



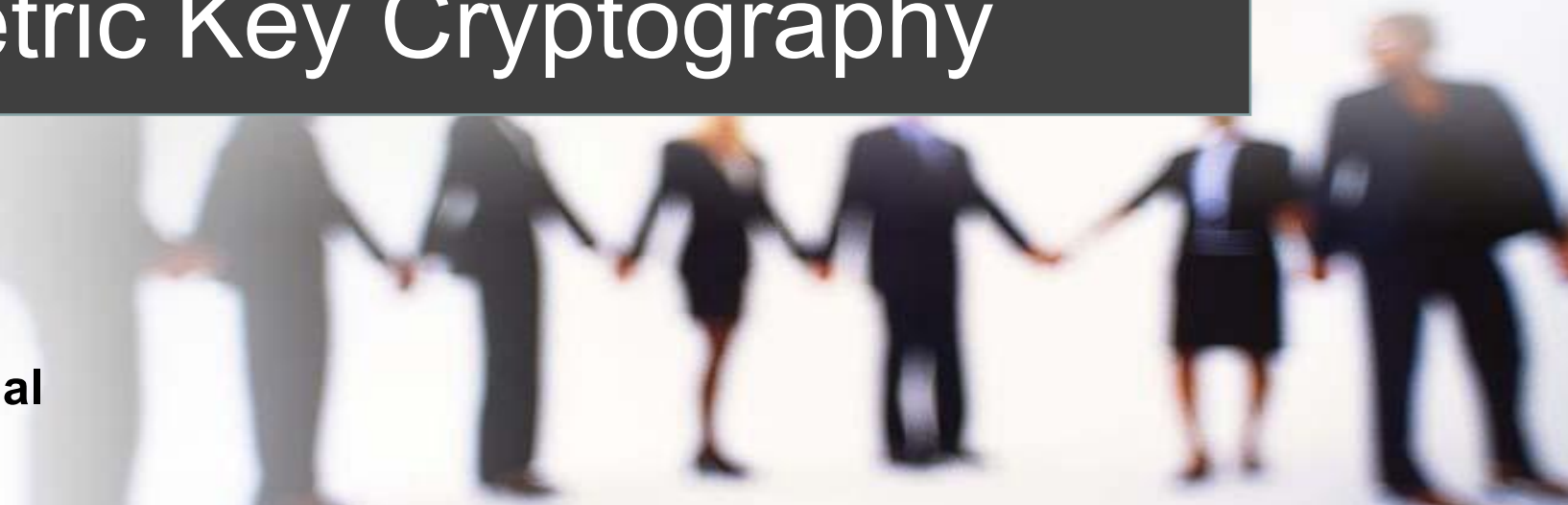
National Institute of Technology, Warangal

(Department of Computer Science Engineering)



Symmetric Key Cryptography

Lecture By:-
Dr R Padmavathy
Dept of CSE, NIT Warangal



Cryptographic Algorithm

Any encryption 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 .

$$C \leftarrow \text{Enc}_k(m)$$

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

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

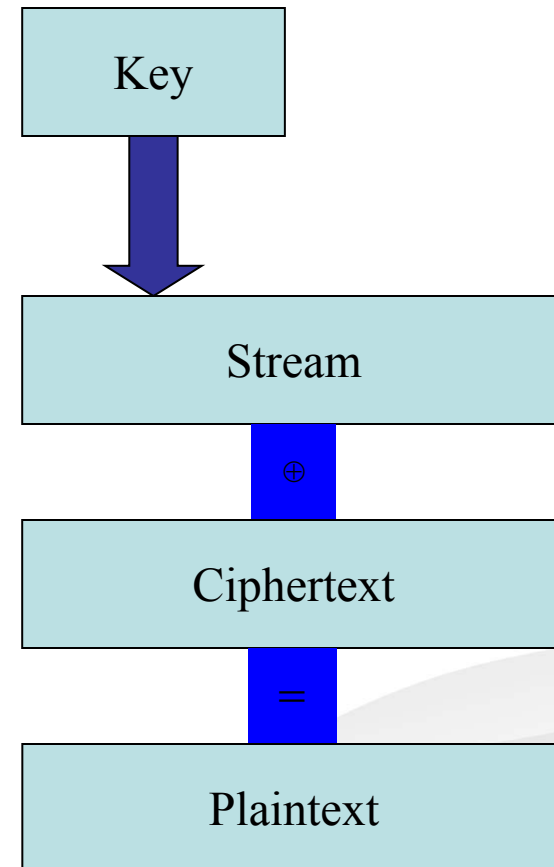
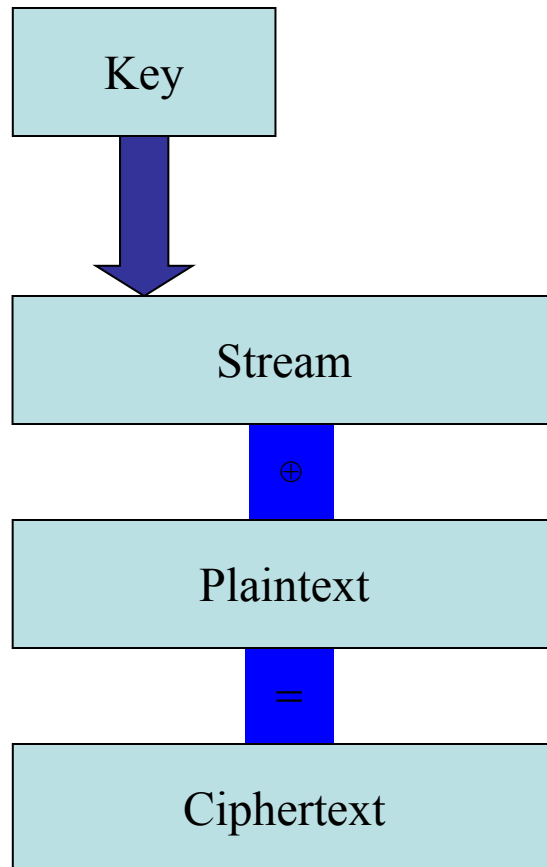


Stream Ciphers

- 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)

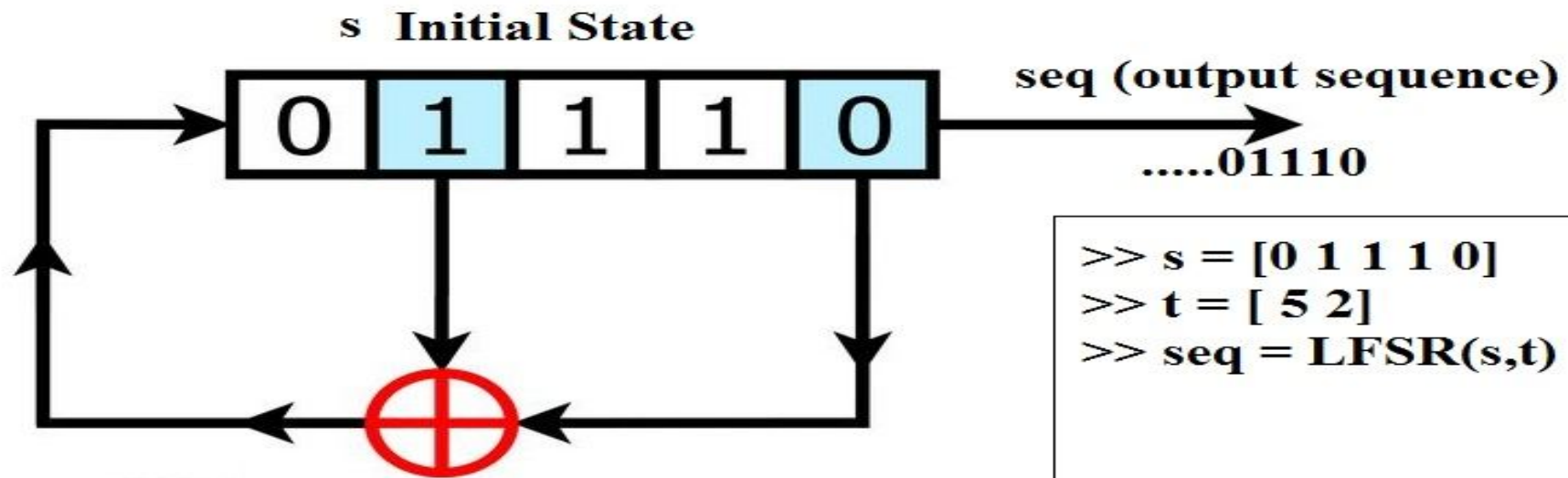


Example of Stream Encryption

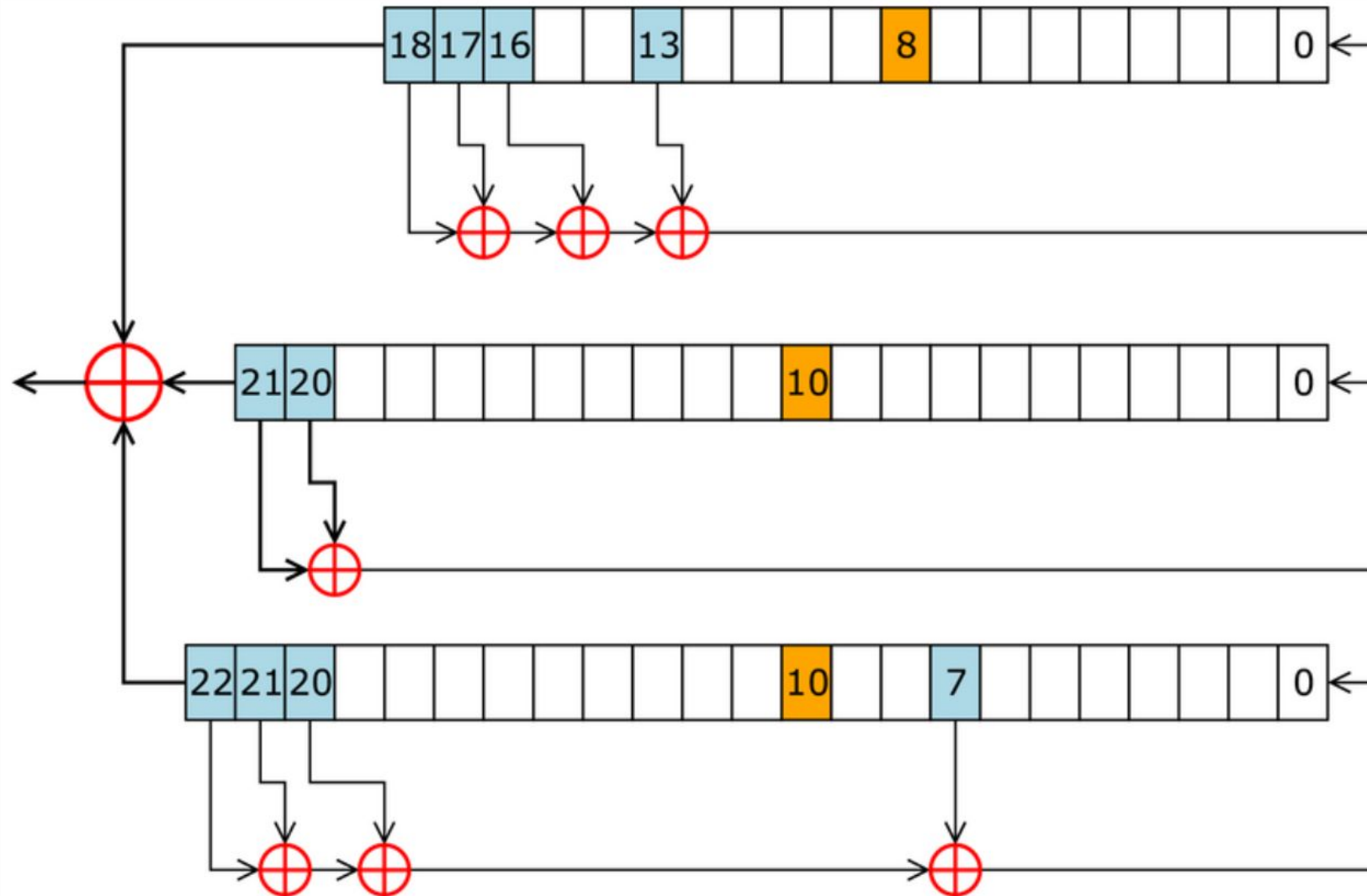


Linear Feedback Shift Register

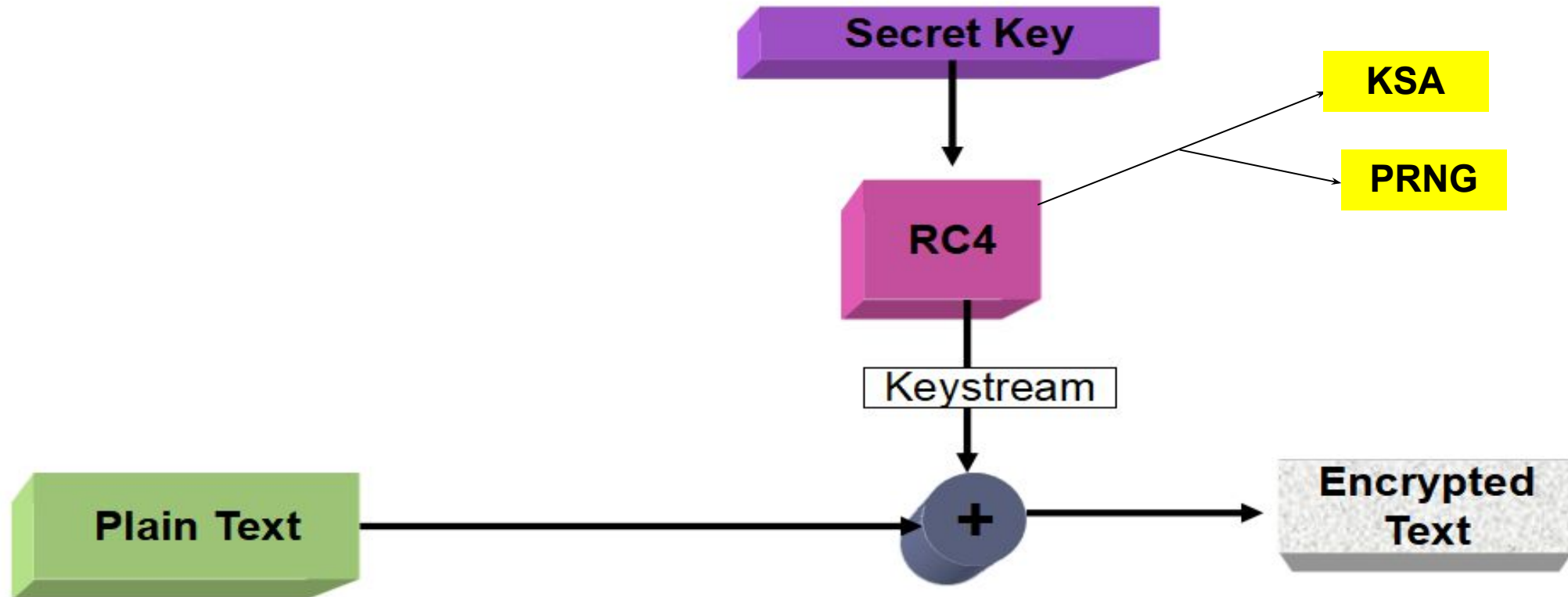
LFSR



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

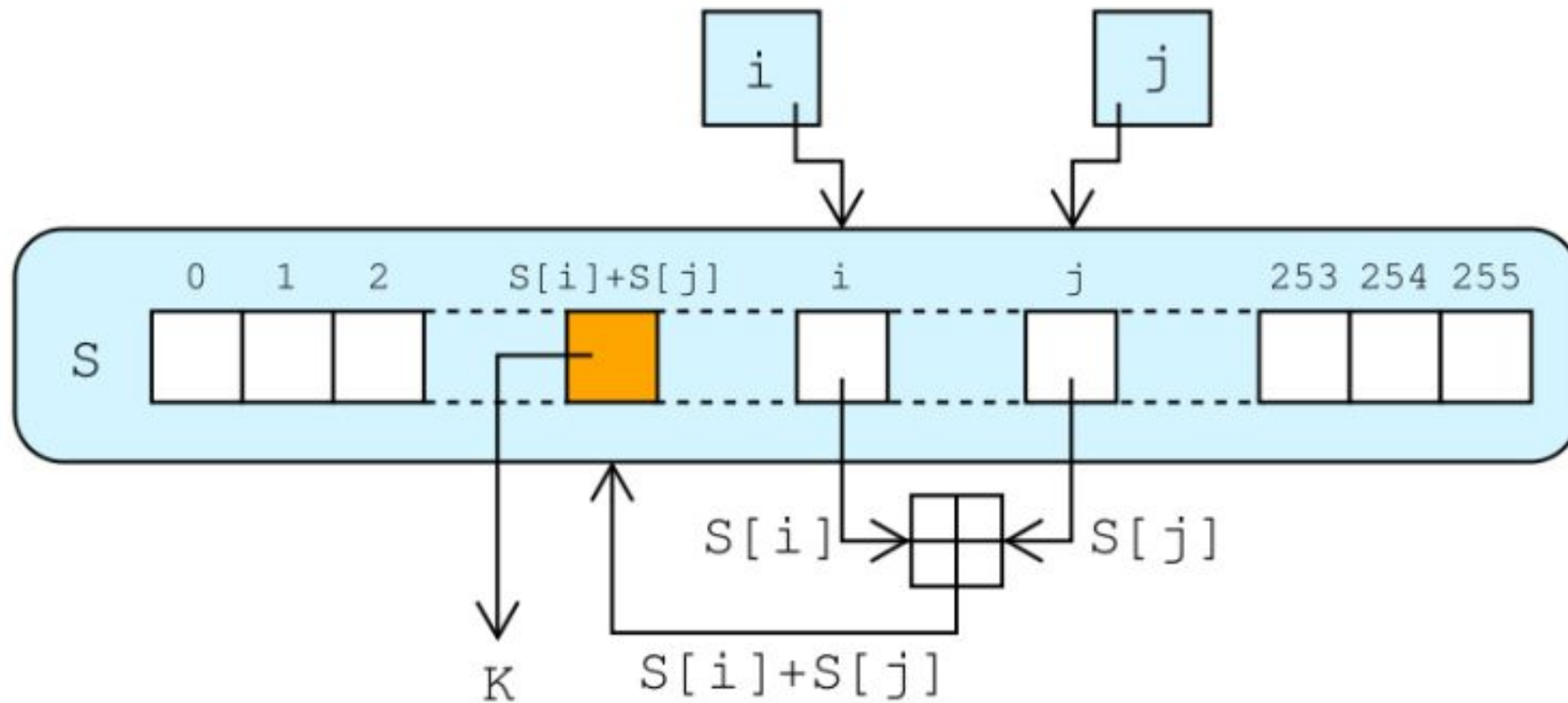
$j := (j + S[i] + \text{key}[i \bmod \text{keylength}]) \bmod 256$

 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

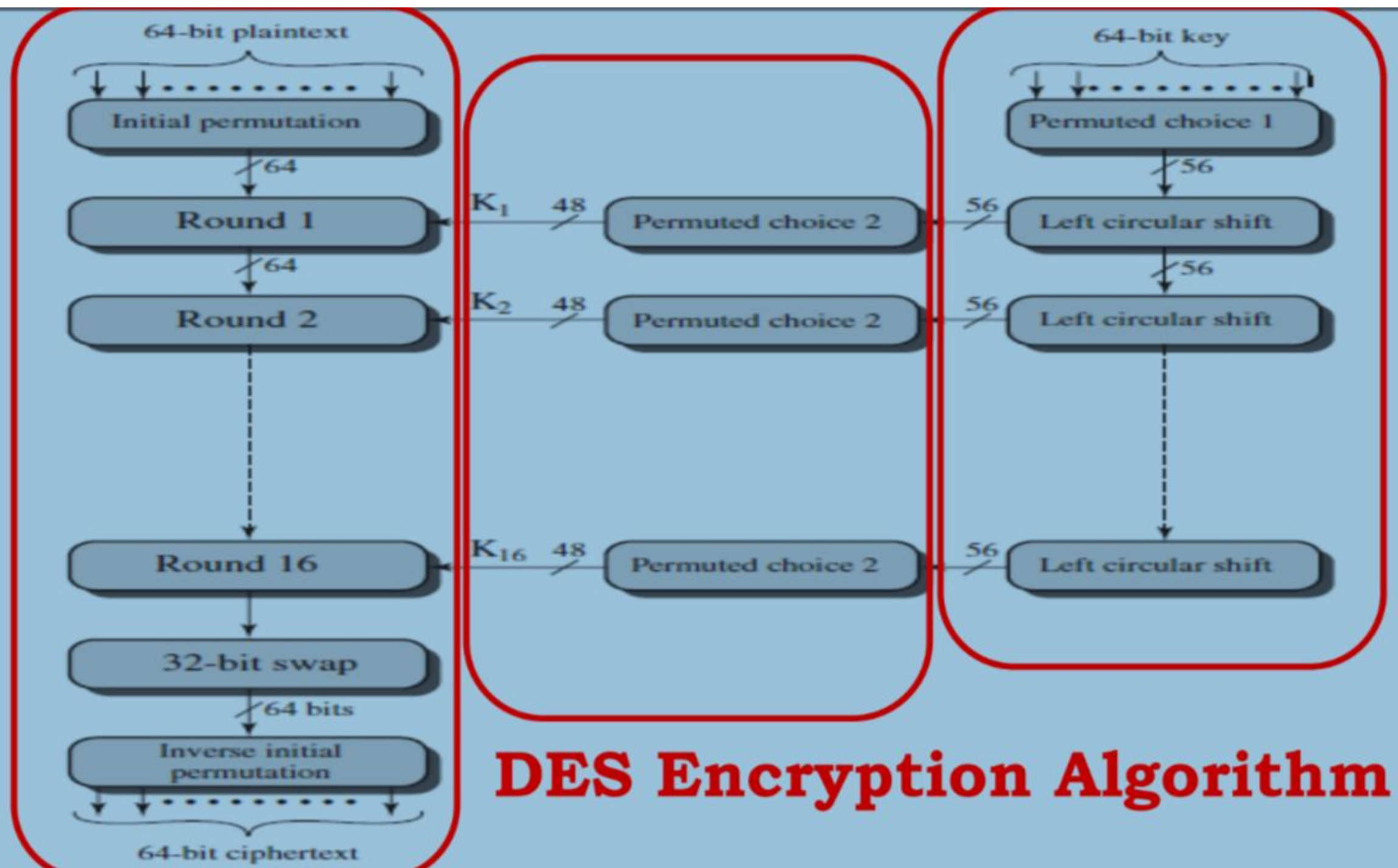
- Encrypt a block of input to a block of output
- Typically, the two blocks are of the same length
- Most symmetric key systems block size is 64
- In AES block size is 128
- Different modes for encrypting plaintext longer than a block.
- Examples include DES, 3-DES, AES, RC-2, RC-5, IDEA, Blowfish etc.



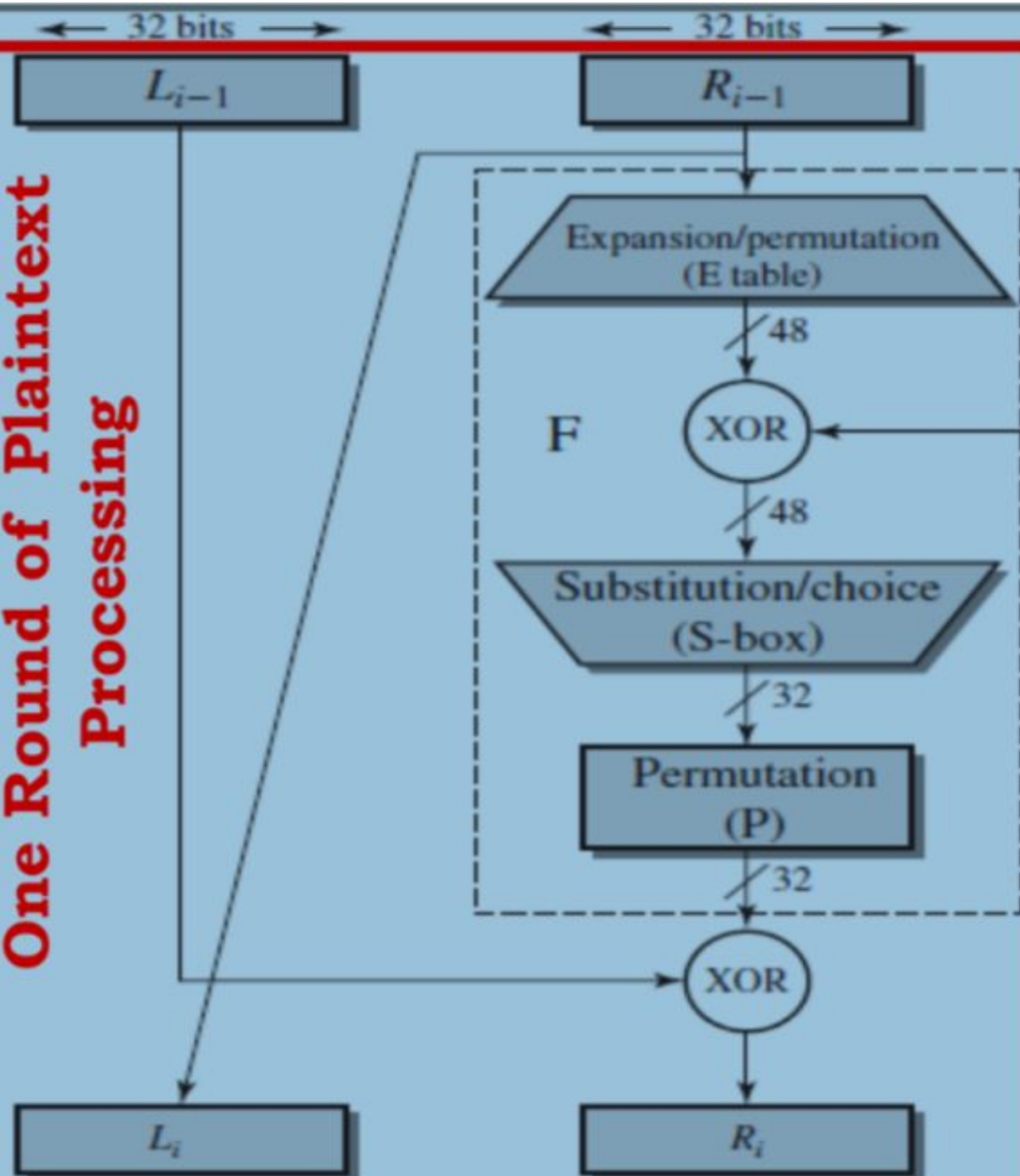
DES Algorithm

- ❖ 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

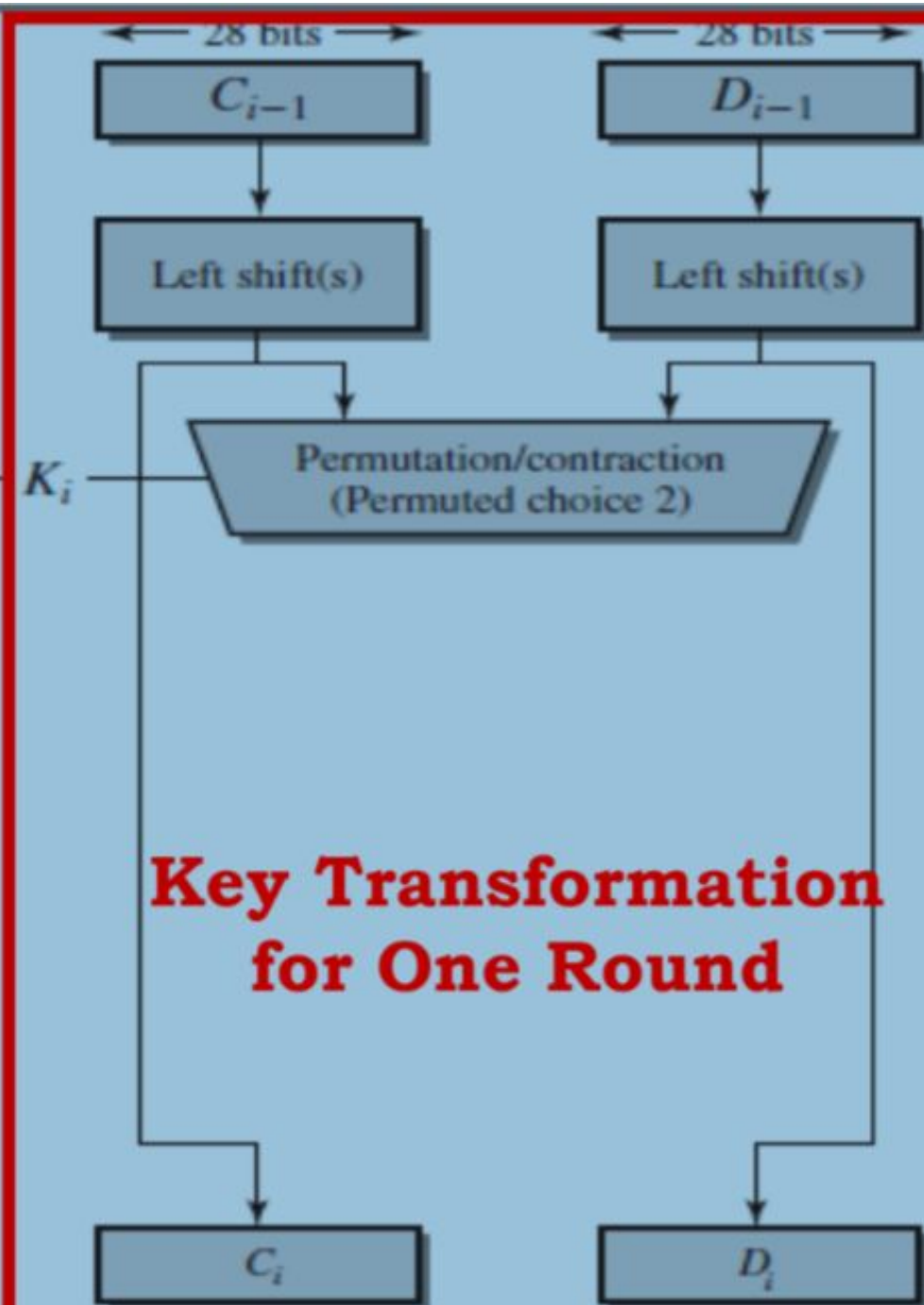




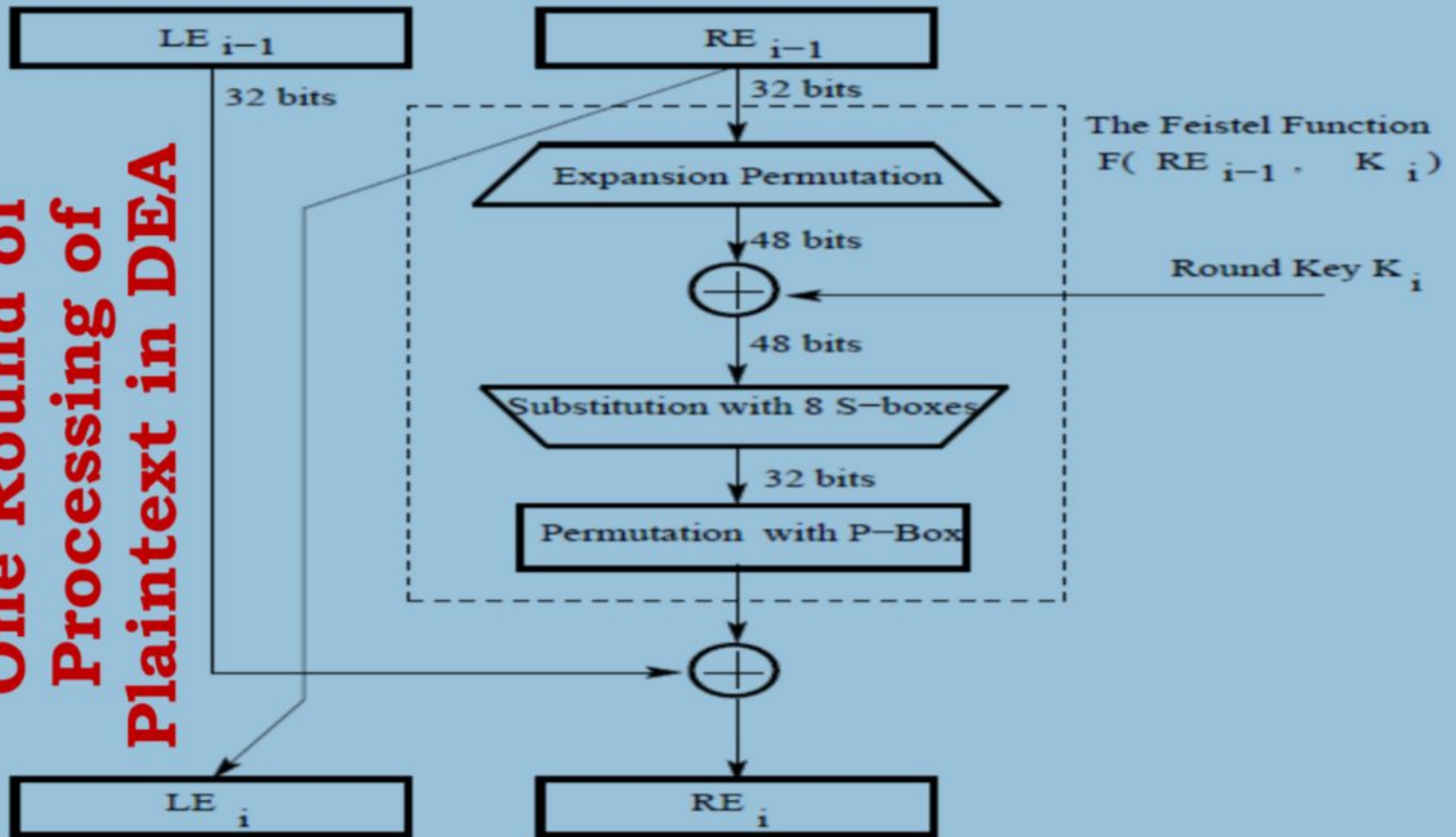
One Round of Plaintext Processing

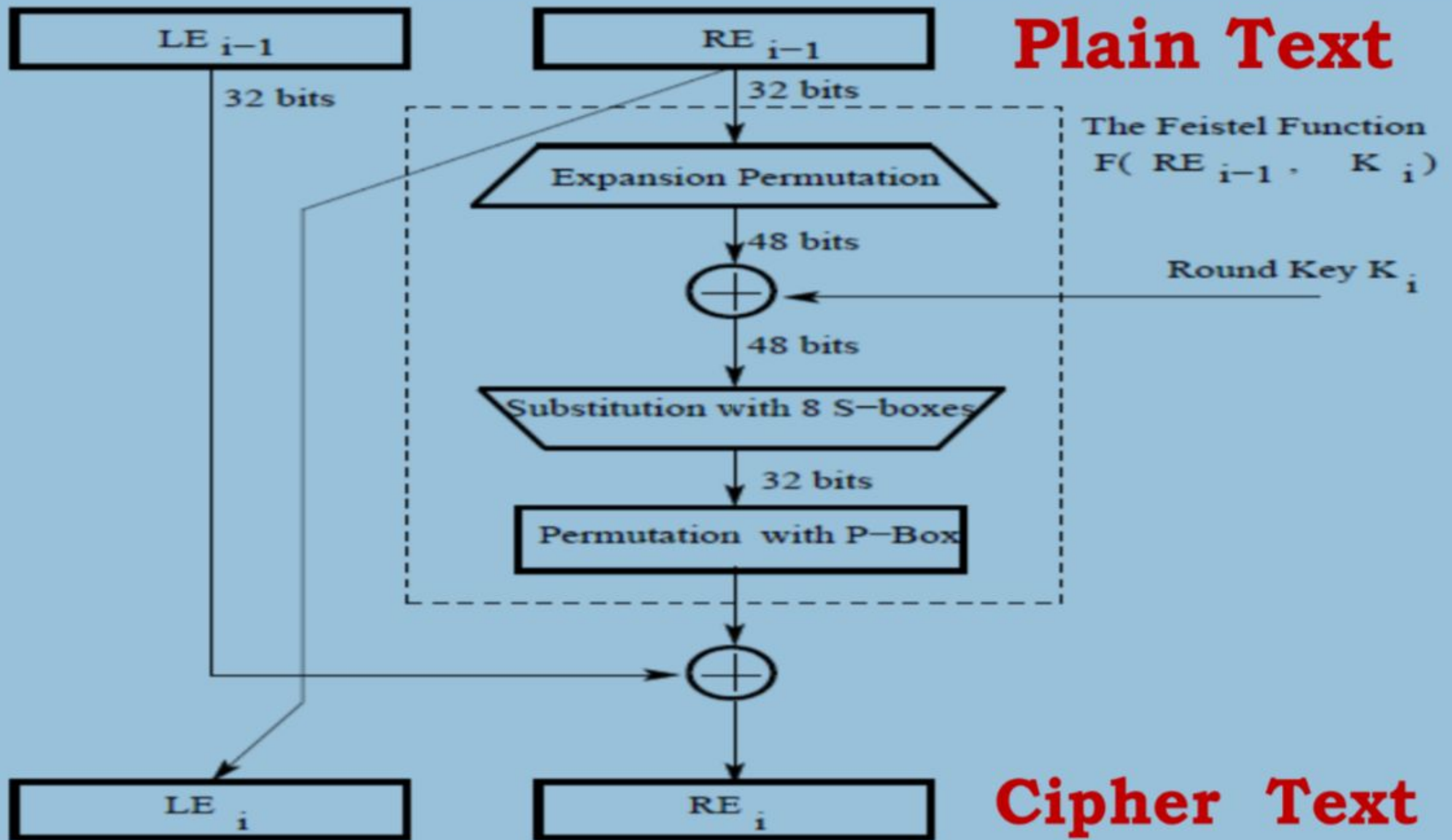


Key Transformation for One Round



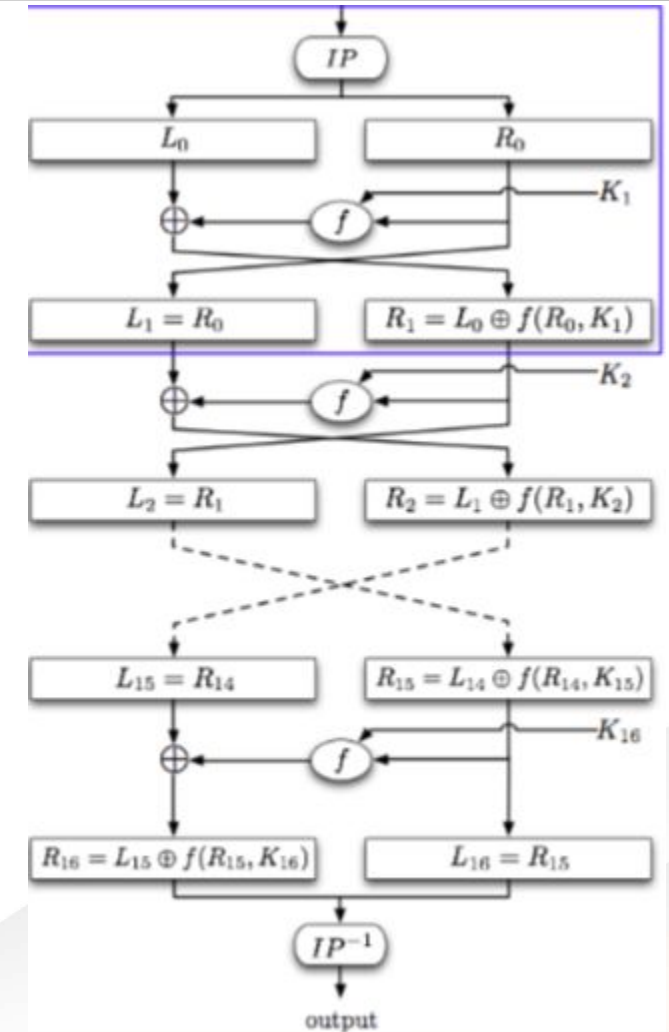
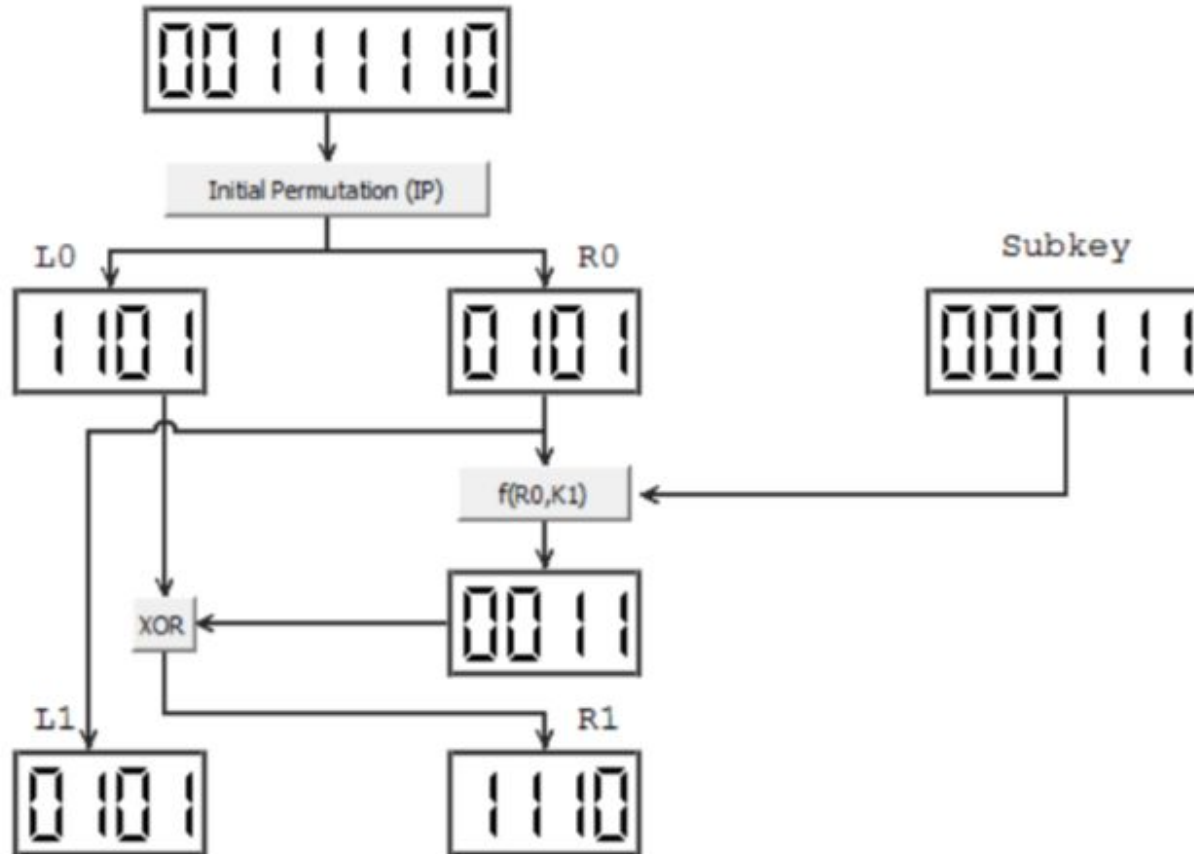
One Round of Processing of Plaintext in DEA



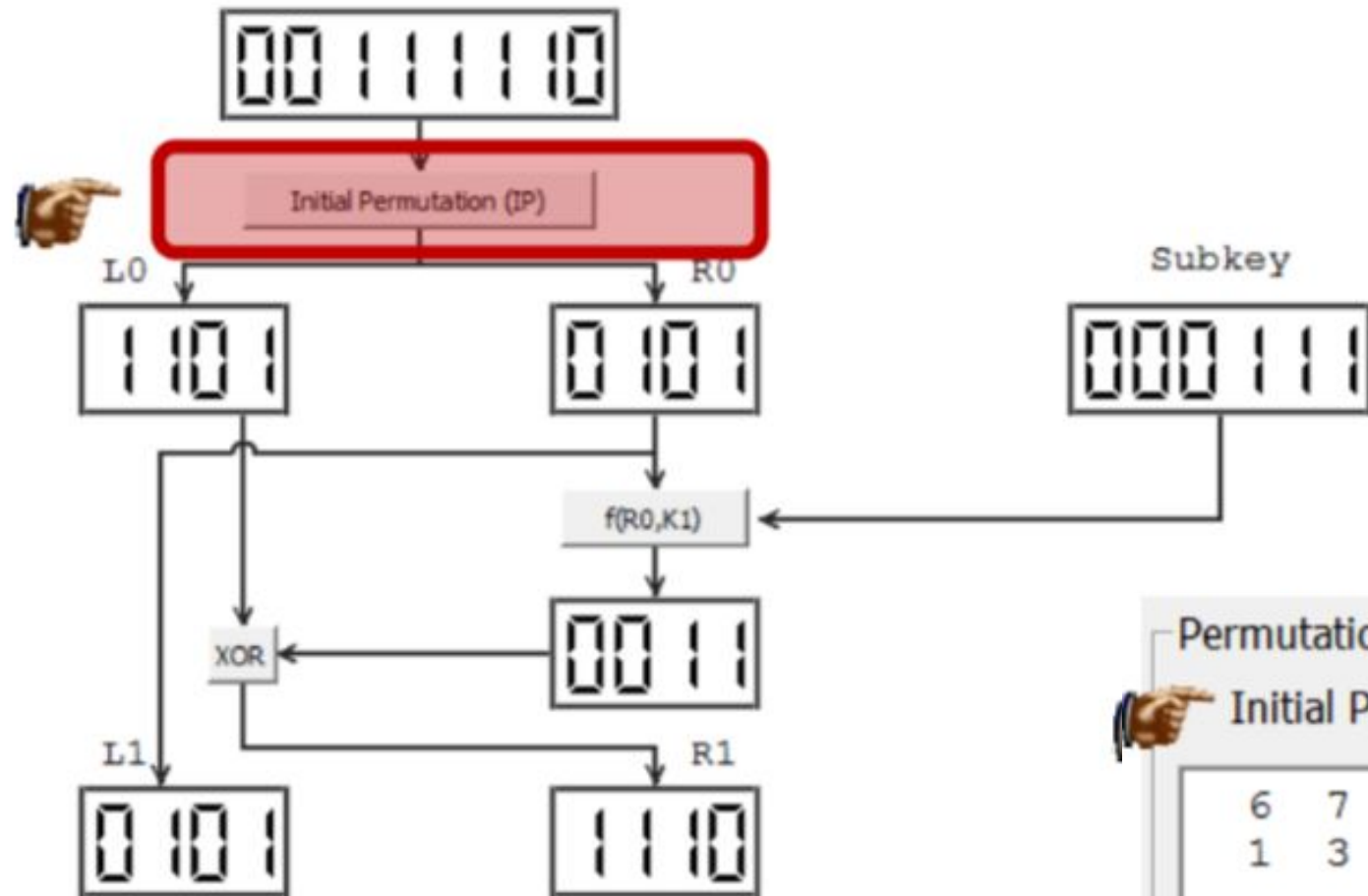


DES Encryption

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



Initial Permutation

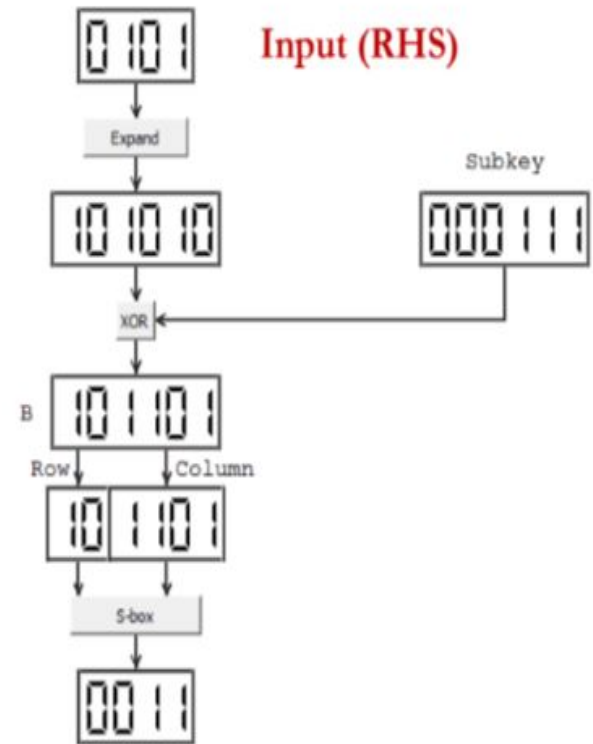
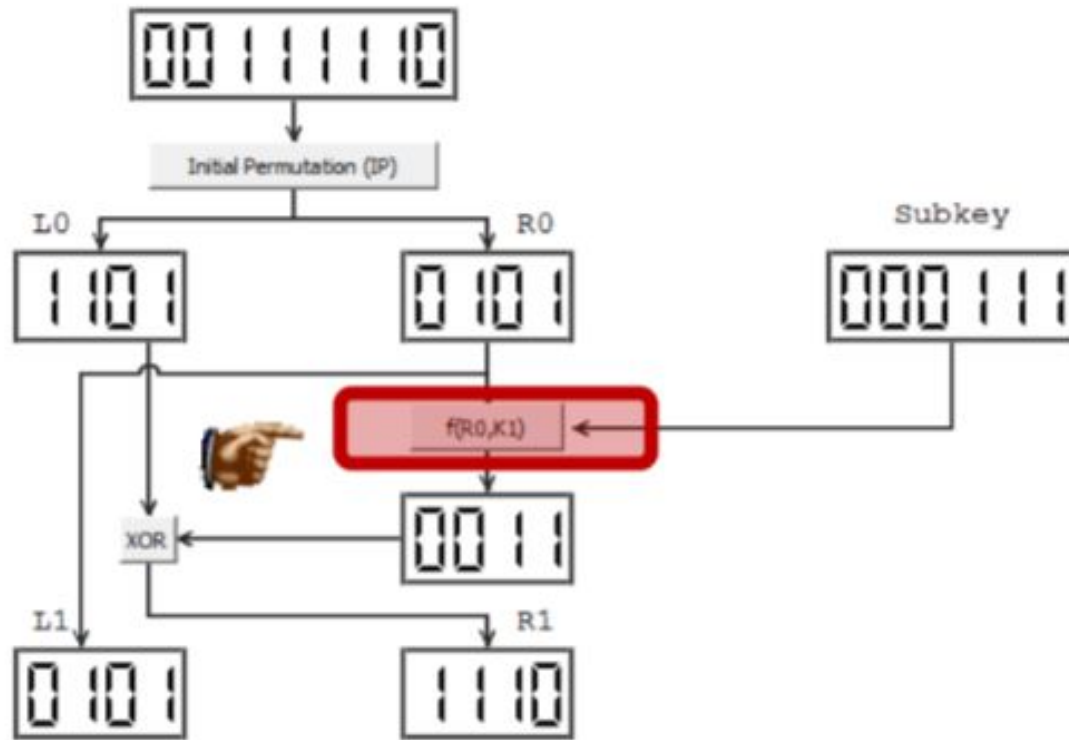


Permutation

Initial Permutation

6	7	8	5
1	3	2	4

Function: $F(R0, K1)$



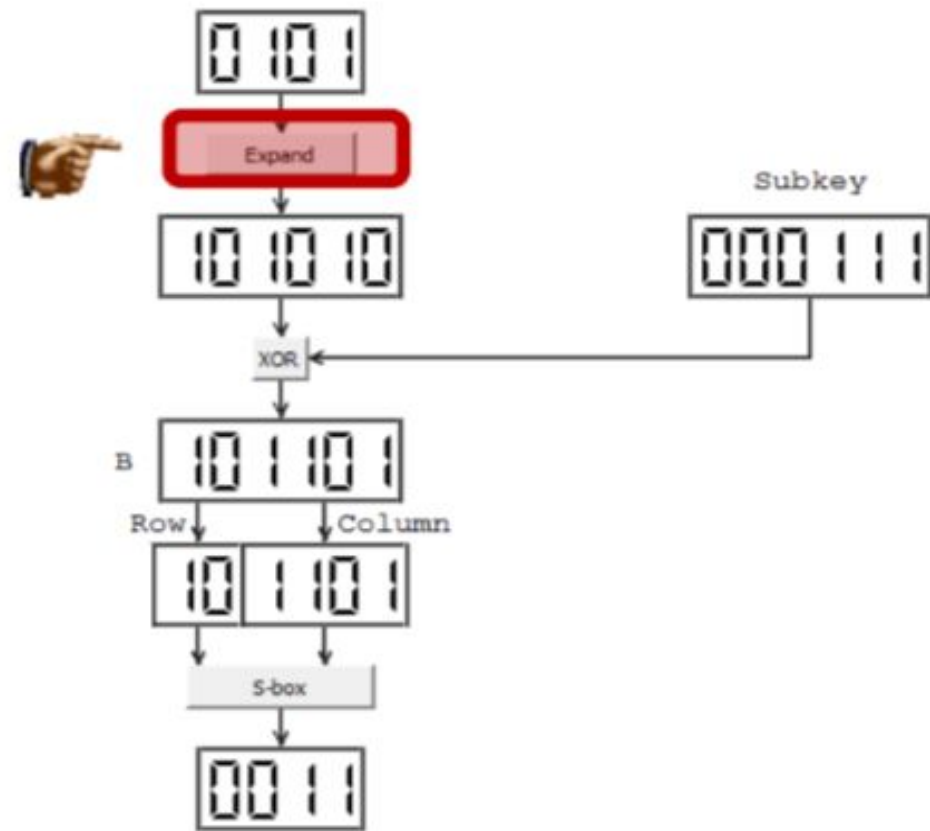
Function: Expand

f Function

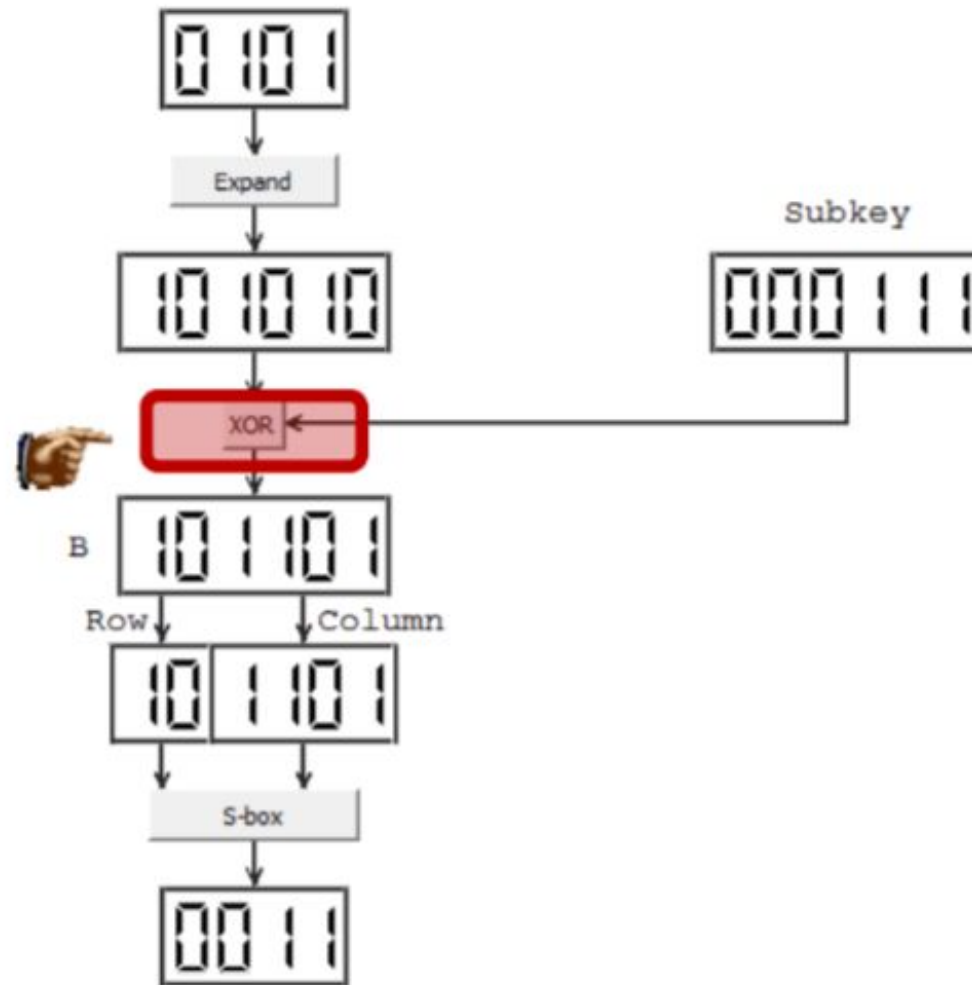
This table determines how the 4-bit data block expands to 6-bit.

Expand Table

4	1	2	3	4	1
---	---	---	---	---	---



XOR



Function S-Box

f Function

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

S-box:

Row	Column															
	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
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

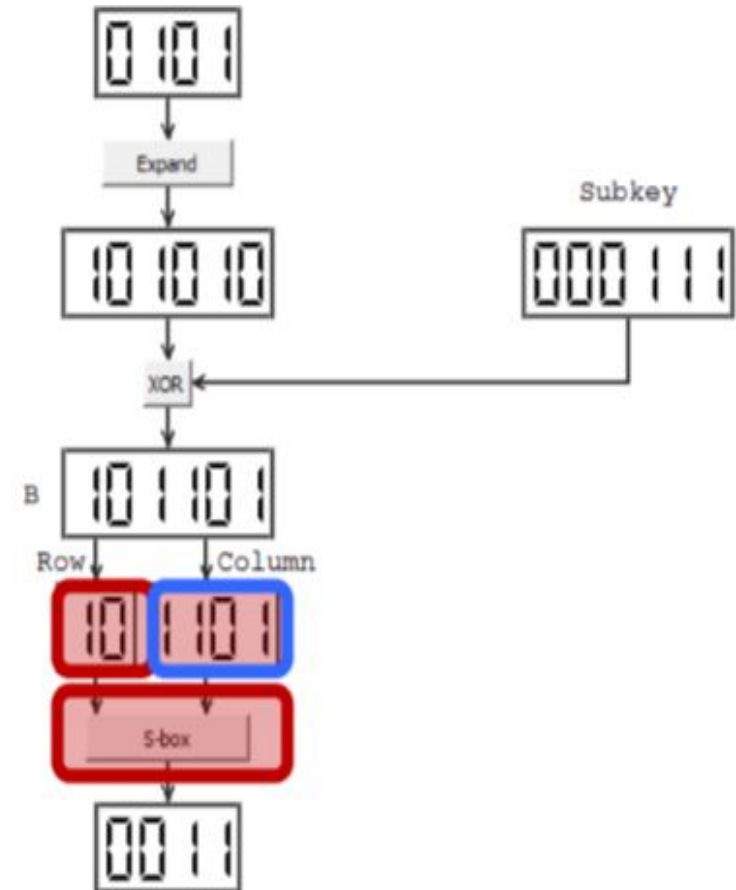
Calculation:

Row1: (10b): 2

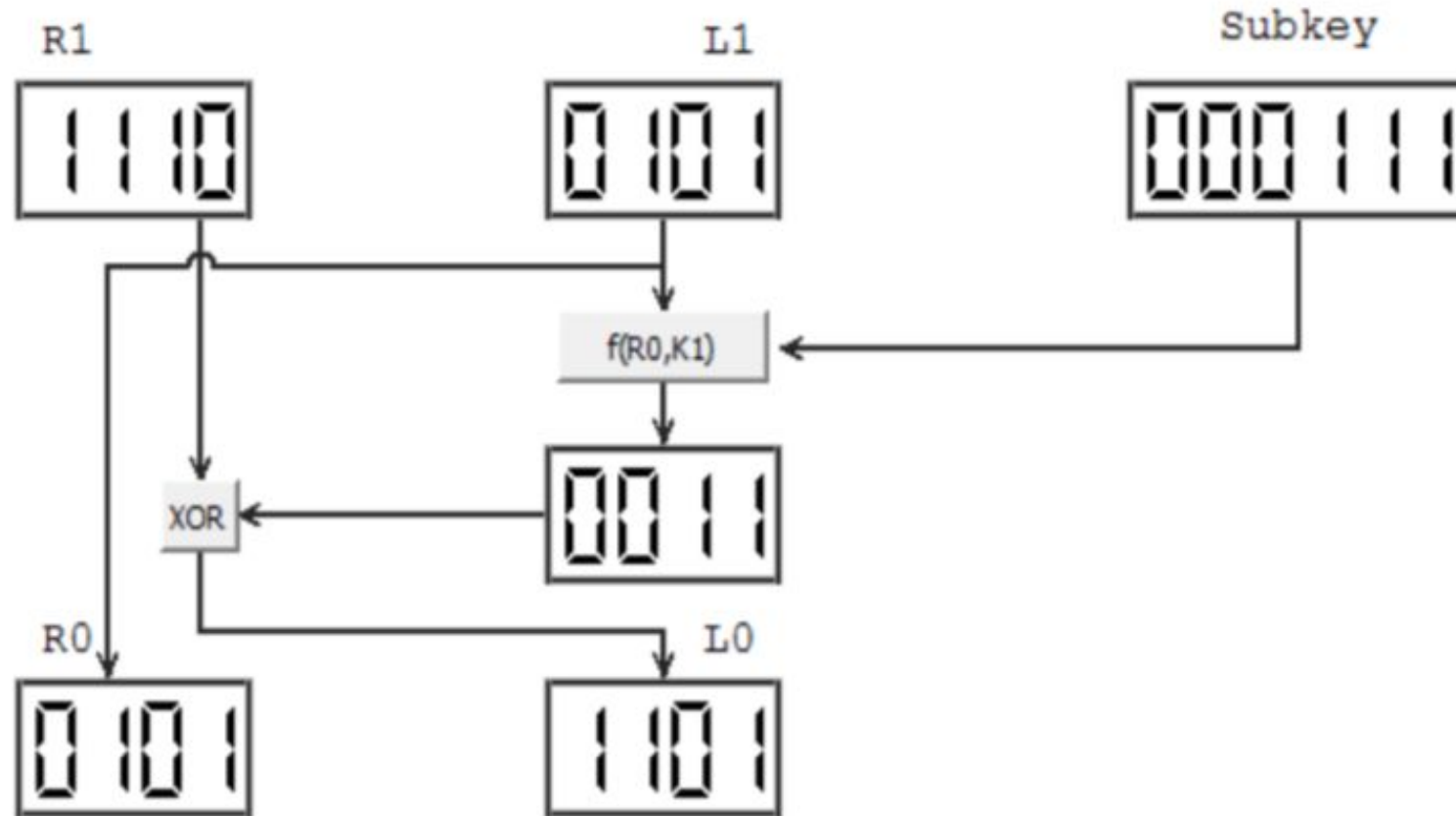
Column1: (1101b): 13

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

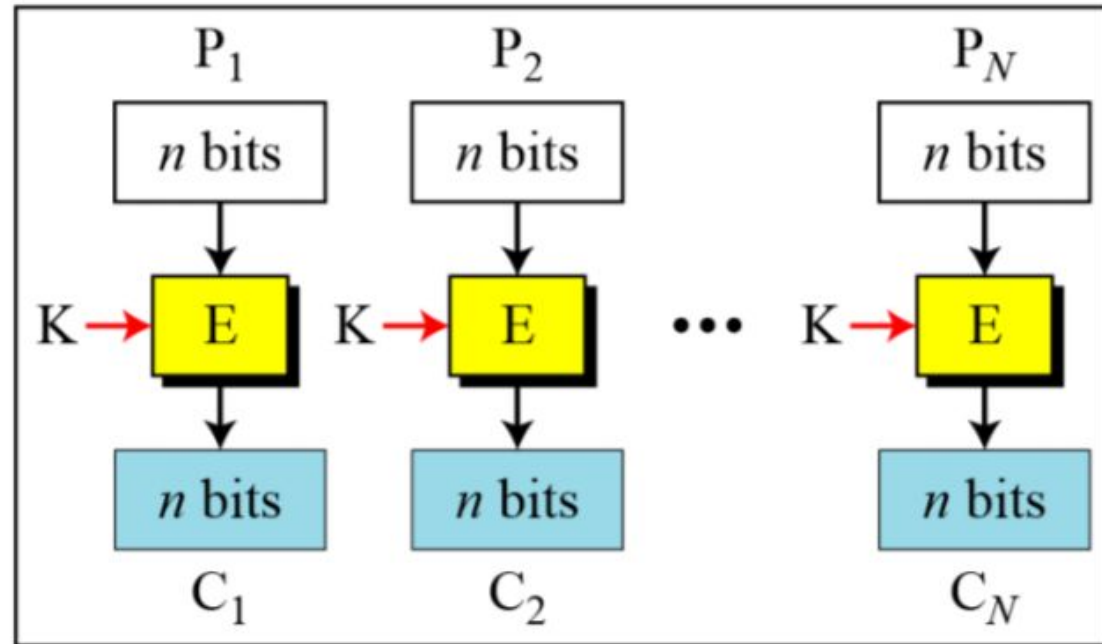
E: Encryption

D: Decryption

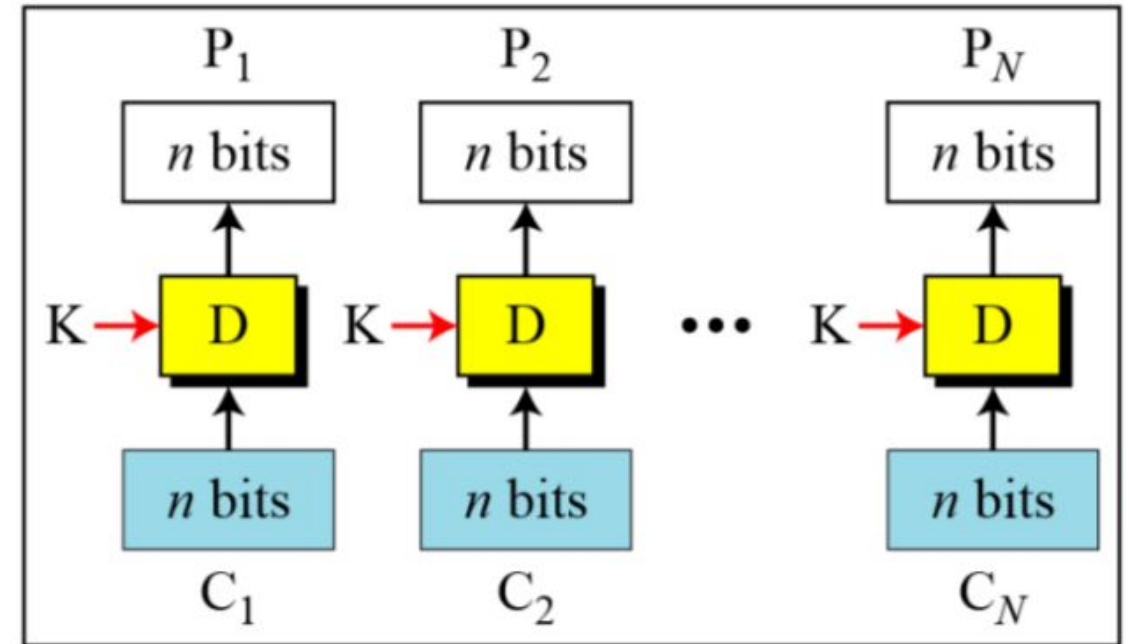
P_i : Plaintext block i

C_i : Ciphertext block i

K: Secret key

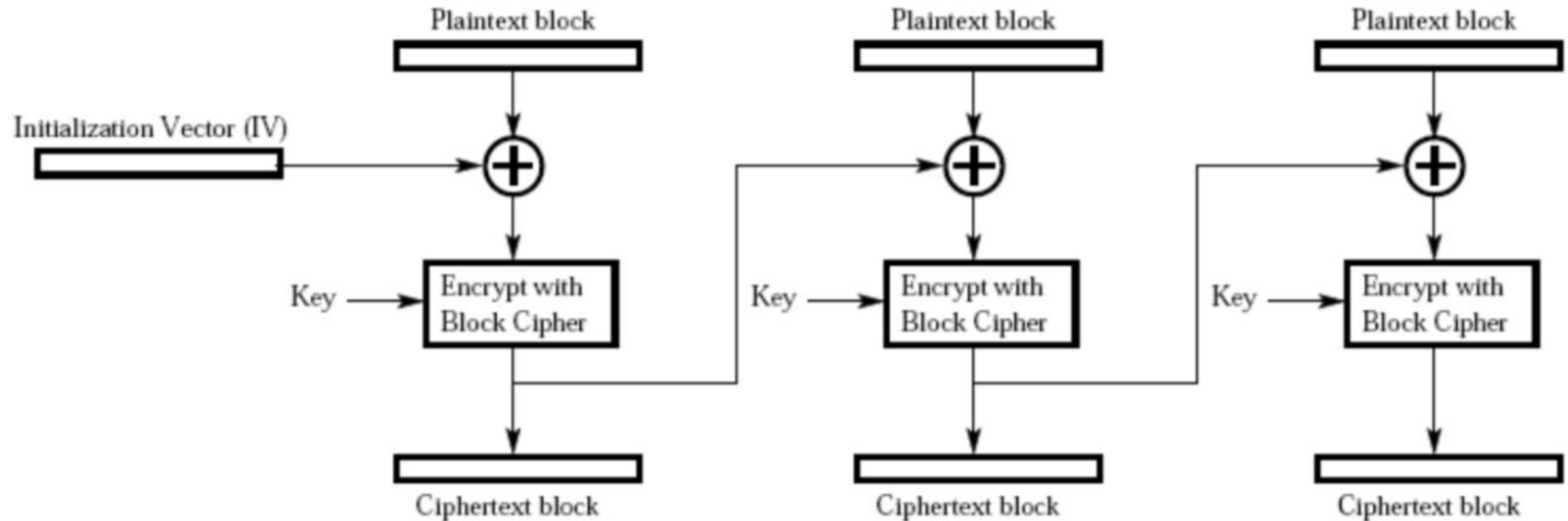


Encryption



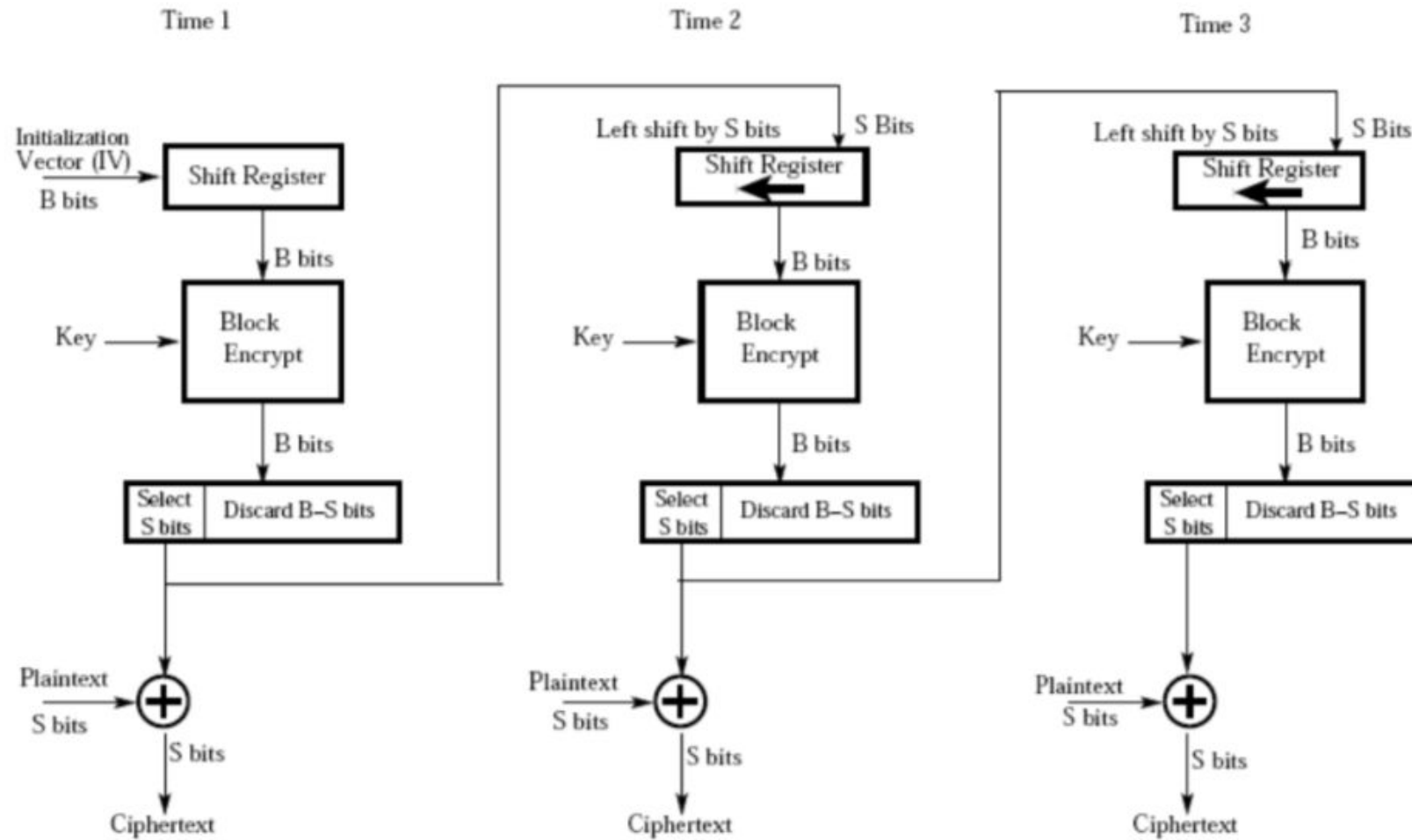
Decryption

The Cipher Block Chaining Mode (CBC):



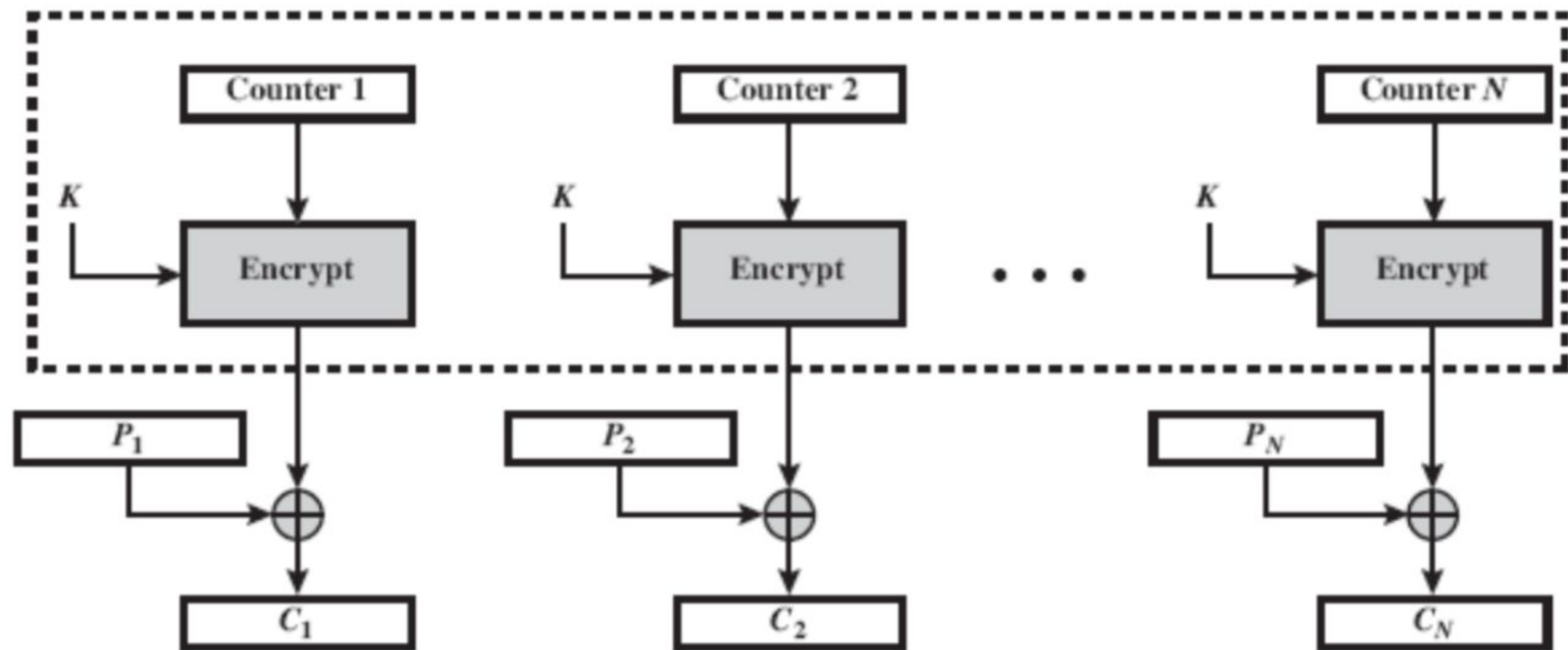
CBC Encryption

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...

