National Institute of Technology, Warangal

(*Department of Computer Science Engineering*)

Symmetric Key Cryptography

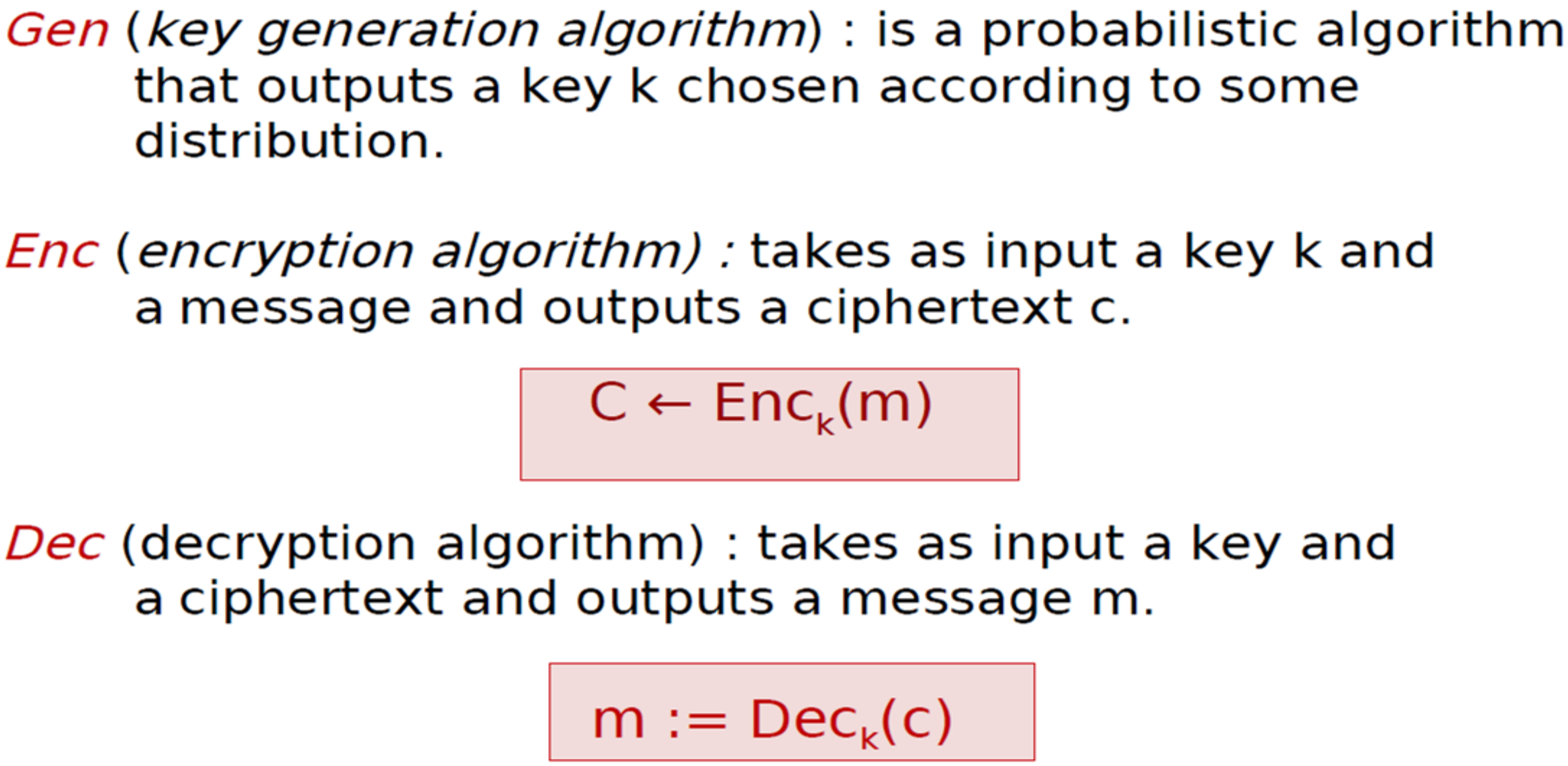
Lecture By:-

Dr R Padmavathy

Dept of CSE, NIT Warangal

Cryptographic Algorithm

Any encrpytion scheme(Gen, Enc, Dec) is defined by three algorithms:



Gen (*key generation algorithm*) : is a probabilistic algorithm that outputs a key k chosen according to some distribution.

Enc (*encryption algorithm) :* takes as input a key k and a message and outputs a ciphertext c.

$$\boxed{C \leftarrow \mathrm{Enc}_k(m)}$$

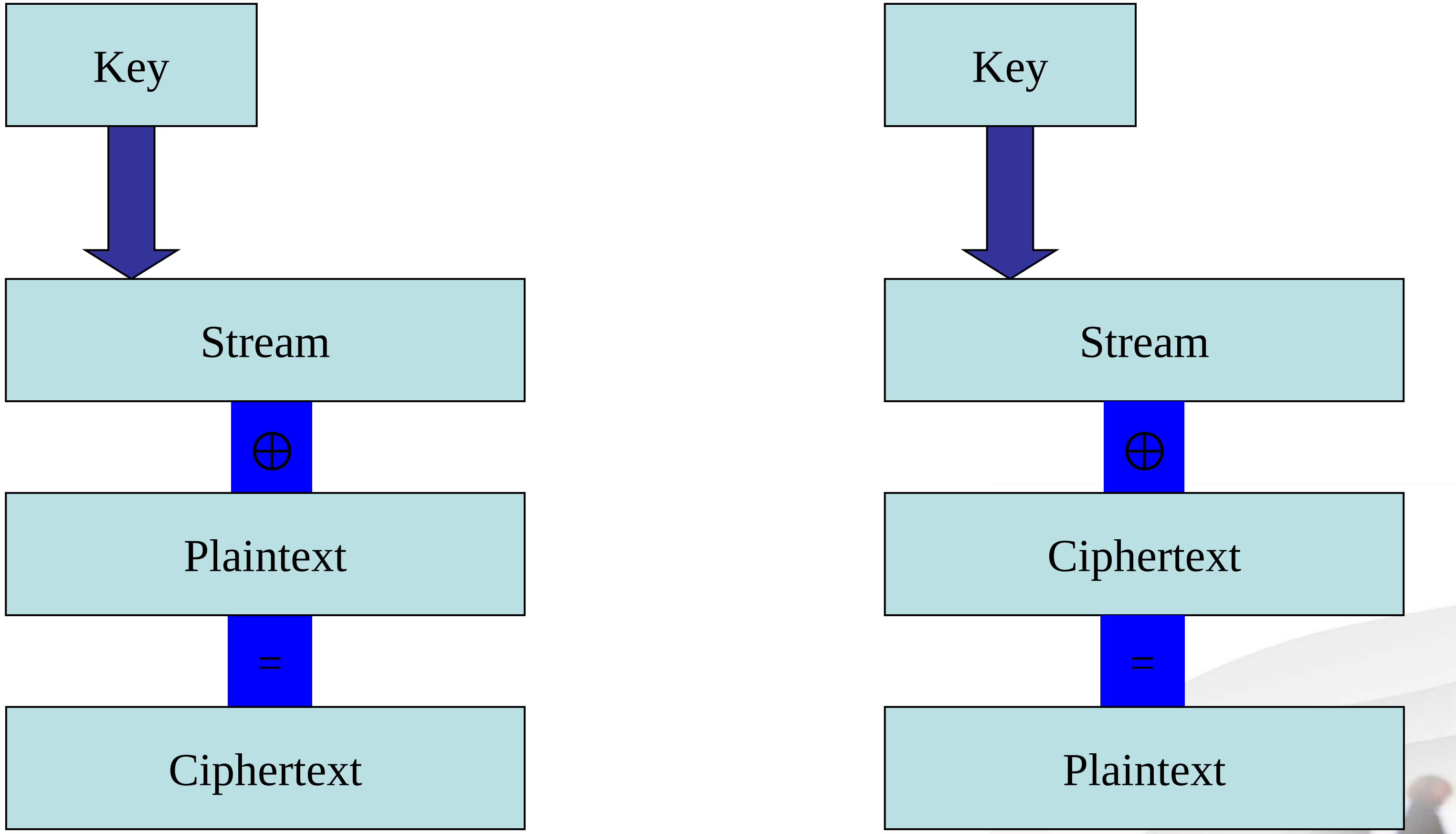
Dec (decryption algorithm) : takes as input a key and a ciphertext and outputs a message m.

$$\boxed{m := \mathrm{Dec}_k(c)}$$

Stream Ciphers

- Start with a secret key (“seed”)
- Generate a keying stream
- *i*-th bit/byte of keying stream is a function of the key and the first *i*-1 ciphertext bits.
- Combine the stream with the plaintext to produce the ciphertext (typically by XOR)
- **Examples** are
  - A5 – encrypting GSM handset to base station communication
  - RC-4 (Ron’s Code)

Example of Stream Encryption



Key

Stream

⊕

Plaintext

=

Ciphertext

Key

Stream

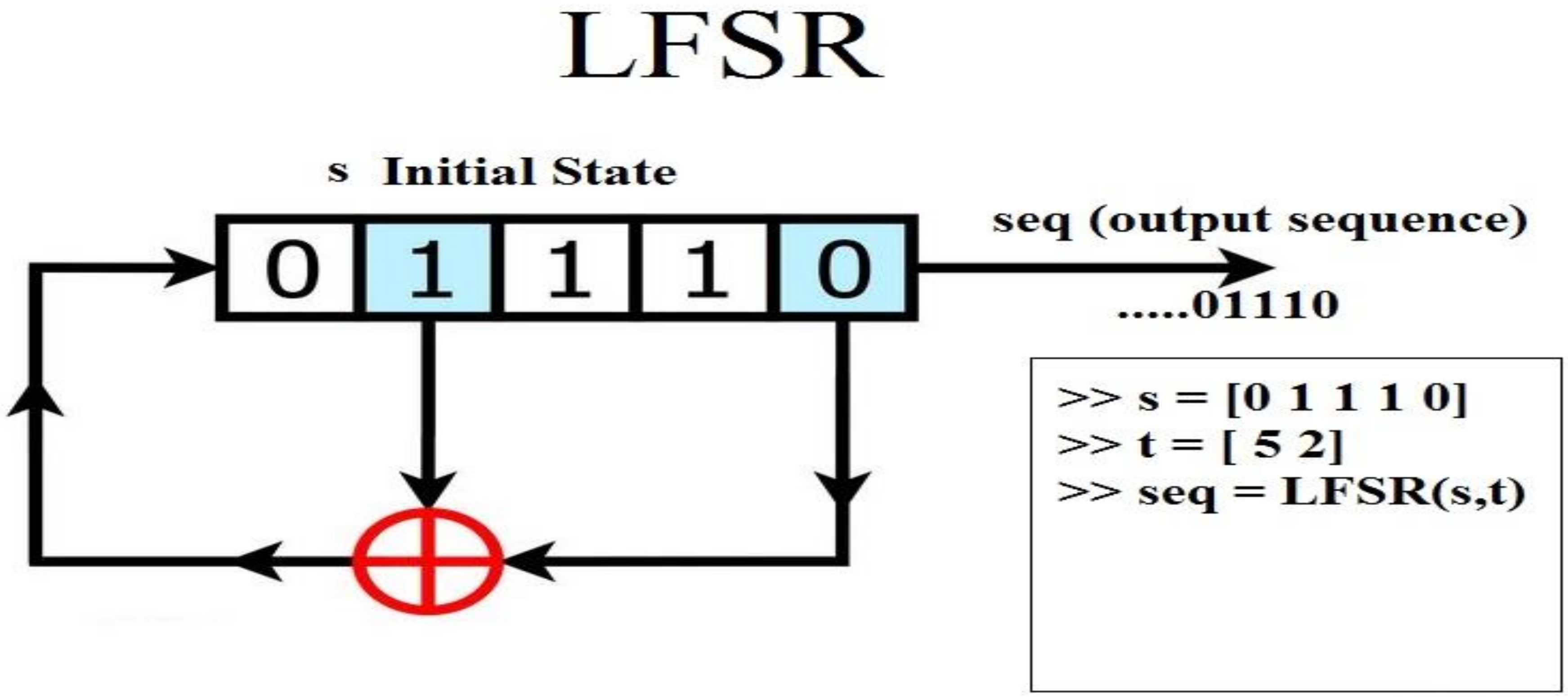
⊕

Ciphertext

=

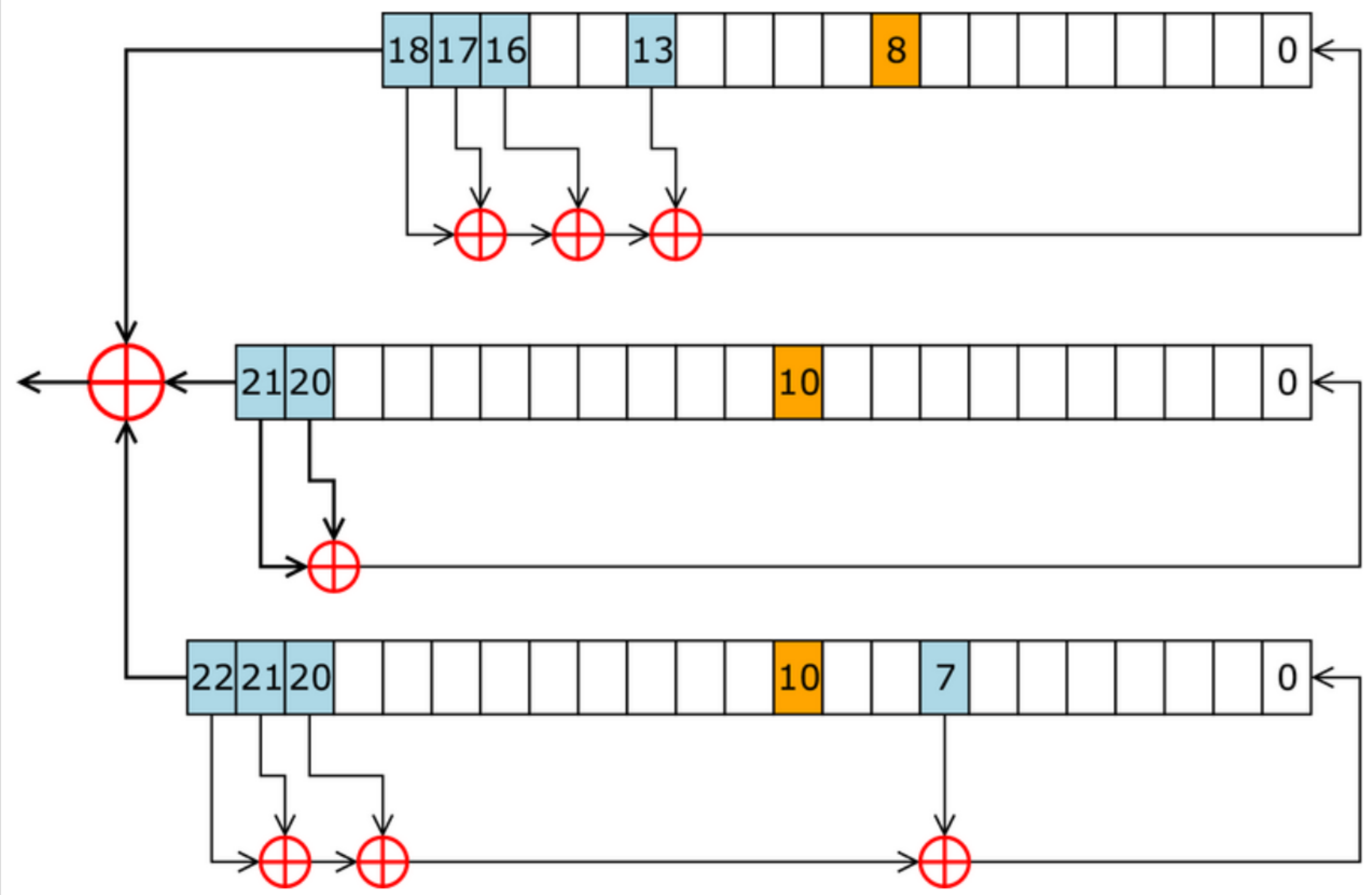
Plaintext

Linear Feedback Shift Register

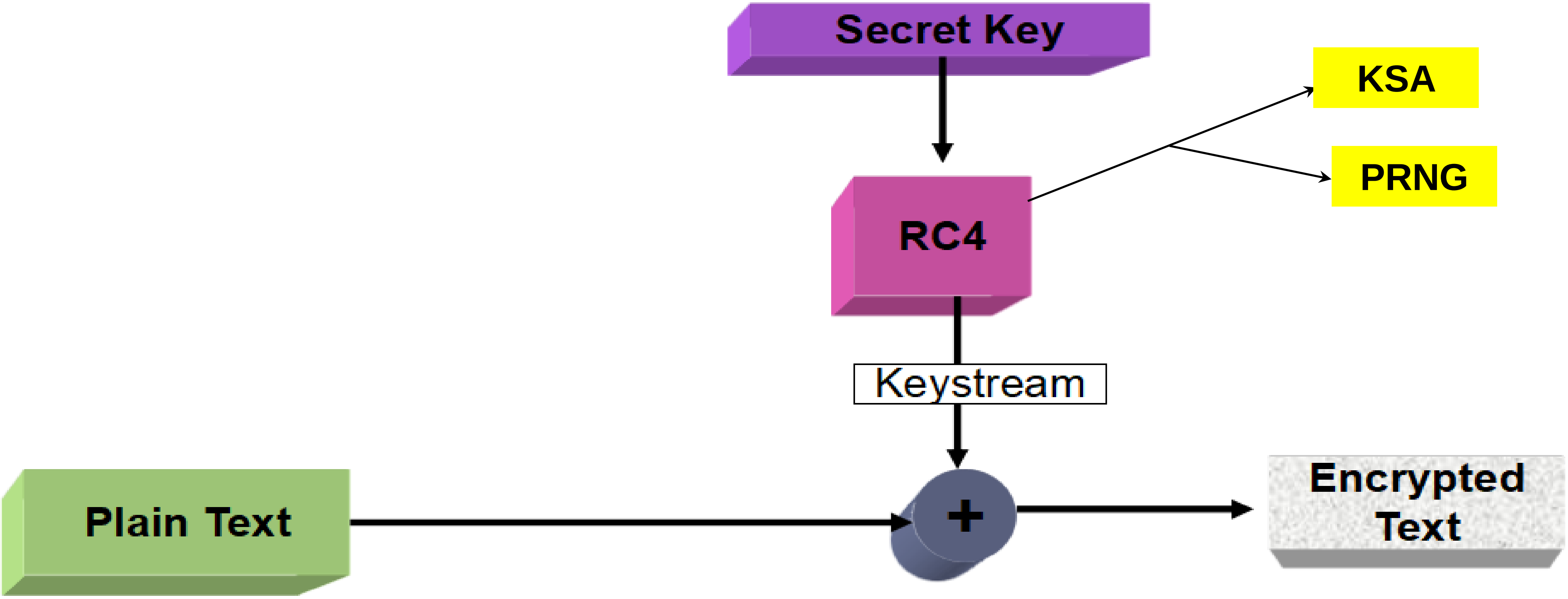


```
>> s = [0 1 1 1 0]
>> t = [ 5 2]
>> seq = LFSR(s,t)
```

A5/1 Algorithm



RC4 Algorithm

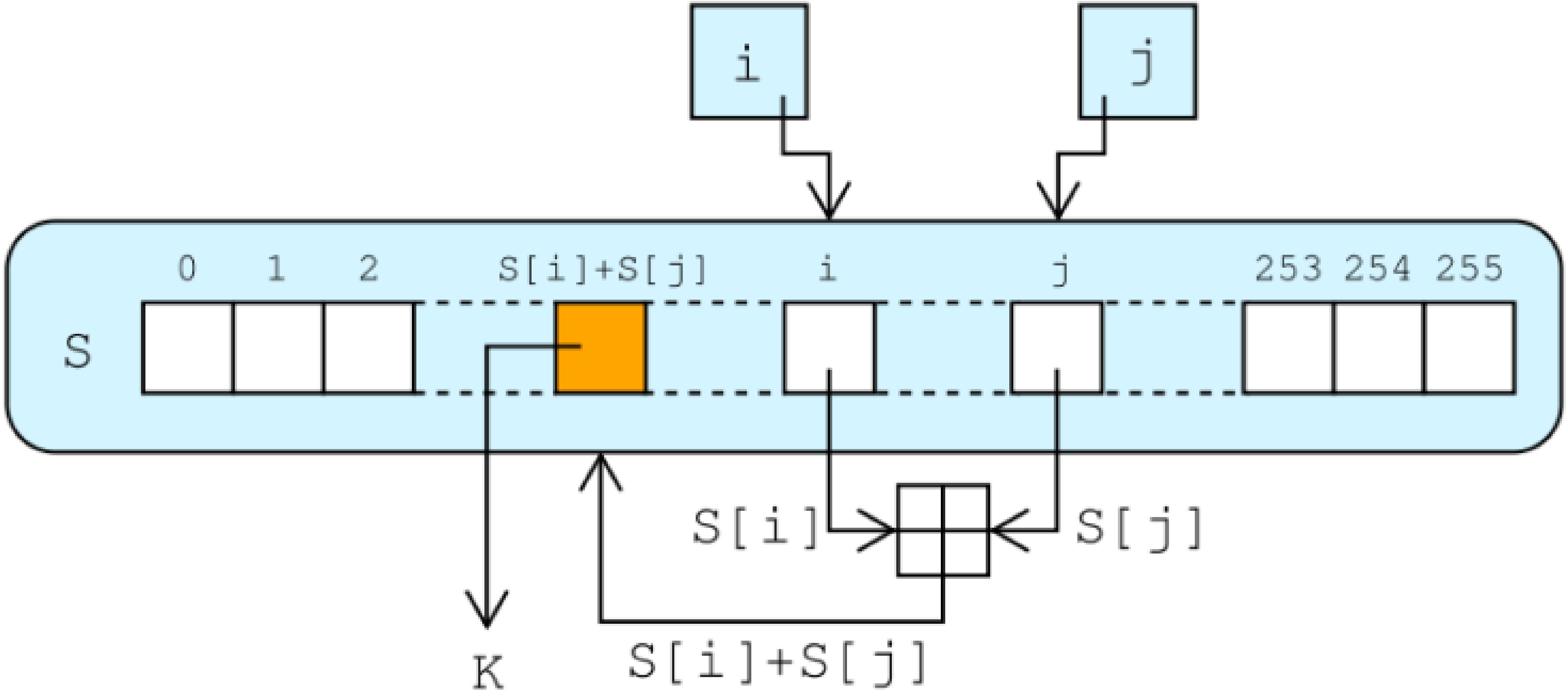


RC4 - KSA

Key Scheduling Algorithm

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

RC4 - PRNG



RC4 Usage

- WEP
- WPA default
- Bit Torrent Protocol Encryption
- Microsoft Point-to-Point Encryption
- SSL (optionally)
- SSH (optionally)
- Remote Desktop Protocol
- Kerberos (optionally)

Block Ciphers

- Encrypt a block of input to a block of output
- Typically, the two blocks are of the same length
- Most symmetric key systems block size is 64
- In AES block size is 128
- Different modes for encrypting plaintext longer than a block.
- Examples include DES, 3-DES, AES, RC-2, RC-5, IDEA, Blowfish etc.

DES Algorihtm

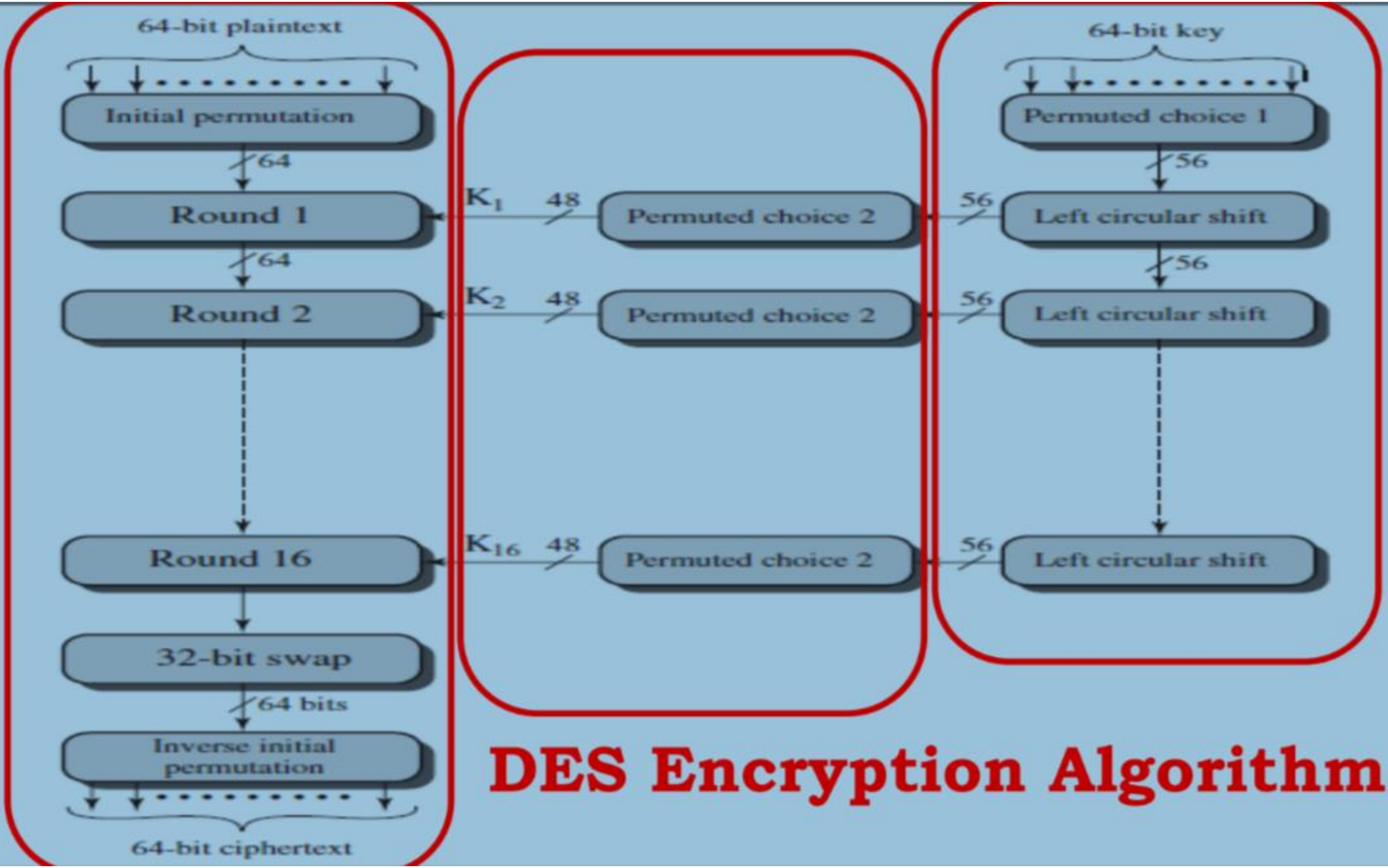
❖ DES is a Block Cipher;

✓ It encrypts plaintext in 64-bit blocks ; The plaintext must be 64 bits in length

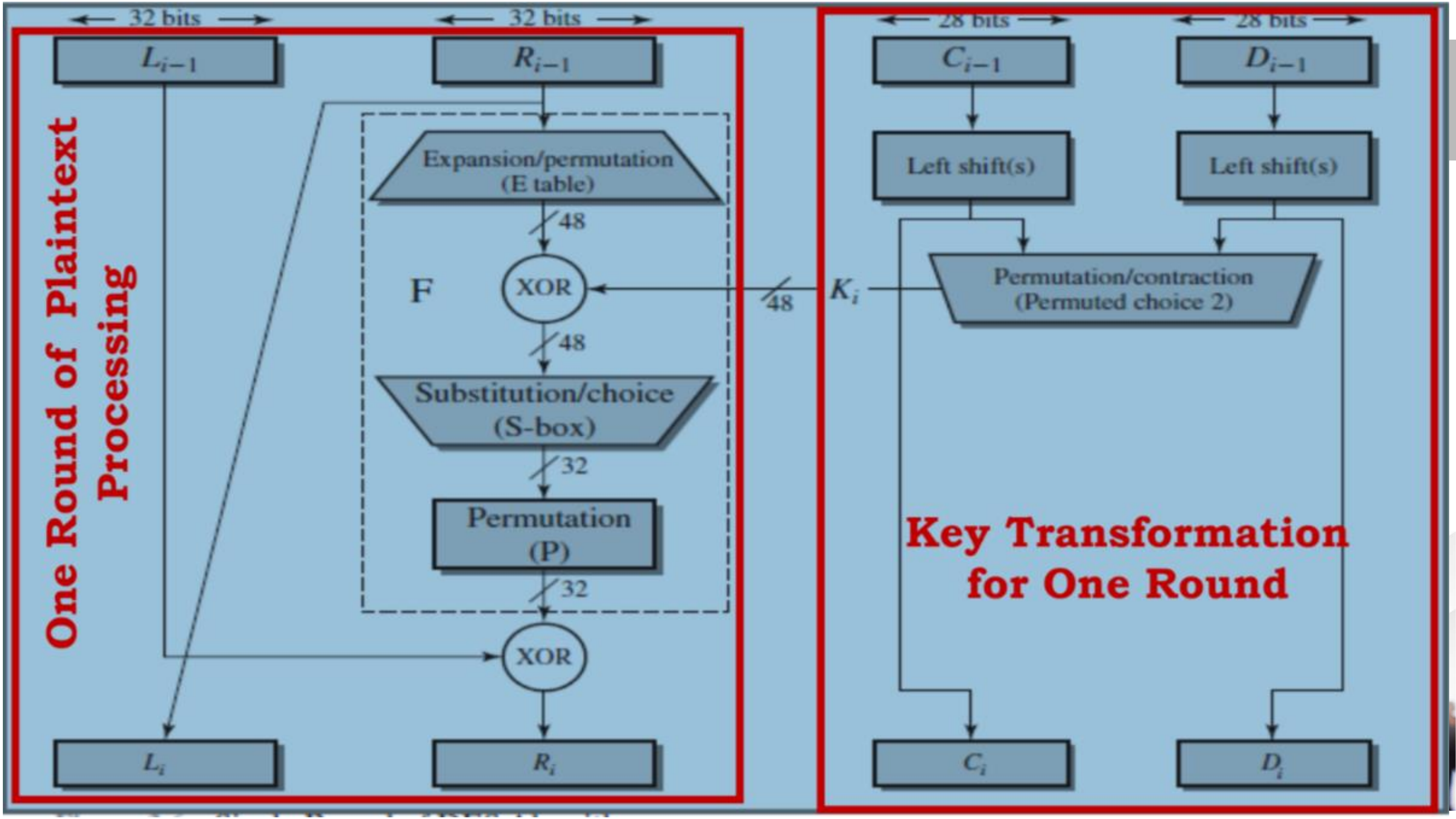
✓ The key is 56 bits in length.

❖ DES is a symmetric algorithm;

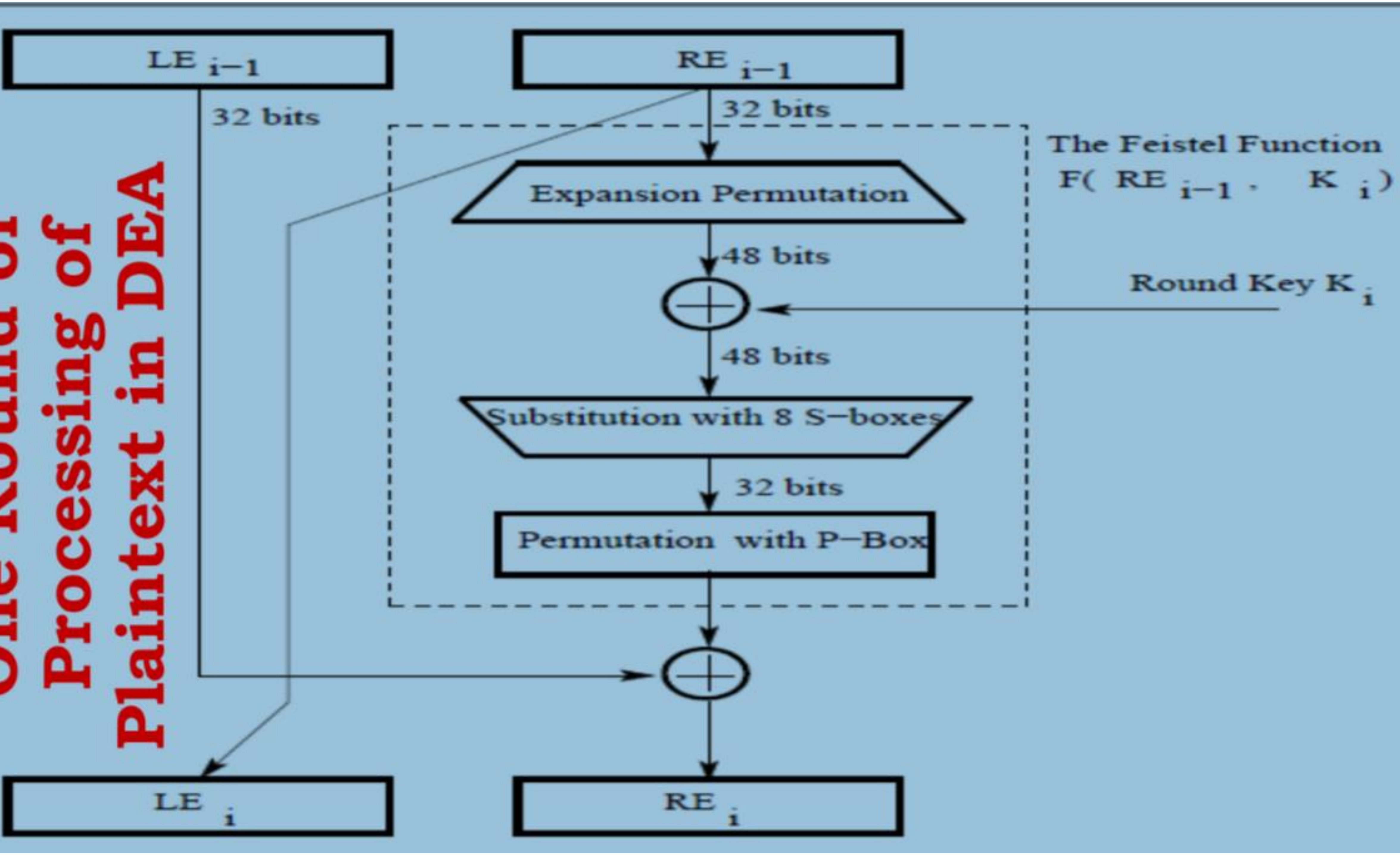
✓ The same algorithm and key are used for both encryption and decryption

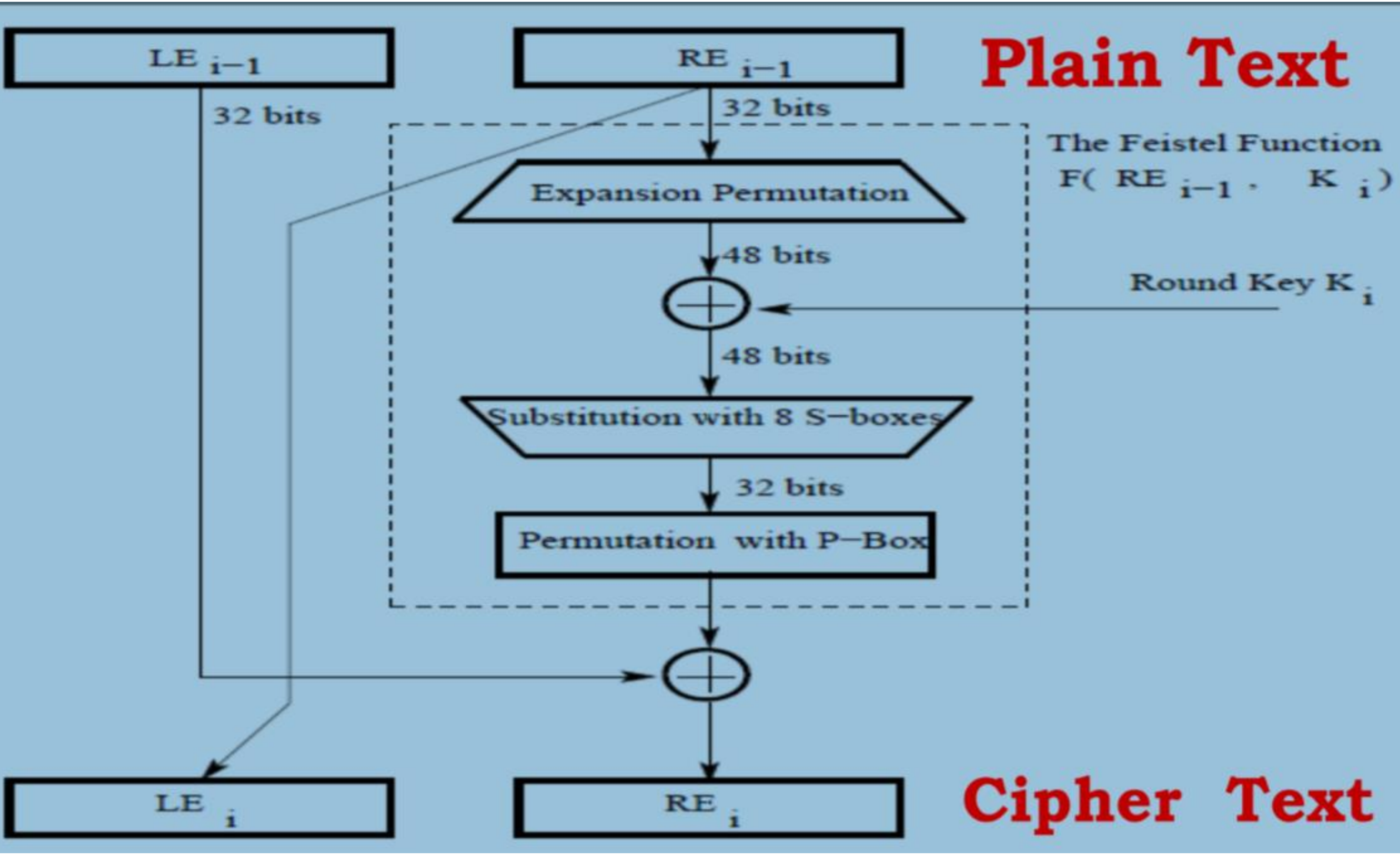


DES Encryption Algorithm


One Round of Plaintext Processing
32 bits
32 bits
L_{i-1}
R_{i-1}
Expansion/permutation (E table)
48
F
XOR
48
48
K_i
Substitution/choice (S-box)
32
Permutation (P)
32
XOR
L_i
R_i
28 bits
28 bits
C_{i-1}
D_{i-1}
Left shift(s)
Left shift(s)
Permutation/contraction (Permuted choice 2)
Key Transformation for One Round
C_i
D_i

One Round of Processing of Plaintext in DEA





Plain Text

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

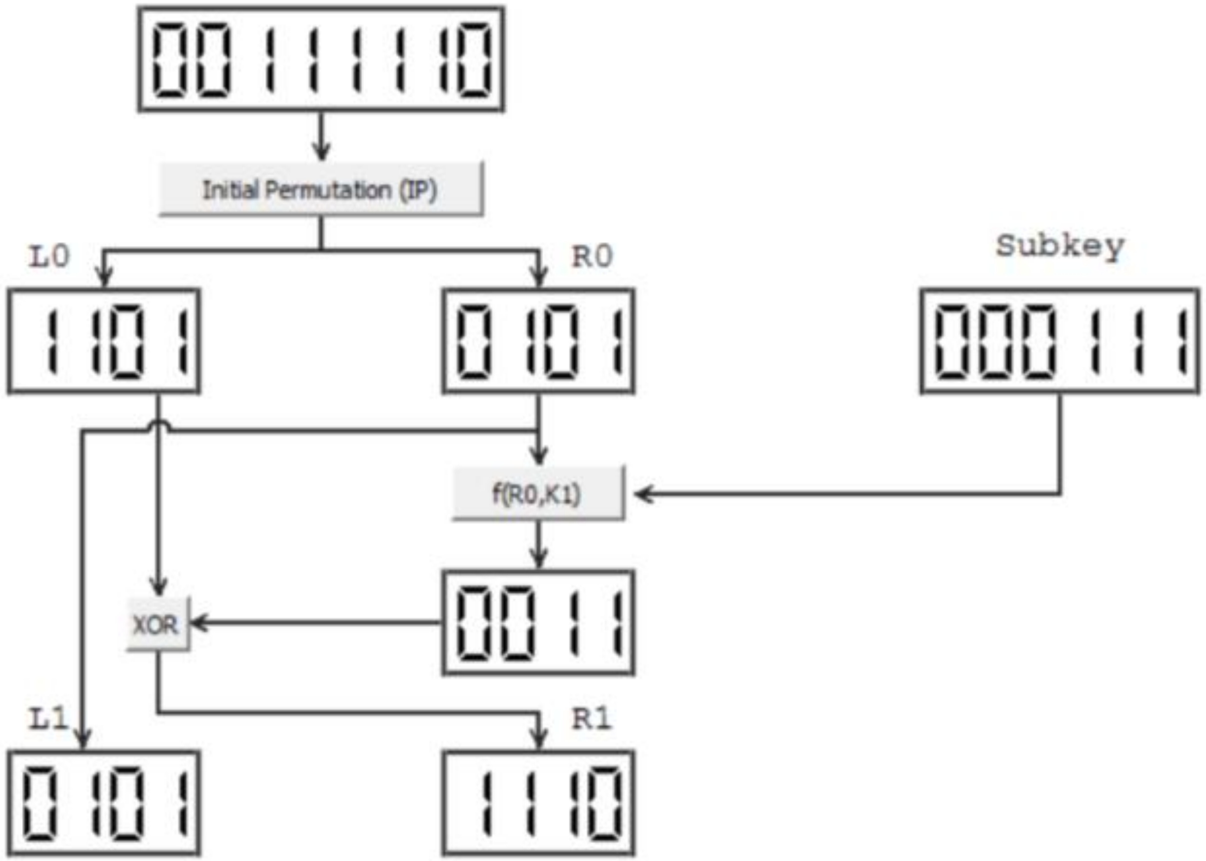
LE_i

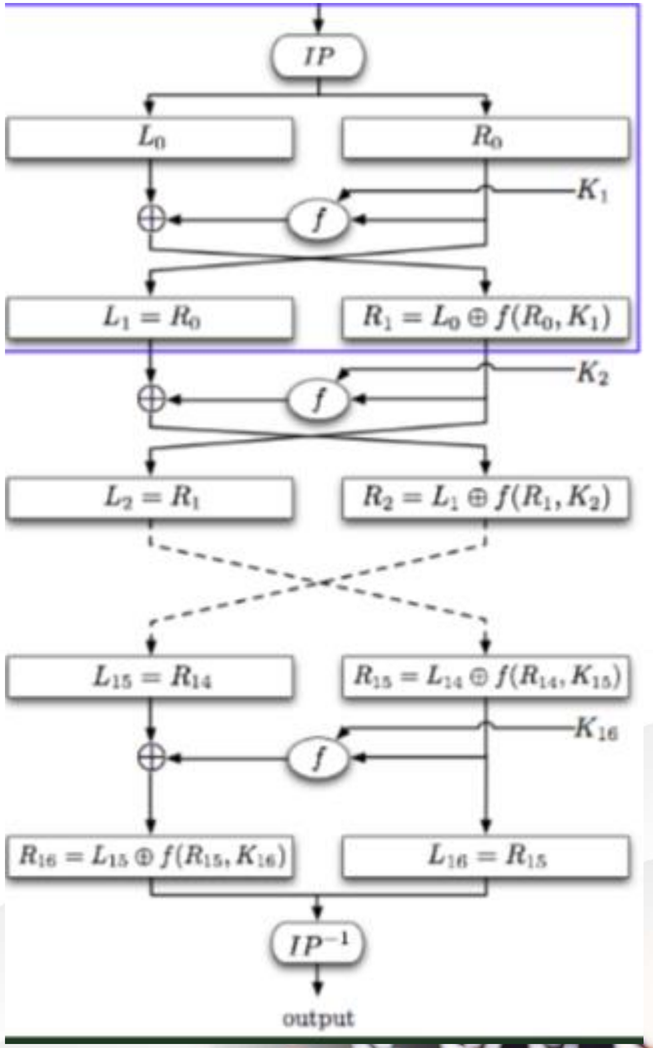
RE_i

Cipher Text

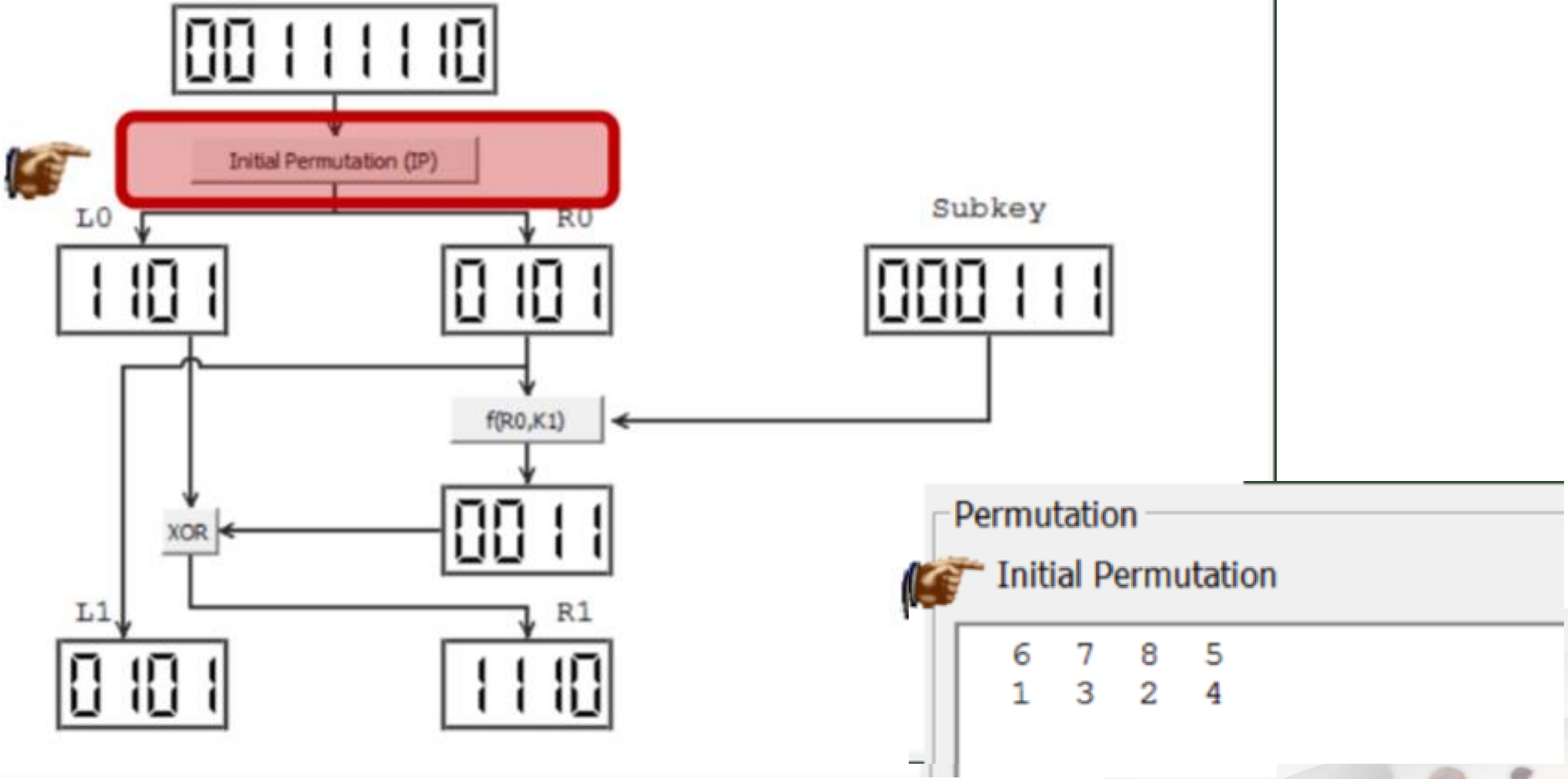
DES Encryption

DES Example(8-Bit)
Plain Text: 64 ; Key: 7




IP
L_0
R_0
K_1
f
$L_1 = R_0$
$R_1 = L_0 \oplus f(R_0, K_1)$
K_2
f
$L_2 = R_1$
$R_2 = L_1 \oplus f(R_1, K_2)$
$L_{15} = R_{14}$
$R_{15} = L_{14} \oplus f(R_{14}, K_{15})$
K_{16}
f
$R_{16} = L_{15} \oplus f(R_{15}, K_{16})$
$L_{16} = R_{15}$
IP^{-1}
output

Initial Permutation

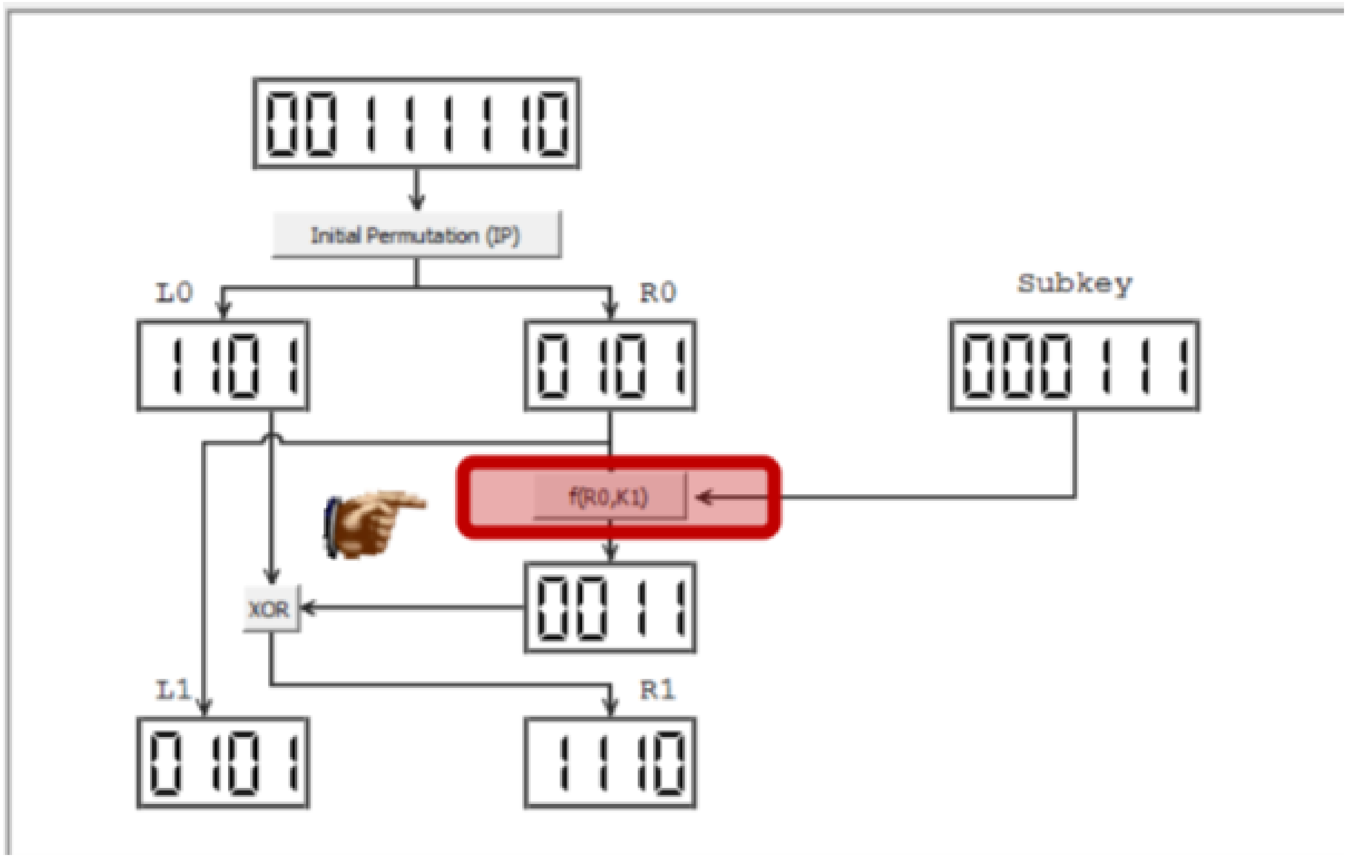


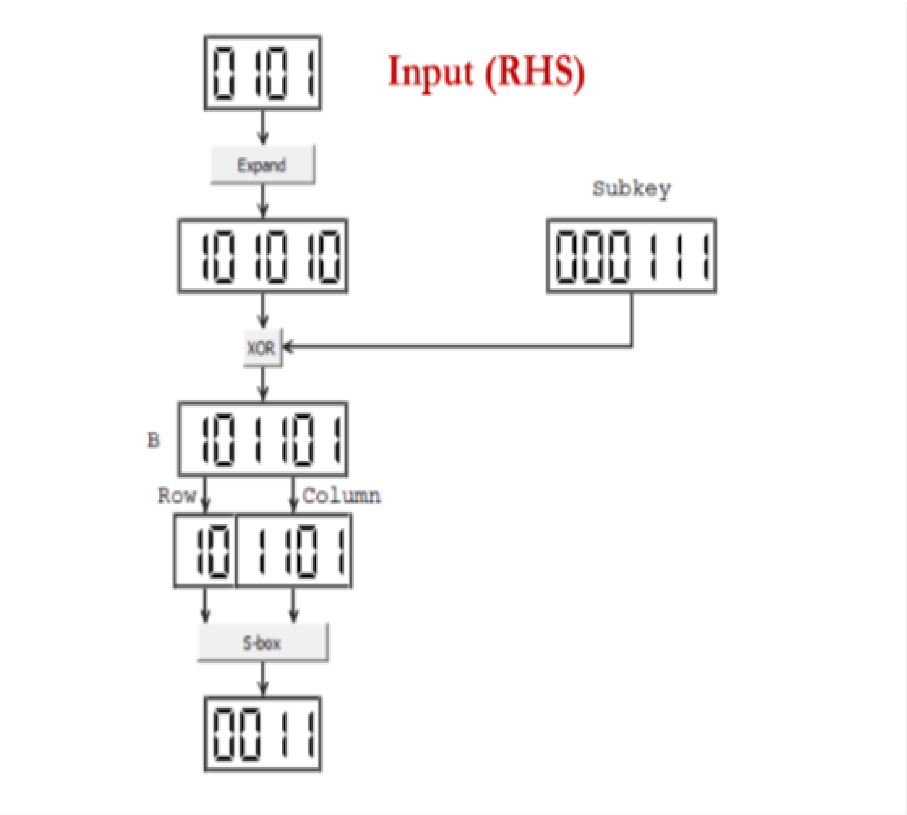
Permutation

Initial Permutation

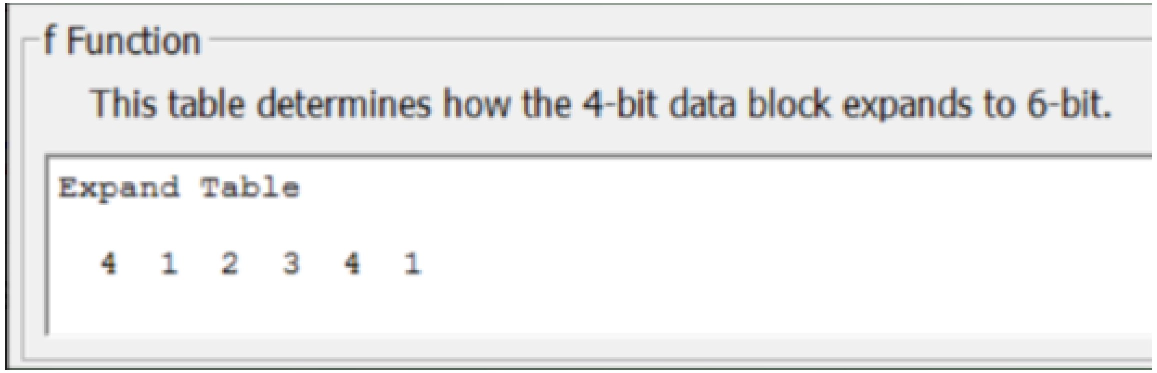
```
6   7   8   5
1   3   2   4
```

Function: F(R0,K1)





Function: Expand

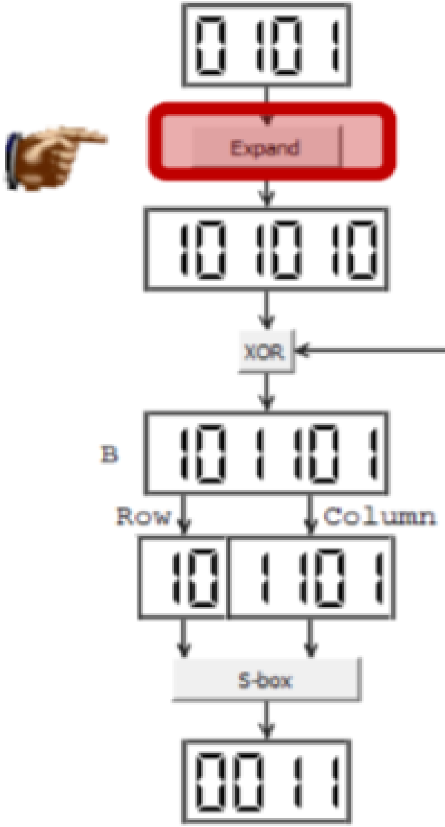


f Function

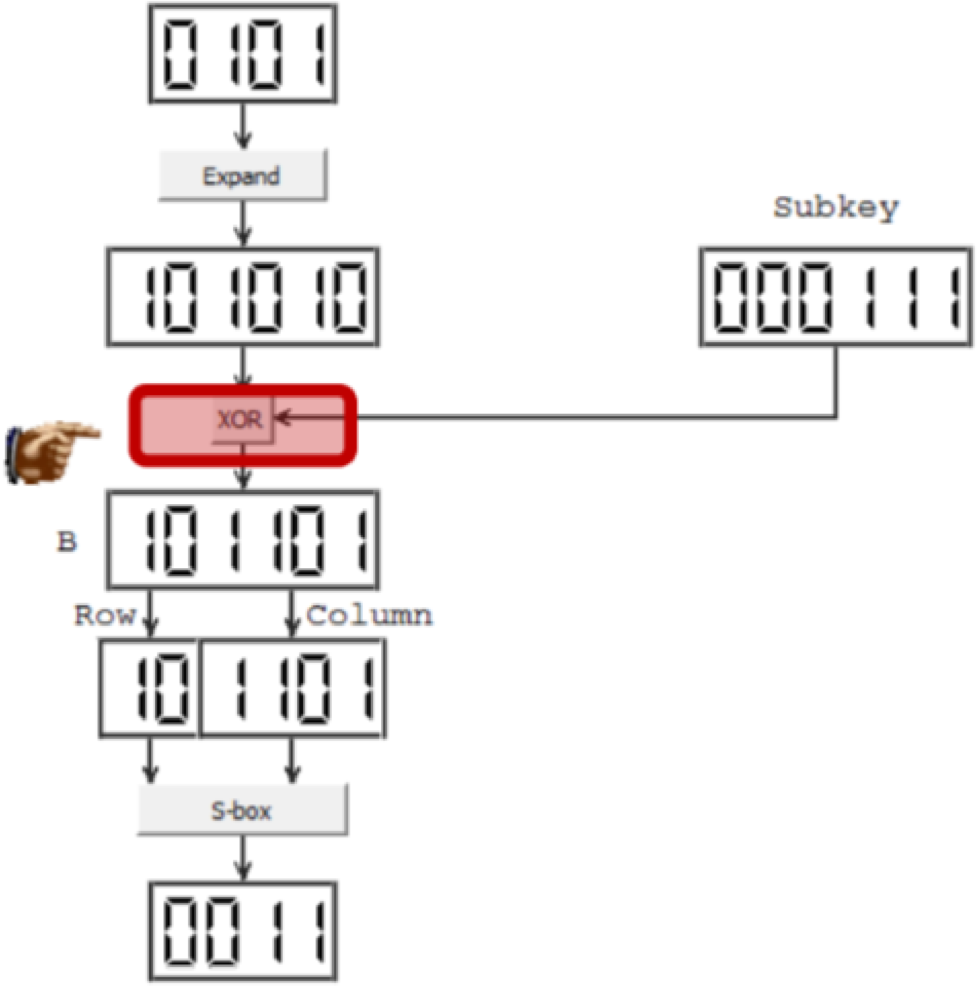
This table determines how the 4-bit data block expands to 6-bit.

```
Expand Table

  4  1  2  3  4  1
```

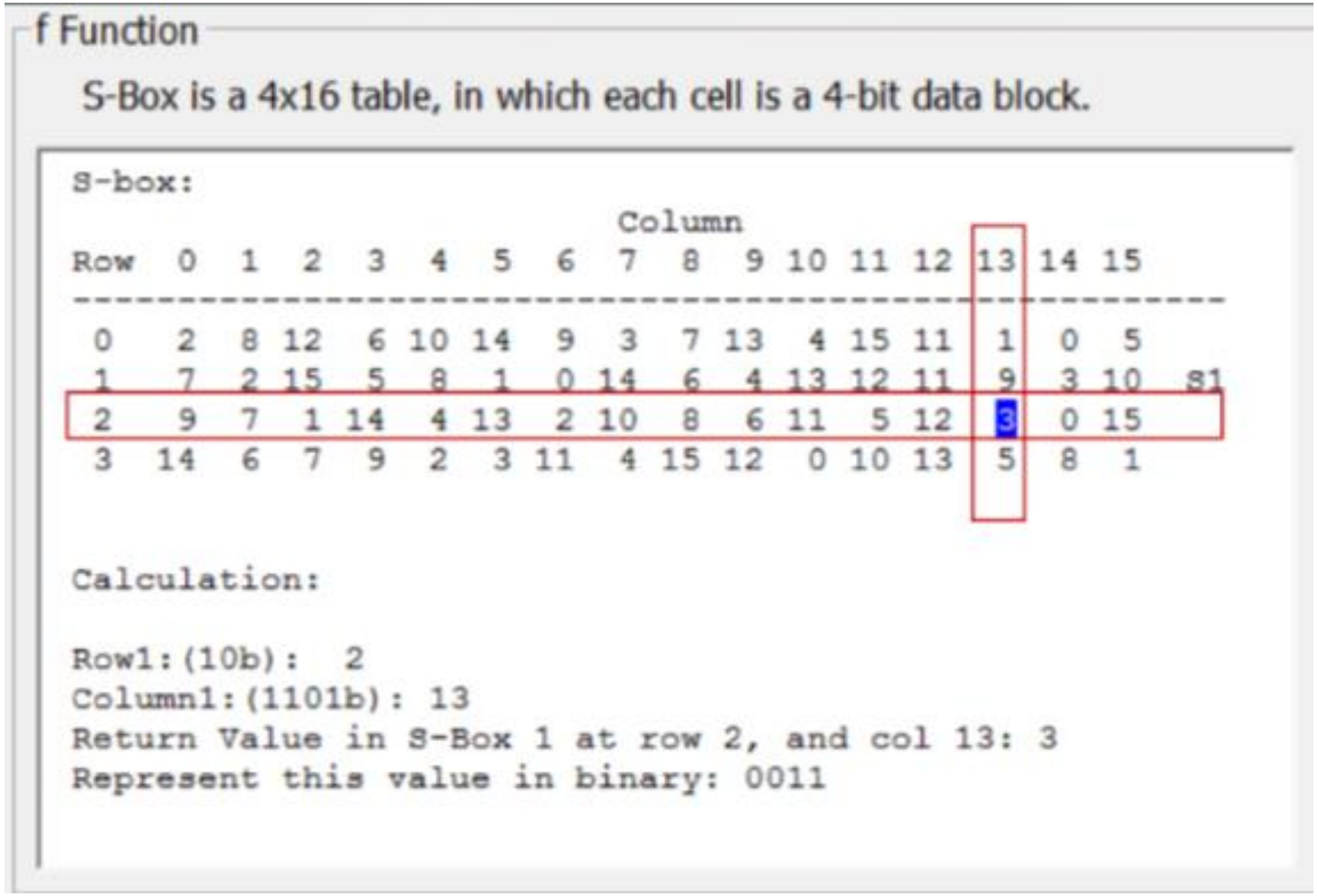


XOR



0101
Expand
101010
Subkey
000111
XOR
B
101101
Row
Column
10
1101
S-box
0011

Function S-Box



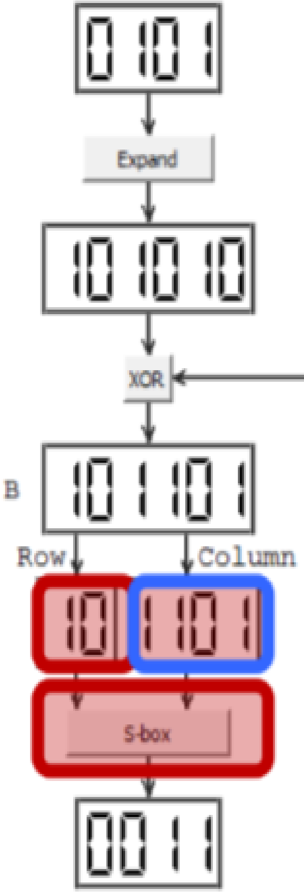
f Function

S-Box is a 4x16 table, in which each cell is a 4-bit data block.

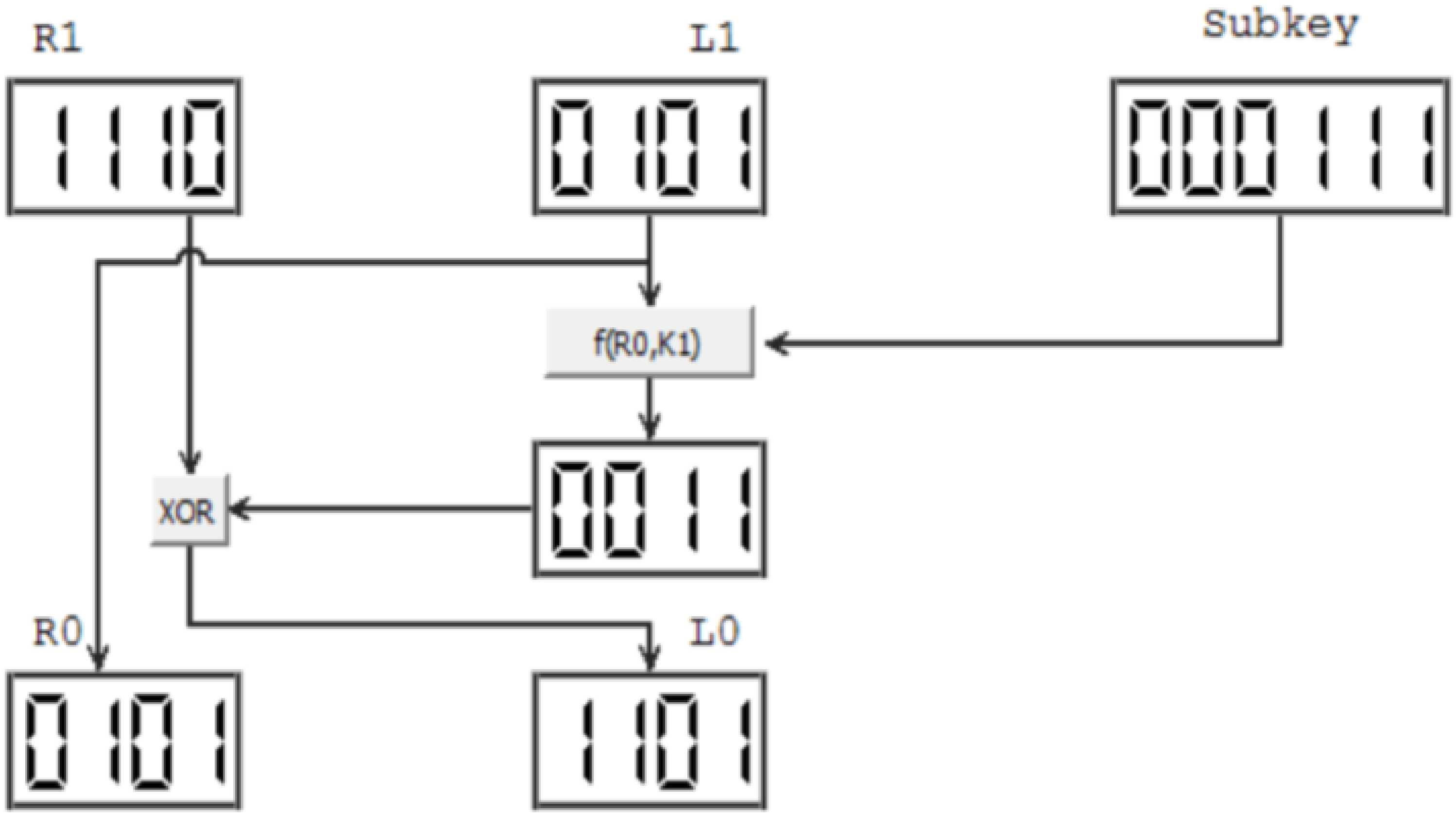
```
S-box:
                              Column
Row   0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
-------------------------------------------------------
 0    2  8 12  6 10 14  9  3  7 13  4 15 11  1  0  5
 1    7  2 15  5  8  1  0 14  6  4 13 12 11  9  3 10    S1
 2    9  7  1 14  4 13  2 10  8  6 11  5 12  3  0 15
 3   14  6  7  9  2  3 11  4 15 12  0 10 13  5  8  1


Calculation:

Row1:(10b):   2
Column1:(1101b): 13
Return Value in S-Box 1 at row 2, and col 13: 3
Represent this value in binary: 0011
```



DES Decryption



Block Ciphers - Modes of Operation :

✓ Electronic Codebook (ECB) Mode

✓ Cipher Block Chaining (CBC) Mode

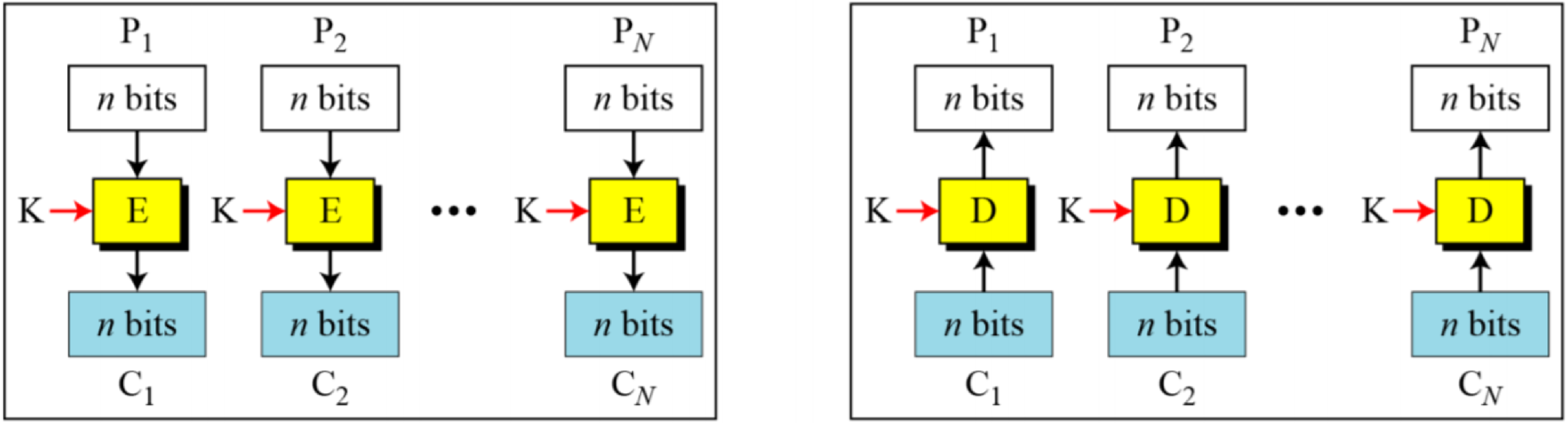
✓ Cipher Feedback (CFB) Mode

✓ Output Feedback (OFB) Mode

✓ Counter (CTR) Mode

Electronic Codebook (ECB) Mode

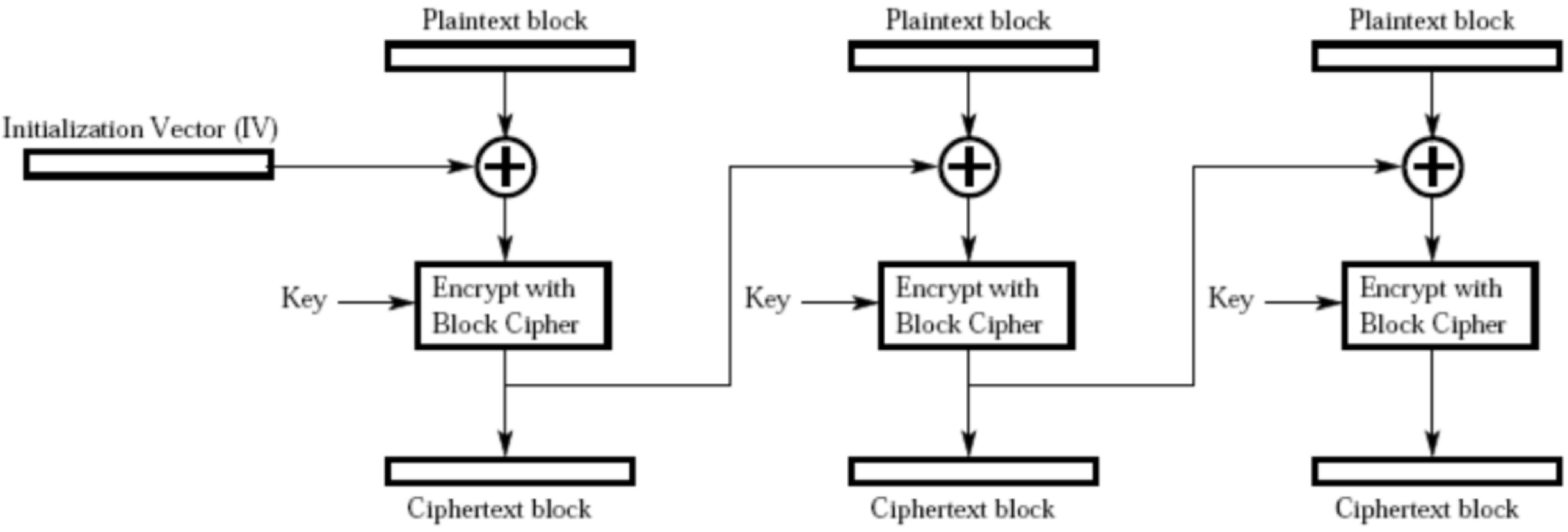
E: Encryption
D: Decryption
P_i: Plaintext block *i*
C_i: Ciphertext block *i*
K: Secret key



Encryption

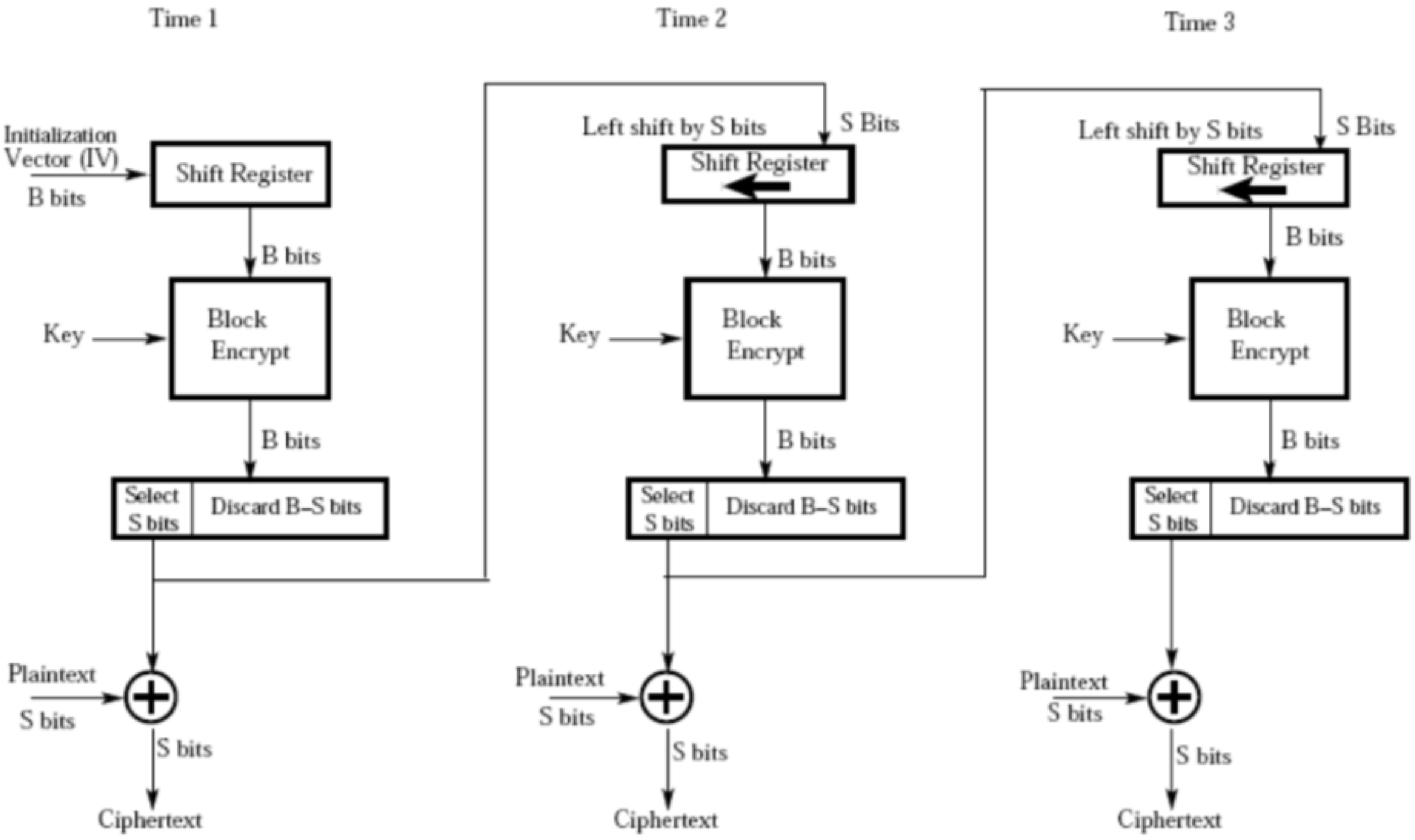
Decryption

The Cipher Block Chaining Mode (CBC):



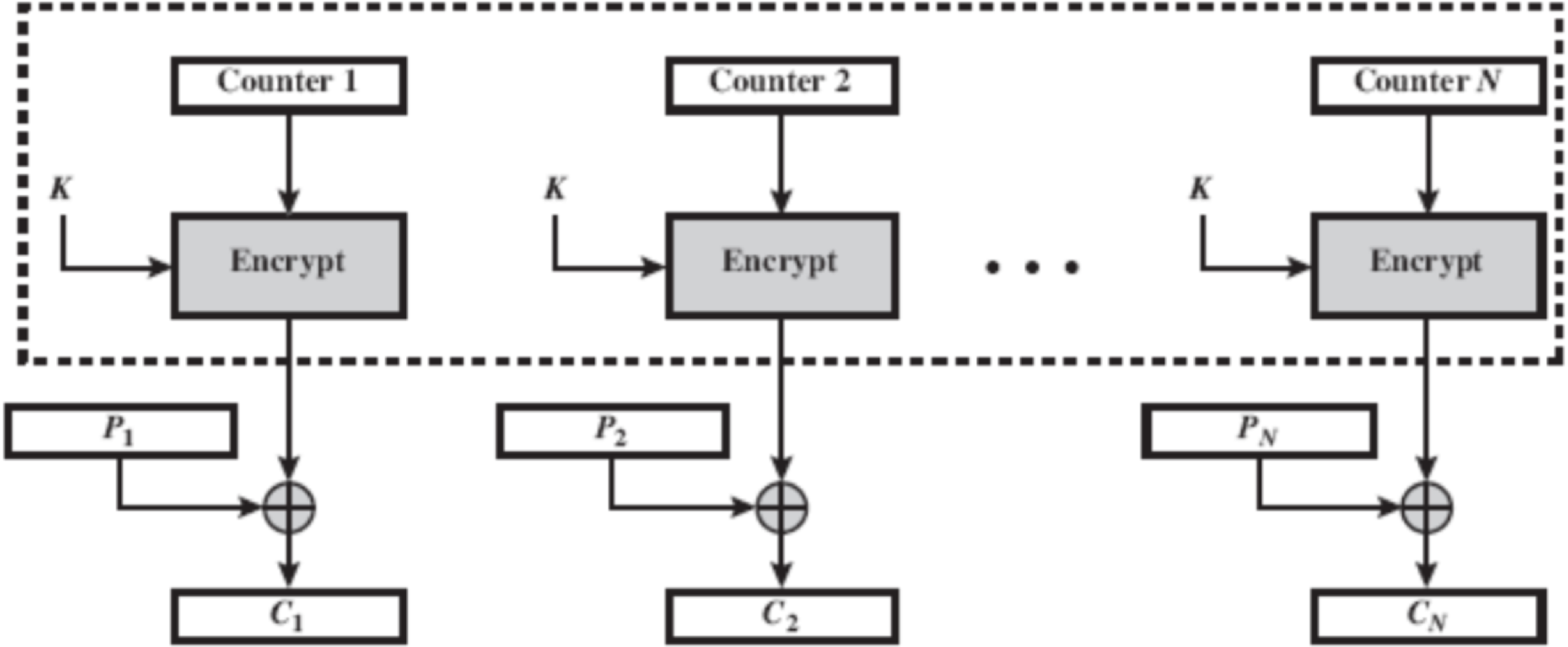
CBC Encryption

The Output Feedback Mode (OFB)



OFB Encryption

The Counter Mode (CTR)



(a) Encryption

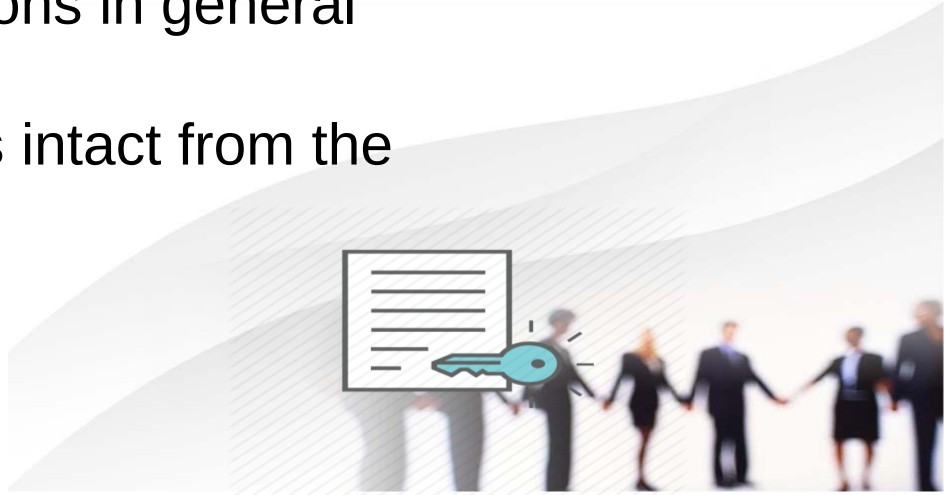
Symmetric Key Cryptography Assumptions

The assumptions are :

- The same key is use for both encryption and decryption and
- the two communicants already share secret key, which somehow has been distributed to them; or
- the use of a key distribution center.

Problems:

- ***key distribution*** – how to have secure communications in general without having to trust a KDC with your key.
- ***digital signatures*** – how to verify a message comes intact from the claimed sender.



Thank You…