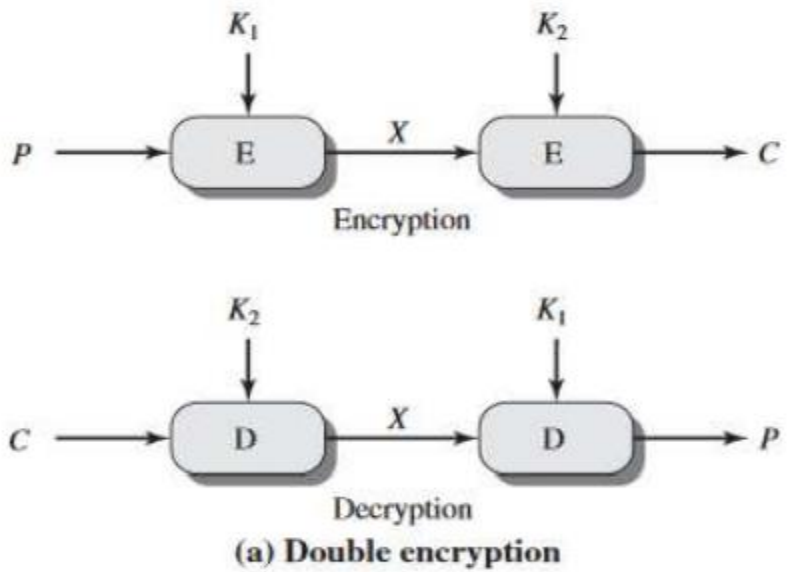
## Double DES Encryption

Given a plaintext P and two encryption keys $K_1$ and $K_2$, a cipher text can be generated as,

$$C = E(K_2, E(K_1, P))$$

Decryption requires that the keys be applied in reverse order,

$$P = D(K_1, D(K_2, C))$$




(a) Double encryption