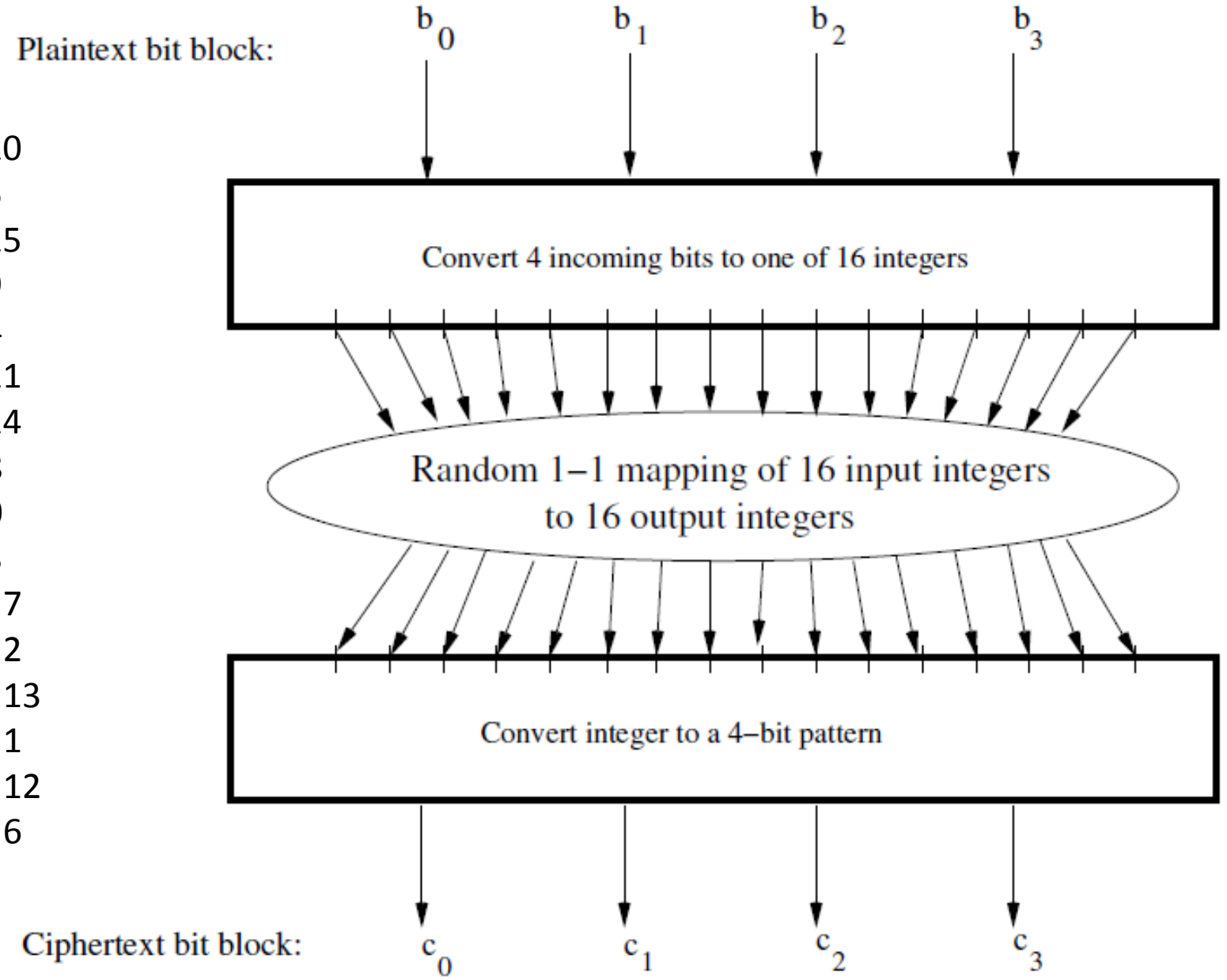
# Data and Network Security

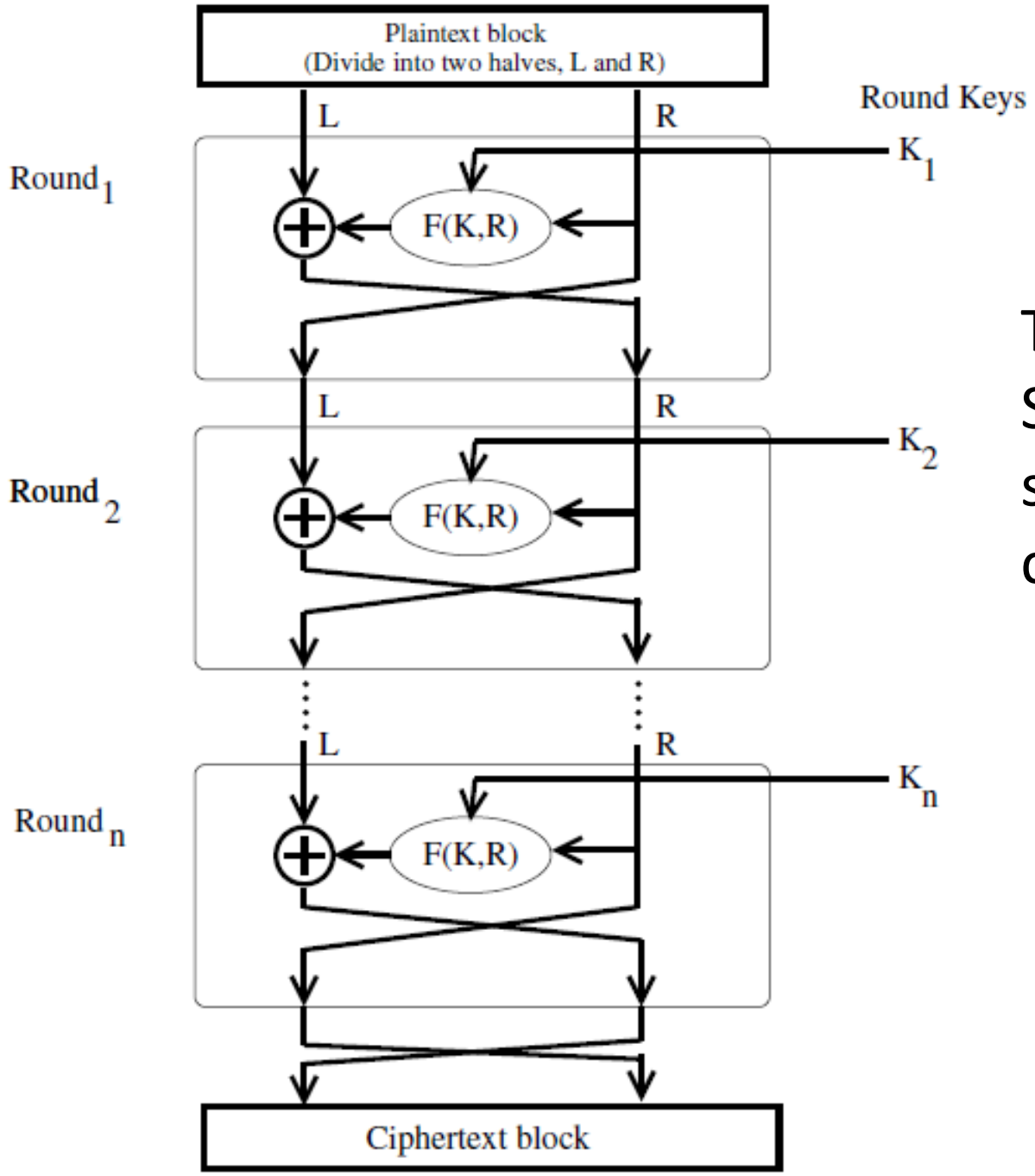
Course Code: IT-4542

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



# The Feistel Structure For Block Ciphers

- Named after the IBM cryptographer Horst Feistel and first implemented in the Lucifer cipher by Horst Feistel and Don Coppersmith.
- There are multiple rounds of processing of the plaintext, with each round consisting of a substitution step followed by a permutation step.
- The block, R goes through unchanged. The left half, L, goes through an operation. The operation carried out on L is referred to as the Feistel Function.
- The permutation step: swapping the modified L and R.
- Examples: DES, Blowfish, CAST-128, and KASUMI




The Feistel Structure for symmetric key cryptography

- Let $LE_i$ and $RE_i$ denote the output half-blocks at the end of the *i*th round of processing. The letter '$E$' denotes encryption.

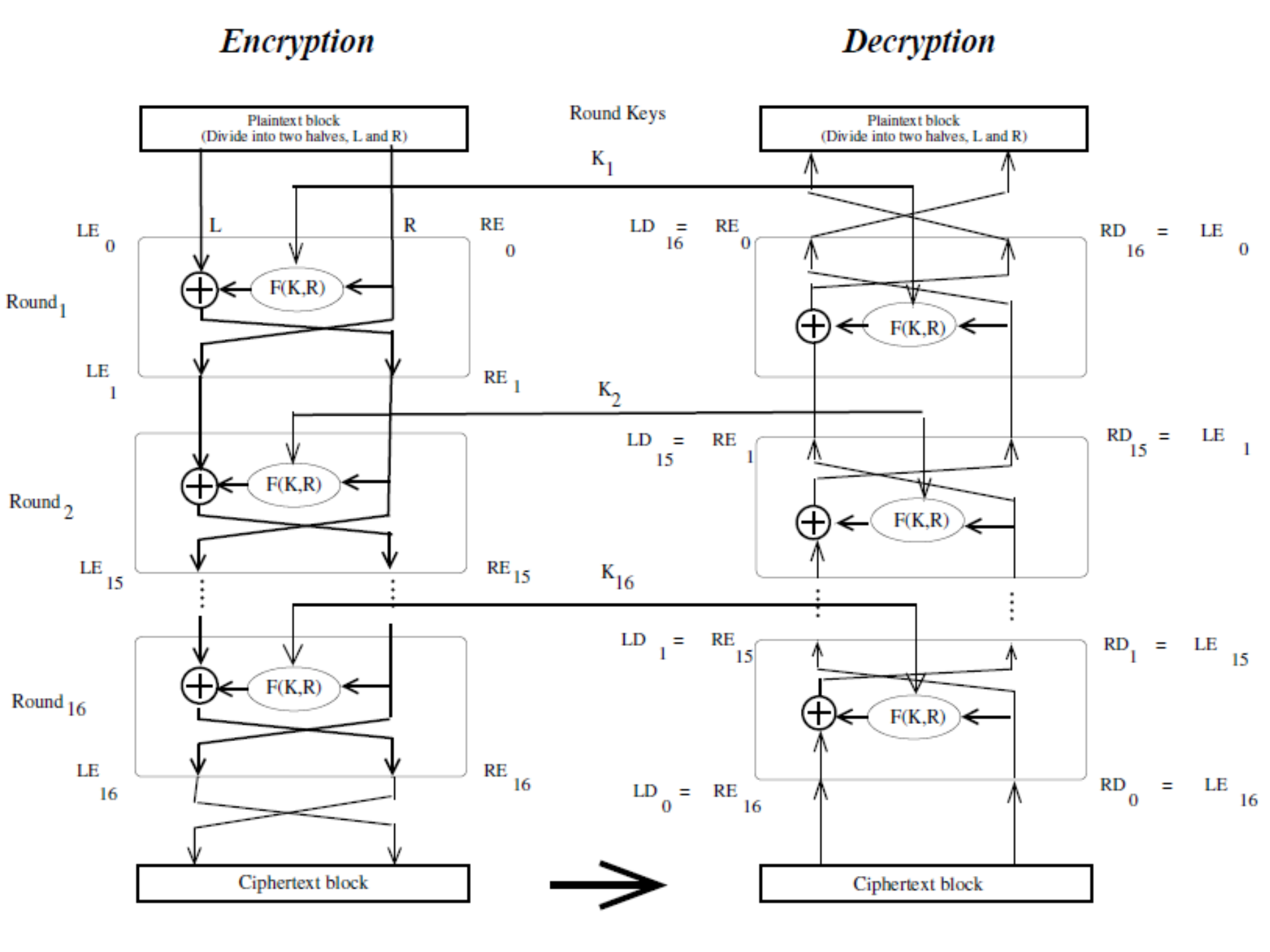
$$\begin{aligned} LE_i &= RE_{i-1} \\ RE_i &= LE_{i-1} \oplus F(RE_{i-1}, K_i) \end{aligned}$$

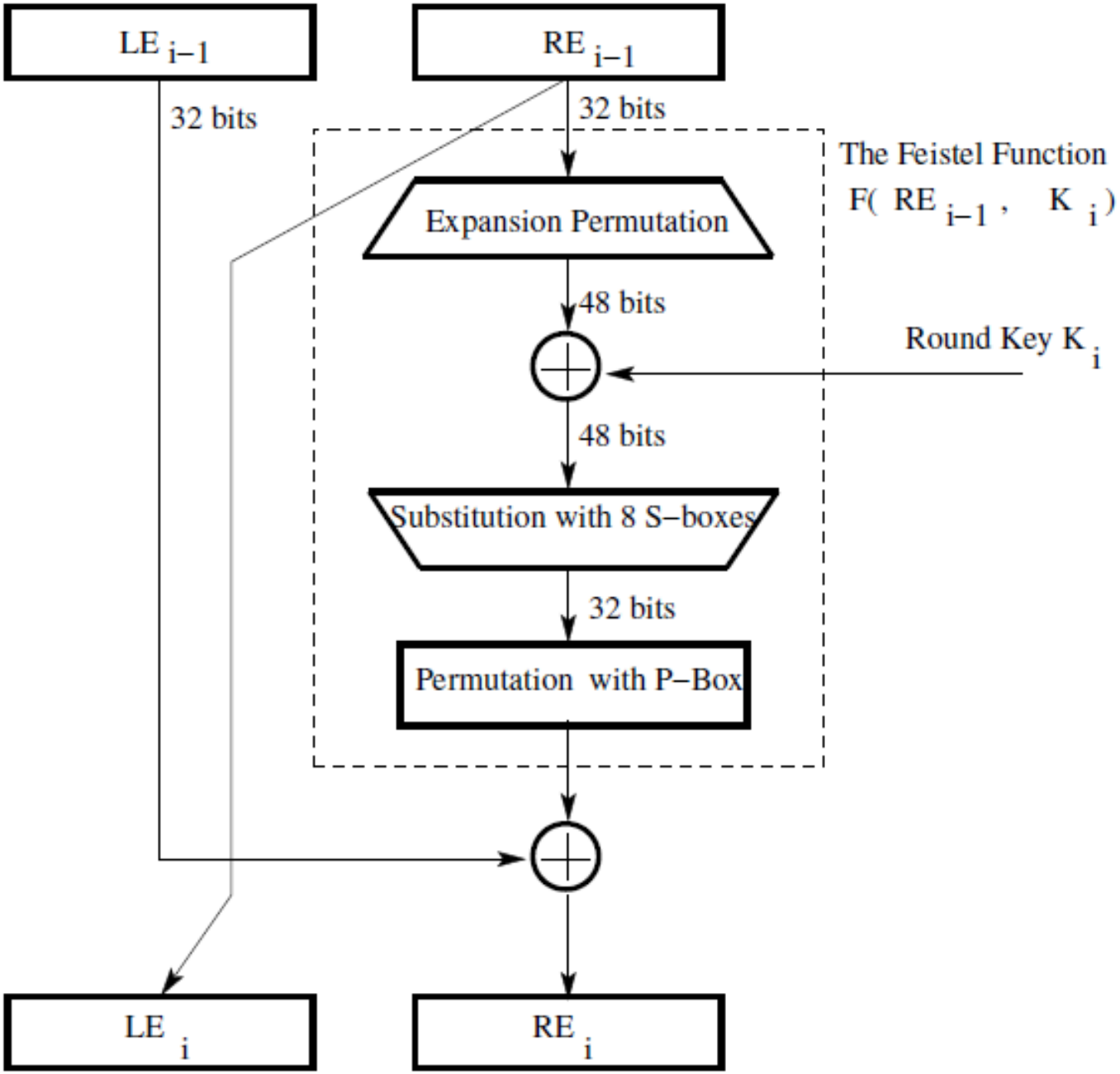
- $F$ denotes the operation that "scrambles" $RE_{i-1}$ of the previous round with the round key $K_i$.
- For Example, 16th rounds of processing

$$\begin{aligned} LE_{16} &= RE_{15} \\ RE_{16} &= LE_{15} \oplus F(RE_{15}, K_{16}) \end{aligned}$$

# Decryption in Ciphers Based on the Feistel Structure

- The decryption algorithm is exactly the same as the encryption algorithm with the only difference that the round keys are used in the reverse order.


Encryption
Decryption
Plaintext block
(Divide into two halves, L and R)
Round Keys
K1
L
R
LE0
RE0
F(K,R)
Round1
LE1
RE1
K2
Round2
LE15
RE15
K16
Round16
LE16
RE16
Ciphertext block
LD16 = RE0
RD16 = LE0
LD15 = RE1
RD15 = LE1
LD1 = RE15
RD1 = LE15
LD0 = RE16
RD0 = LE16


LE i−1
RE i−1
32 bits
32 bits
The Feistel Function
F( RE i−1 , K i )
Expansion Permutation
48 bits
Round Key K i
48 bits
Substitution with 8 S−boxes
32 bits
Permutation with P−Box
LE i
RE i

# Data Encryption Algorithm

- The Expansion step:
  - first divide the 32-bit block into eight 4-bit words
  - attach an additional bit on the left to each 4-bit word that is the last bit of the previous 4-bit word
  - attach an additional bit to the right of each 4-bit word that is the beginning bit of the next 4-bit word.
  - Example: 1010 1010 1111

    010101

| 1111 | 0000 | 1010 | 1010 | 1111 | 0000 | 1010 | 1010 |
|---|---|---|---|---|---|---|---|
| 011110 | 100001 | 010101 | 010101 | 011110 | 100001 | 010101 | ? |

# Data Encryption Algorithm

- The Expansion step:
  - first divide the 32-bit block into eight 4-bit words
  - attach an additional bit on the left to each 4-bit word that is the last bit of the previous 4-bit word
  - attach an additional bit to the right of each 4-bit word that is the beginning bit of the next 4-bit word.
  - Example: 1010 1010 1111

010101

1111 0000 1010 1010 1111 0000 1010 1010

011110 100001 010101 010101 011110 100001 010101 ?

010101

# Data Encryption Algorithm

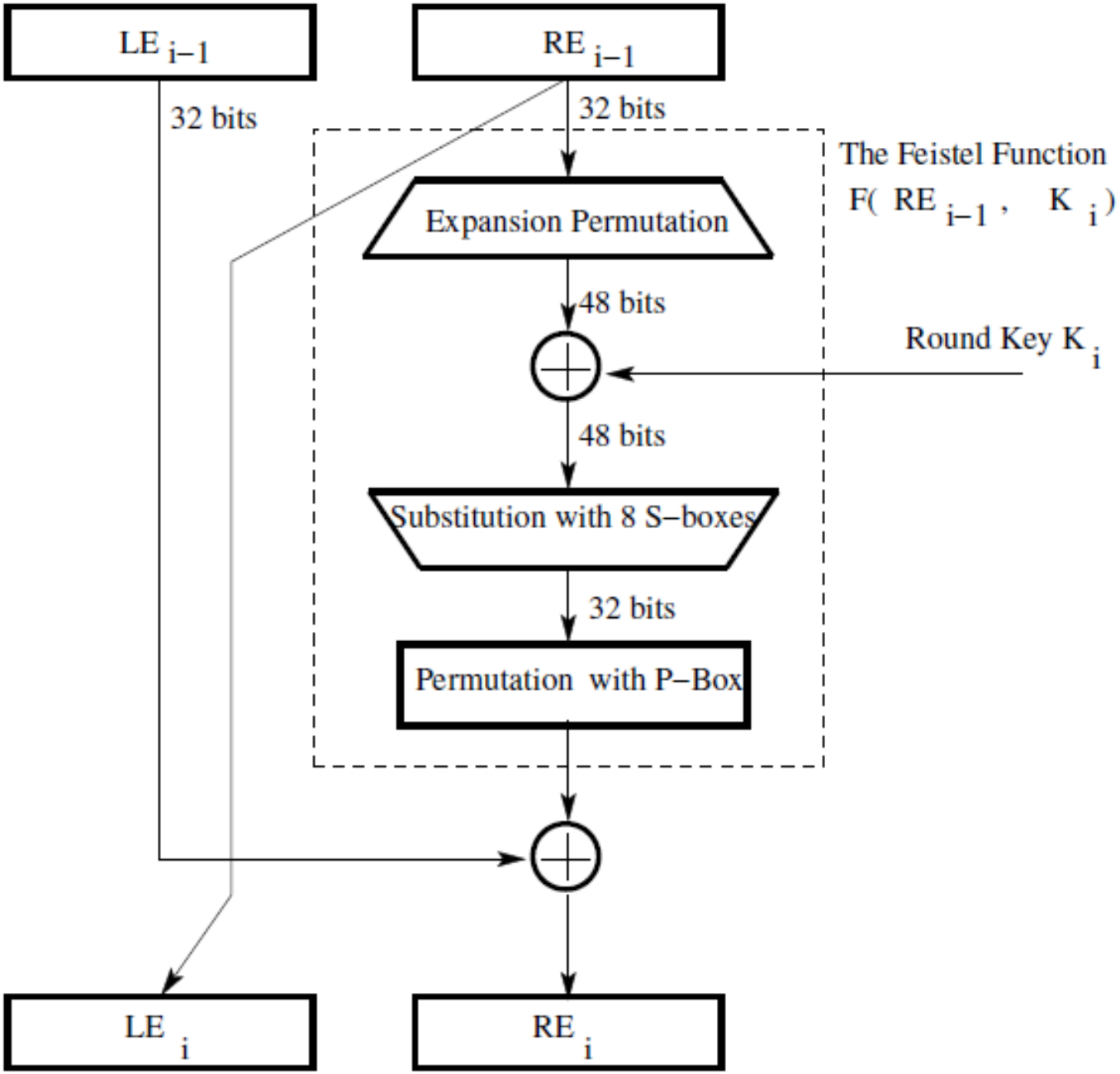
- The Expansion step:
  - first divide the 32-bit block into eight 4-bit words
  - attach an additional bit on the left to each 4-bit word that is the last bit of the previous 4-bit word
  - attach an additional bit to the right of each 4-bit word that is the beginning bit of the next 4-bit word.
  - Example: 1010 1010 1111

010101

1111 0000 1010 1010 1111 0000 1010 1010

011110 100001 010101 010101 011110 100001 010101 ?

01111010000101010101010111101000010101010101


LE i−1
RE i−1
32 bits
32 bits
The Feistel Function
F( RE i−1 , K i )
Expansion Permutation
48 bits
Round Key K i
48 bits
Substitution with 8 S−boxes
32 bits
Permutation with P−Box
LE i
RE i

# The DES Key Schedule: Generating the Round Keys

- The 56-bit encryption key is represented by 8 bytes, with the last bit (the least significant bit) of each byte used as a parity bit.
- The relevant 56 bits are subject to a permutation at the beginning before any round keys are generated. This is referred to as Key Permutation 1.
- At the beginning of each round, we divide the 56 relevant key bits into two 28 bit halves and circularly shift to the left each half by one or two bits, depending on the round.

Key with even parity

01100110 10010101 11010100 01010101

01111011 01100101 01011010 01100011

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

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

Key Permutation 1

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

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

0

Key Permutation 1

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

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

0 0

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

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

0 0 0

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

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

0 0 0 0 0

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

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

0 0 0 0 0 1 1

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

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

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

Key Permutation 1

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

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

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

Key Permutation 1

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

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

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

Key Permutation 1

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

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

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

Key Permutation 1

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

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

0 0 0 0 0 1 1

0 1 1 1 1 1 1

0 1 1 0 1 1 0

0 0 1 0 1 0 1

1 1 0 1 0 0 0

1 0 0 1 0 1 1

1 1 0 1 0 1 0

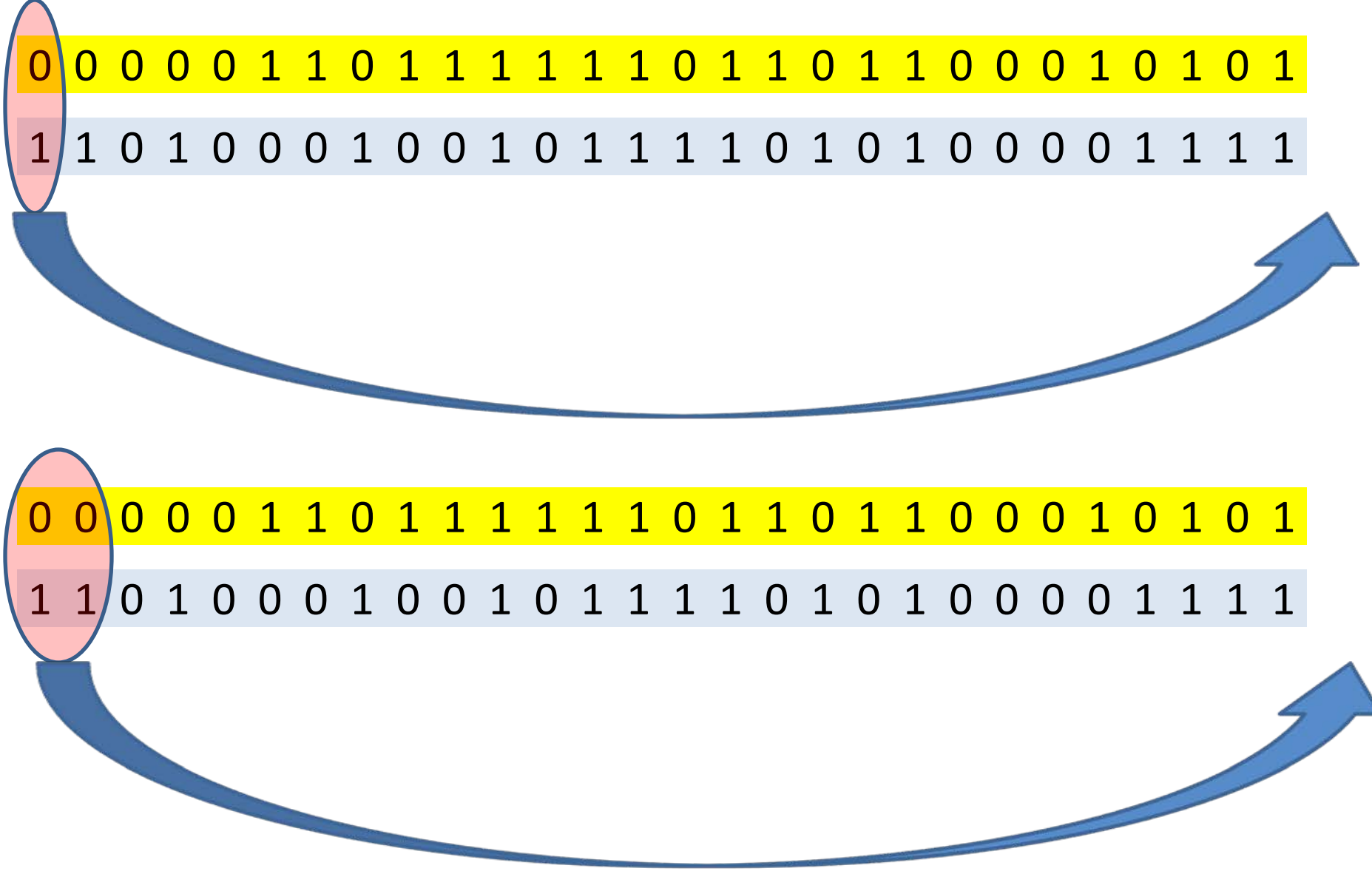
0 0 0 1 1 1 1

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

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

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

| *Round Number* | *Number of left shifts* |
|---|---|
| 1 | 1 |
| 2 | 1 |
| 3 | 2 |
| 4 | 2 |
| 5 | 2 |
| 6 | 2 |
| 7 | 2 |
| 8 | 2 |
| 9 | 1 |
| 10 | 2 |
| 11 | 2 |
| 12 | 2 |
| 13 | 2 |
| 14 | 2 |
| 15 | 2 |
| 16 | 1 |


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

# The DES Key Schedule: Generating the Round Keys

- Contraction-Permutation: Join together the two halves and apply a 56 bit to 48 bit contracting permutation (this is referred to as Permutation Choice 2).

| Key Permutation 2 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 13 | 16 | 10 | 23 | 0 | 4 | 2 | 27 |
| 14 | 5 | 20 | 9 | 22 | 18 | 11 | 3 |
| 25 | 7 | 15 | 6 | 26 | 19 | 12 | 1 |
| 40 | 51 | 30 | 36 | 46 | 54 | 29 | 39 |
| 50 | 44 | 32 | 47 | 43 | 48 | 38 | 55 |
| 33 | 52 | 45 | 41 | 49 | 35 | 28 | 31 |

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

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

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

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

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

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

| Key Permutation 2 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 13 | 16 | 10 | 23 | 0 | 4 | 2 | 27 |
| 14 | 5 | 20 | 9 | 22 | 18 | 11 | 3 |
| 25 | 7 | 15 | 6 | 26 | 19 | 12 | 1 |
| 40 | 51 | 30 | 36 | 46 | 54 | 29 | 39 |
| 50 | 44 | 32 | 47 | 43 | 48 | 38 | 55 |
| 33 | 52 | 45 | 41 | 49 | 35 | 28 | 31 |

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

1 1 1 1

| Key Permutation 2 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 13 | 16 | 10 | 23 | 0 | 4 | 2 | 27 |
| 14 | 5 | 20 | 9 | 22 | 18 | 11 | 3 |
| 25 | 7 | 15 | 6 | 26 | 19 | 12 | 1 |
| 40 | 51 | 30 | 36 | 46 | 54 | 29 | 39 |
| 50 | 44 | 32 | 47 | 43 | 48 | 38 | 55 |
| 33 | 52 | 45 | 41 | 49 | 35 | 28 | 31 |

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

1 1 1 1 0 1 0 0

1 0 0 1 0 0 1 1

| Key Permutation 2 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 13 | 16 | 10 | 23 | 0 | 4 | 2 | 27 |
| 14 | 5 | 20 | 9 | 22 | 18 | 11 | 3 |
| 25 | 7 | 15 | 6 | 26 | 19 | 12 | 1 |
| 40 | 51 | 30 | 36 | 46 | 54 | 29 | 39 |
| 50 | 44 | 32 | 47 | 43 | 48 | 38 | 55 |
| 33 | 52 | 45 | 41 | 49 | 35 | 28 | 31 |

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

1 1 1 1 0 1 0 0

1 0 0 1 0 0 1 1

1 1 0 1 0 0 0 0

1 1 0 1 0 1 1 1

| Key Permutation 2 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 13 | 16 | 10 | 23 | 0 | 4 | 2 | 27 |
| 14 | 5 | 20 | 9 | 22 | 18 | 11 | 3 |
| 25 | 7 | 15 | 6 | 26 | 19 | 12 | 1 |
| 40 | 51 | 30 | 36 | 46 | 54 | 29 | 39 |
| 50 | 44 | 32 | 47 | 43 | 48 | 38 | 55 |
| 33 | 52 | 45 | 41 | 49 | 35 | 28 | 31 |

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

1 1 1 1 0 1 0 0

1 0 0 1 0 0 1 1

1 1 0 1 0 0 0 0

1 1 0 1 0 1 1 1

1 0 0 0 1 0 1 1

1 1 1 1 0 0 0 0

| Key Permutation 2 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 13 | 16 | 10 | 23 | 0 | 4 | 2 | 27 |
| 14 | 5 | 20 | 9 | 22 | 18 | 11 | 3 |
| 25 | 7 | 15 | 6 | 26 | 19 | 12 | 1 |
| 40 | 51 | 30 | 36 | 46 | 54 | 29 | 39 |
| 50 | 44 | 32 | 47 | 43 | 48 | 38 | 55 |
| 33 | 52 | 45 | 41 | 49 | 35 | 28 | 31 |

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

1 1 1 1 0 1 0 0

1 0 0 1 0 0 1 1

1 1 0 1 0 0 0 0

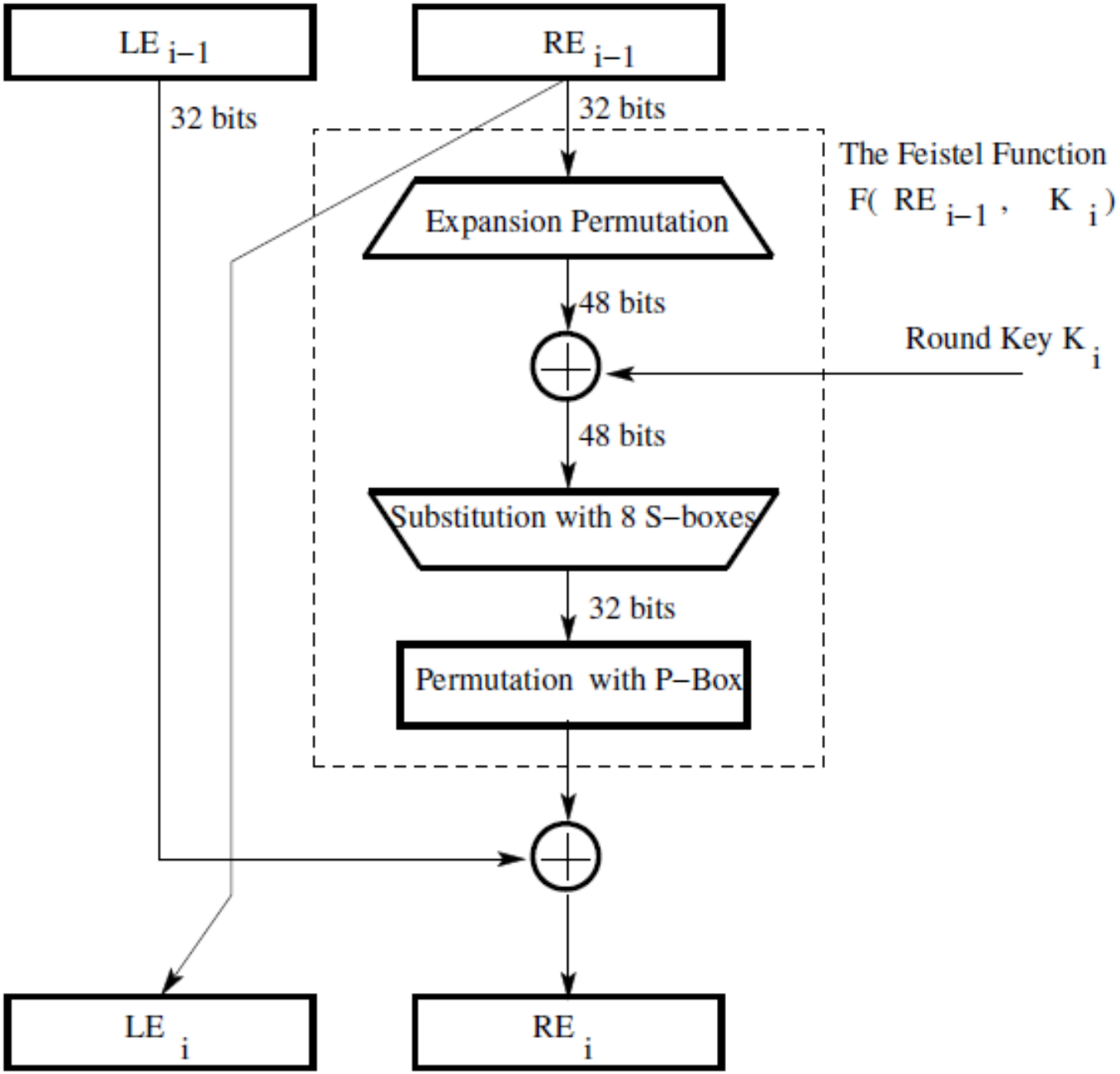
1 1 0 1 0 1 1 1

1 0 0 0 1 0 1 1

1 1 1 1 0 1 0 0

| Key Permutation 2 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 13 | 16 | 10 | 23 | 0 | 4 | 2 | 27 |
| 14 | 5 | 20 | 9 | 22 | 18 | 11 | 3 |
| 25 | 7 | 15 | 6 | 26 | 19 | 12 | 1 |
| 40 | 51 | 30 | 36 | 46 | 54 | 29 | 39 |
| 50 | 44 | 32 | 47 | 43 | 48 | 38 | 55 |

111101001001001111010000110101111000101101110100


LE i−1
RE i−1
32 bits
32 bits
The Feistel Function
F( RE i−1 , K i )
Expansion Permutation
48 bits
Round Key K i
48 bits
Substitution with 8 S−boxes
32 bits
Permutation with P−Box
LE i
RE i

Data:

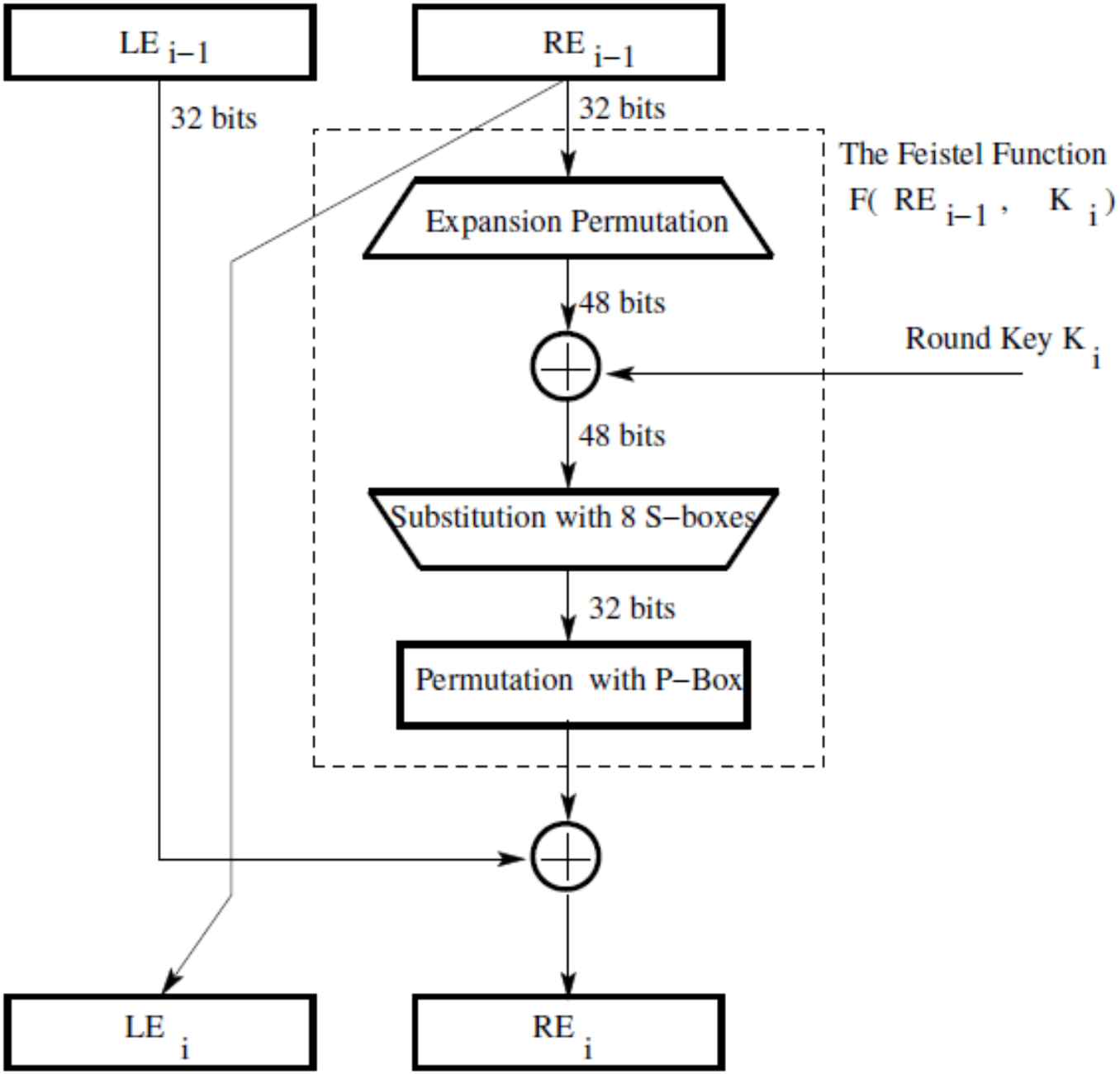
111101001001001111010000110101111000101101110100

Key:

011110100001010101010101011110100001010101010101

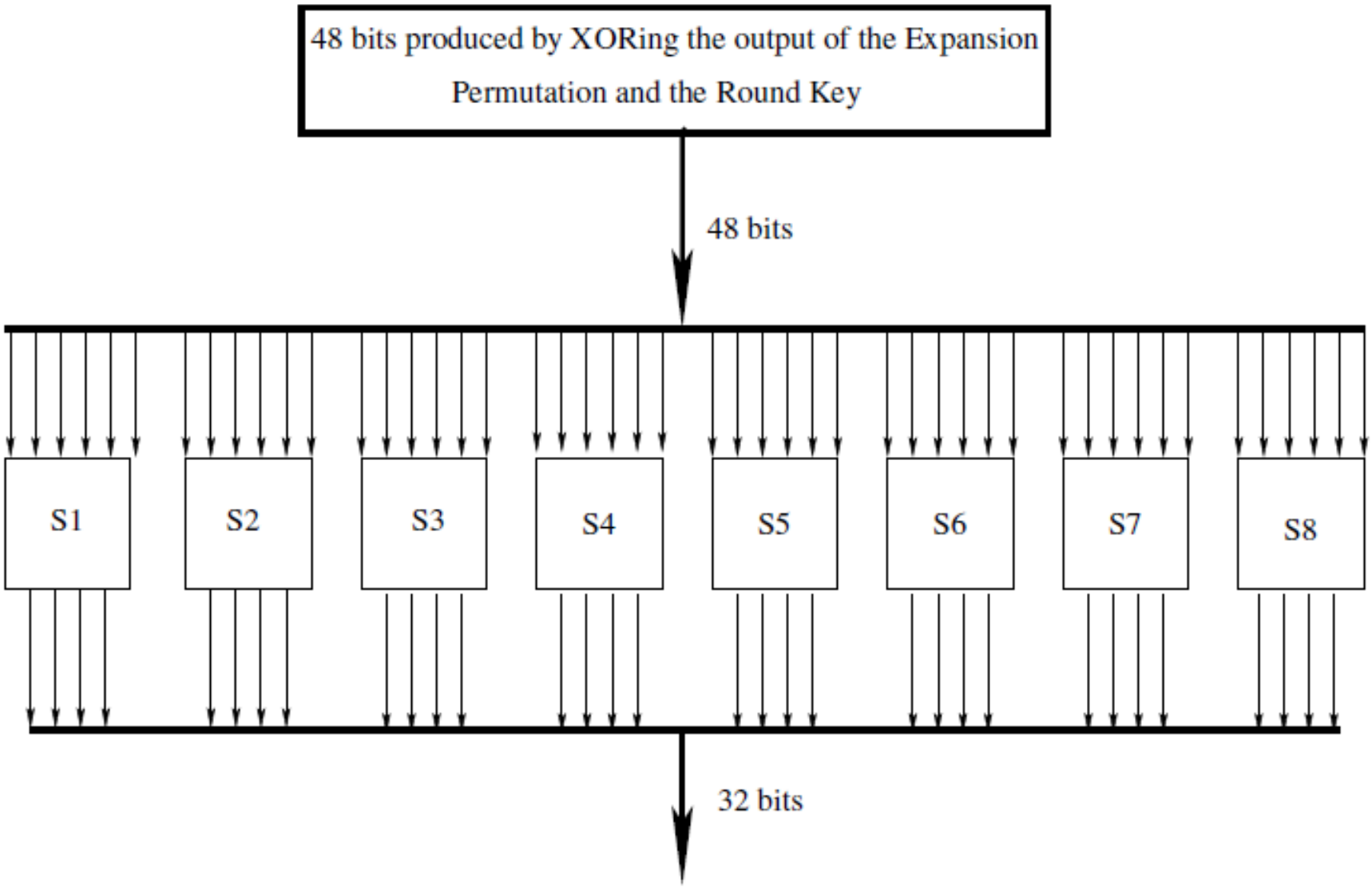
Data XOR Key:

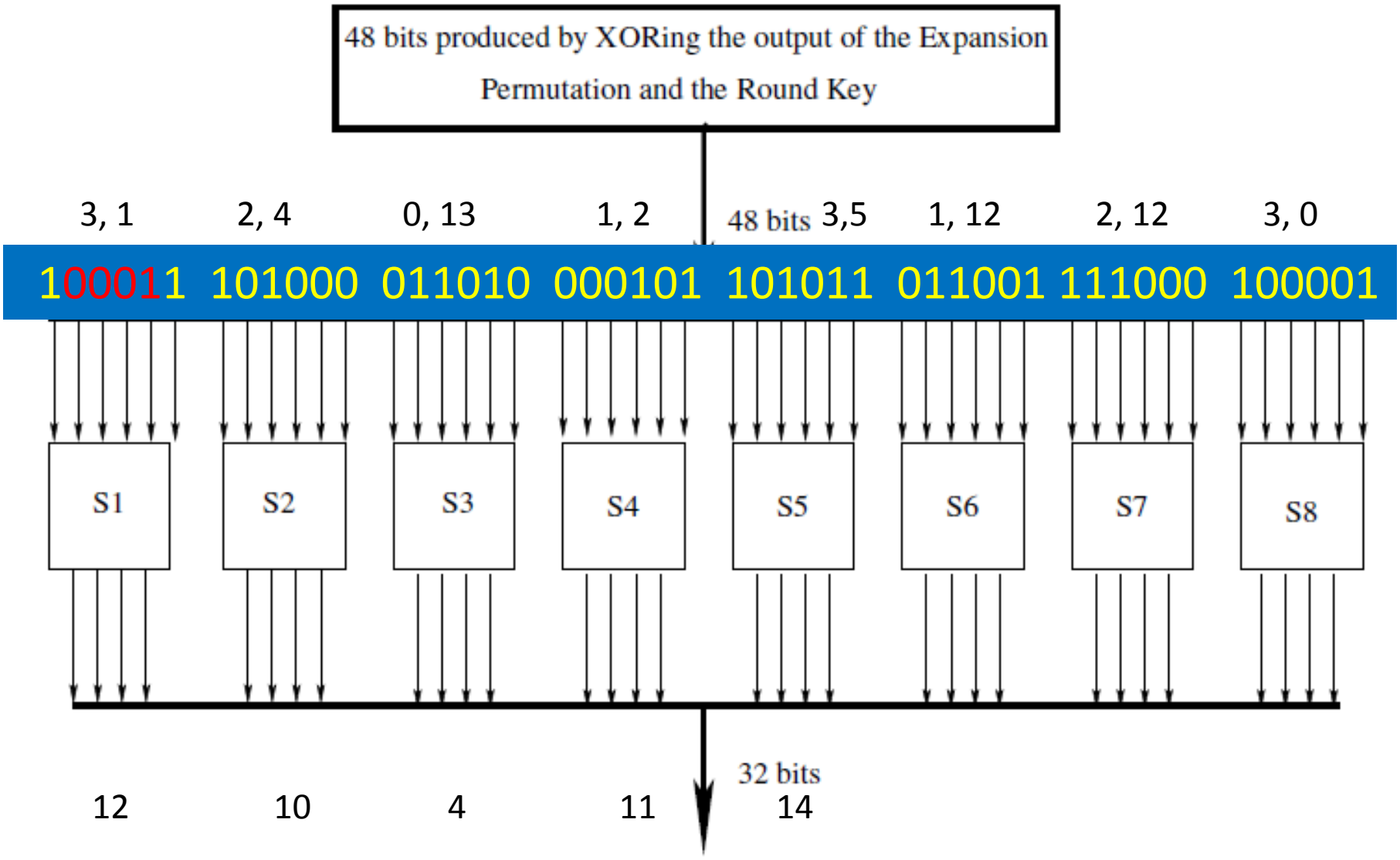
100011101000011010000101101011011001111000100001

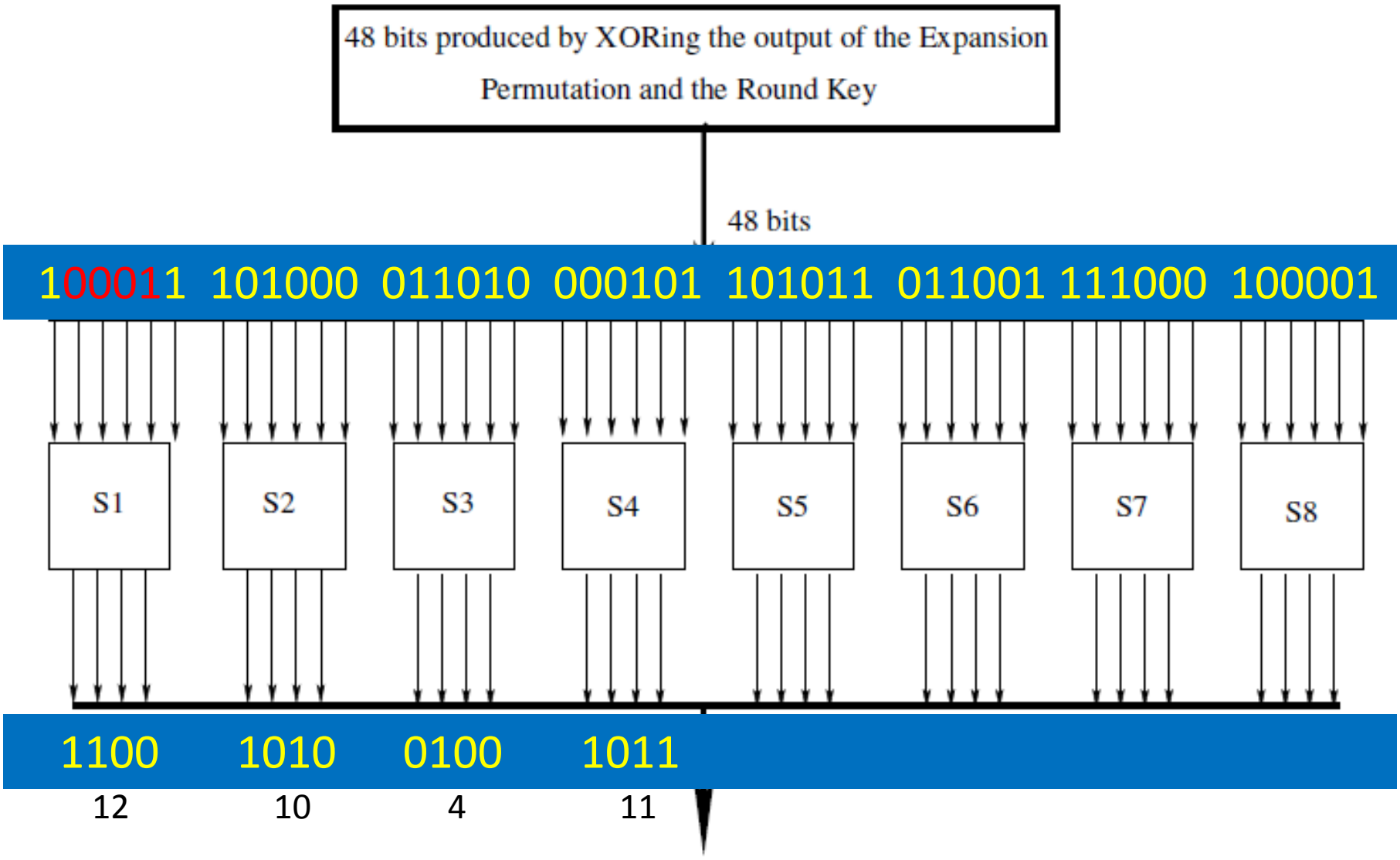

LE i−1
RE i−1
32 bits
32 bits
The Feistel Function
F( RE i−1 , K i )
Expansion Permutation
48 bits
Round Key K i
48 bits
Substitution with 8 S−boxes
32 bits
Permutation with P−Box
LE i
RE i

# The S-Box for the Substitution Step in Each Round

- the 48-bit input word is divided into eight 6-bit words and each 6-bit word fed into a separate S-box. Each S-box produces a 4-bit output.
- Each of the eight S-boxes consists of a 4 × 16 table lookup for an output 4-bit word. The first and the last bit of the 6-bit input word are decoded into one of 4 rows and the middle 4 bits decoded into one of 16 columns for the table lookup.
- The S-boxes were tuned to enhance the resistance of DES to what is known as the differential cryptanalysis attack


48 bits produced by XORing the output of the Expansion Permutation and the Round Key
48 bits
S1
S2
S3
S4
S5
S6
S7
S8
32 bits


48 bits produced by XORing the output of the Expansion Permutation and the Round Key
3, 1
2, 4
0, 13
1, 2
48 bits
3,5
1, 12
2, 12
3, 0
100011 101000 011010 000101 101011 011001 111000 100001
S1
S2
S3
S4
S5
S6
S7
S8
32 bits
12
10
4
11
14


48 bits produced by XORing the output of the Expansion Permutation and the Round Key
48 bits
100011 101000 011010 000101 101011 011001 111000 100001
S1
S2
S3
S4
S5
S6
S7
S8
1100 1010 0100 1011
12 10 4 11

| The $4 \times 16$ substitution table for S-box $S_1$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |
| S-box $S_2$ | | | | | | | | | | | | | | | |
| 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |
| S-box $S_3$ | | | | | | | | | | | | | | | |
| 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |
| S-box $S_4$ | | | | | | | | | | | | | | | |
| 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |

100011 101000 011010 000101 101011 011001 111000 100001

| | | | | | |
|---|---|---|---|---|---|
| 1 | 100011 | 11 | 3 | 12 | 1100 |
| | | 0001 | 1 | | |
| 2 | 101000 | 10 | 2 | 10 | 1010 |
| | | 0100 | 4 | | |
| 3 | 011010 | 00 | 0 | 4 | 0100 |
| | | 1101 | 13 | | |
| 4 | 000101 | 01 | 1 | 11 | 1011 |
| | | 0010 | 2 | | |
| 5 | 101011 | 11 | 3 | 14 | 1110 |
| | | 0101 | 5 | | |
| 6 | 011001 | 01 | 1 | 0 | 0000 |
| | | 1100 | 12 | | |
| 7 | 111000 | 10 | 2 | 0 | 0000 |
| | | 1100 | 12 | | |
| 8 | 100001 | 11 | 3 | 2 | 0010 |
| | | 0000 | 0 | | |

| S-box $S_5$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |

| S-box $S_6$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |

| S-box $S_7$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |

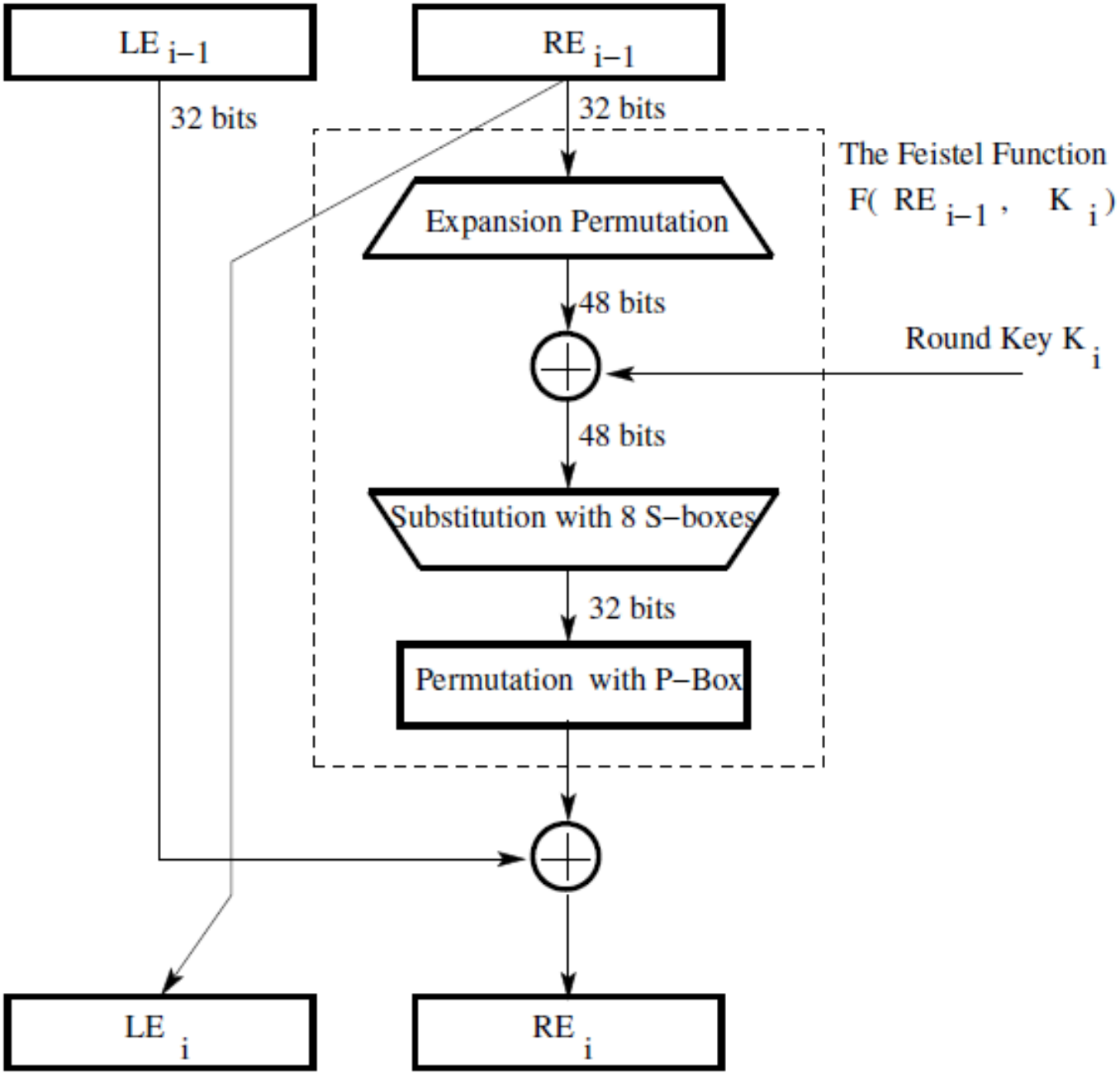
| S-box $S_8$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

100011 101000 011010 000101 101011 011001 111000 100001

| | | | | | |
|---|---|---|---|---|---|
| 1 | 100011 | 11 | 3 | 12 | 1100 |
| | | 0001 | 1 | | |
| 2 | 101000 | 10 | 2 | 10 | 1010 |
| | | 0100 | 4 | | |
| 3 | 011010 | 00 | 0 | 4 | 0100 |
| | | 1101 | 13 | | |
| 4 | 000101 | 01 | 1 | 11 | 1011 |
| | | 0010 | 2 | | |
| 5 | 101011 | 11 | 3 | 14 | 1110 |
| | | 0101 | 5 | | |
| 6 | 011001 | 01 | 1 | 0 | 0000 |
| | | 1100 | 12 | | |
| 7 | 111000 | 10 | 2 | 0 | 0000 |
| | | 1100 | 12 | | |
| 8 | 100001 | 11 | 3 | 2 | 0010 |
| | | 0000 | 0 | | |

| | | | | | |
|---|---|---|---|---|---|
| 1 | 100011 | 11 | 3 | 12 | 1100 |
| | | 0001 | 1 | | |
| 2 | 101000 | 10 | 2 | 10 | 1010 |
| | | 0100 | 4 | | |
| 3 | 011010 | 00 | 0 | 4 | 0100 |
| | | 1101 | 13 | | |
| 4 | 000101 | 01 | 1 | 11 | 1011 |
| | | 0010 | 2 | | |
| 5 | 101011 | 11 | 3 | 14 | 1110 |
| | | 0101 | 5 | | |
| 6 | 011001 | 01 | 1 | 0 | 0000 |
| | | 1100 | 12 | | |
| 7 | 111000 | 10 | 2 | 0 | 0000 |
| | | 1100 | 12 | | |
| 8 | 100001 | 11 | 3 | 2 | 0010 |
| | | 0000 | 0 | | |

1100 1010 0100 1011 1110 0000 0000 0010


LE i−1
RE i−1
32 bits
32 bits
The Feistel Function
F( RE i−1 , K i )
Expansion Permutation
48 bits
Round Key K i
48 bits
Substitution with 8 S−boxes
32 bits
Permutation with P−Box
LE i
RE i

# Permutation with P-Box

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

1100 1010 0100 1011 1110 0000 0000 0010

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

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

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

1100 1010 0100 1011 1110 0000 0000 0010

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

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

1100

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

1100 1010 0100 1011 1110 0000 0000 0010

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

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

1100 0001

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

1100 1010 0100 1011 1110 0000 0000 0010

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

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

1100 0001
1100 1111

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

1100 1010 0100 1011 1110 0000 0000 0010

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

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

1100 0001
1100 1111
1000 0000

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

1100 1010 0100 1011 1110 0000 0000 0010

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

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

1100 0001
1100 1111
1000 0000
1100 0000

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