SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

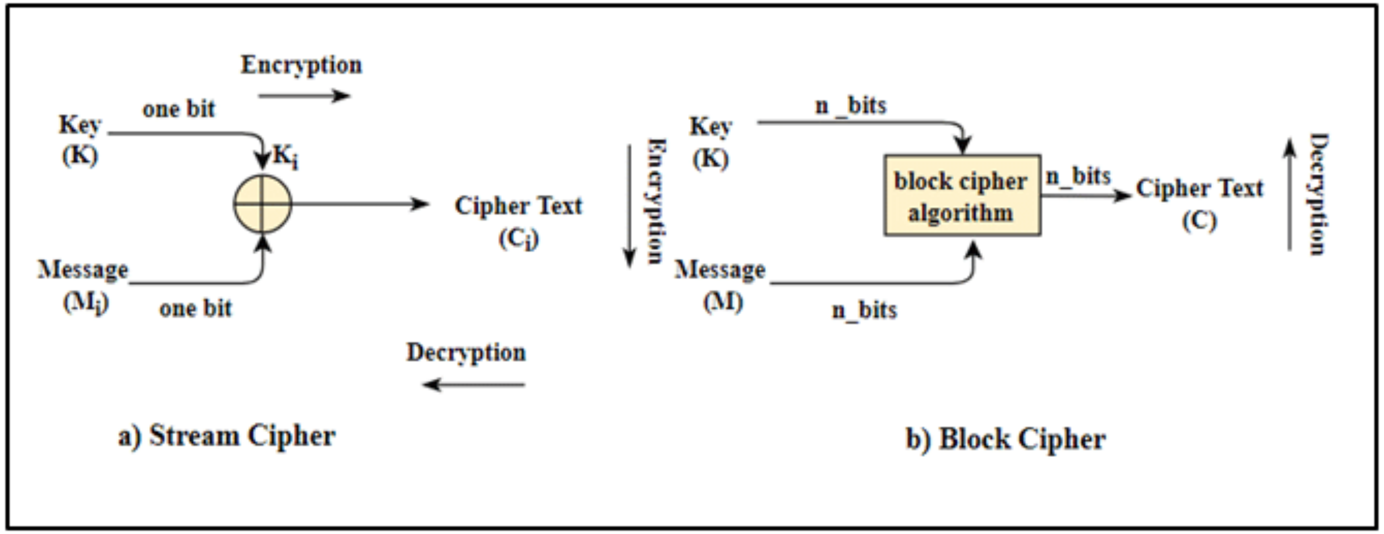
DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

19ITB302-Cryptography and Network Security

UNIT-1 INTRODUCTION TO ENCRYPTION STANDARD

Block Cipher Principles

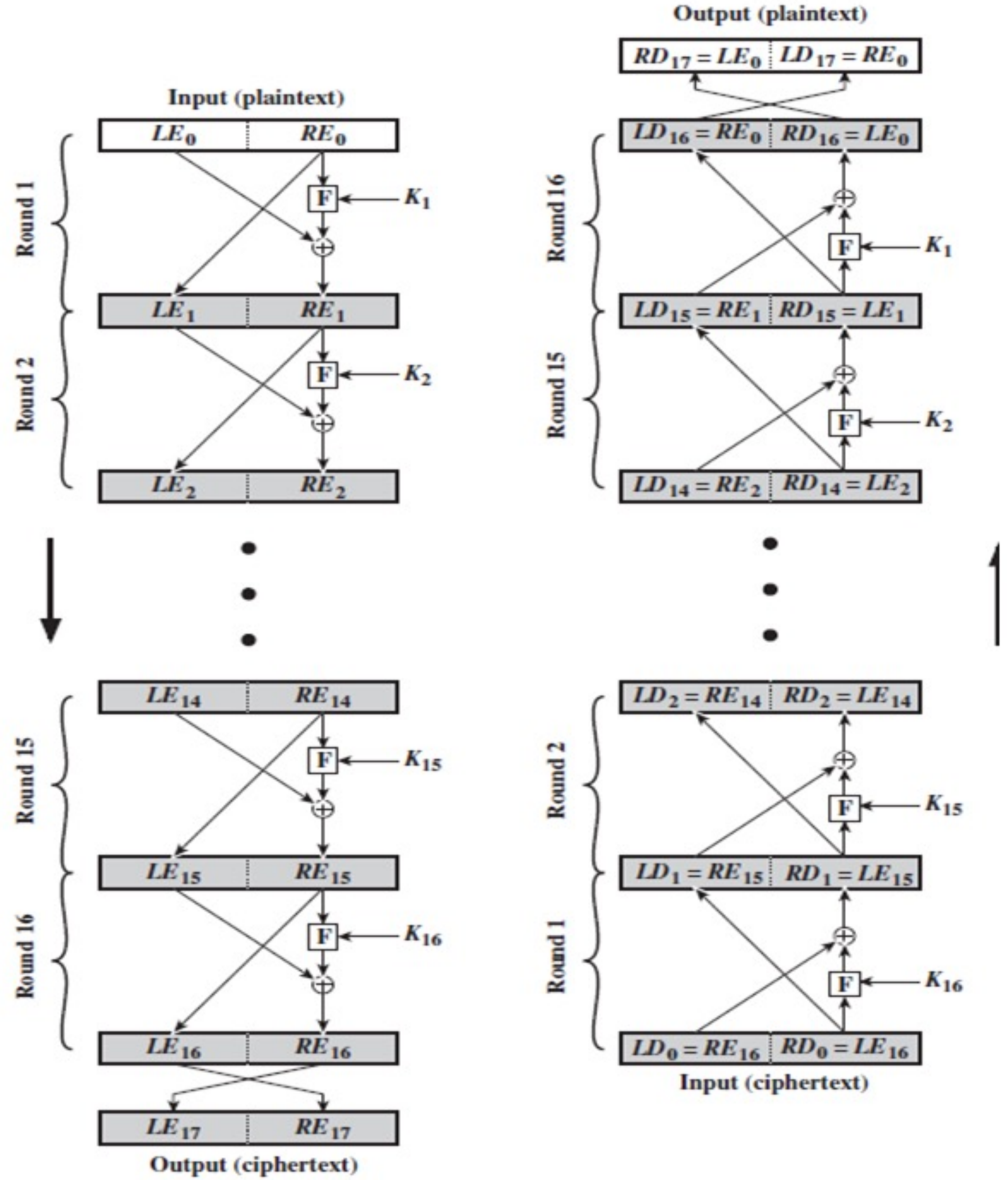
- Block cipher is a type of encryption algorithm that processes fixed-size blocks of data, usually 64 or 128 bits, to produce ciphertext.
- Block cipher has a specific number of **rounds** and **keys** for generating ciphertext.



Feistal Cipher Structure

Feistel cipher structure encrypts plain text in several rounds, where it applies **substitution** and **permutation** to the data.

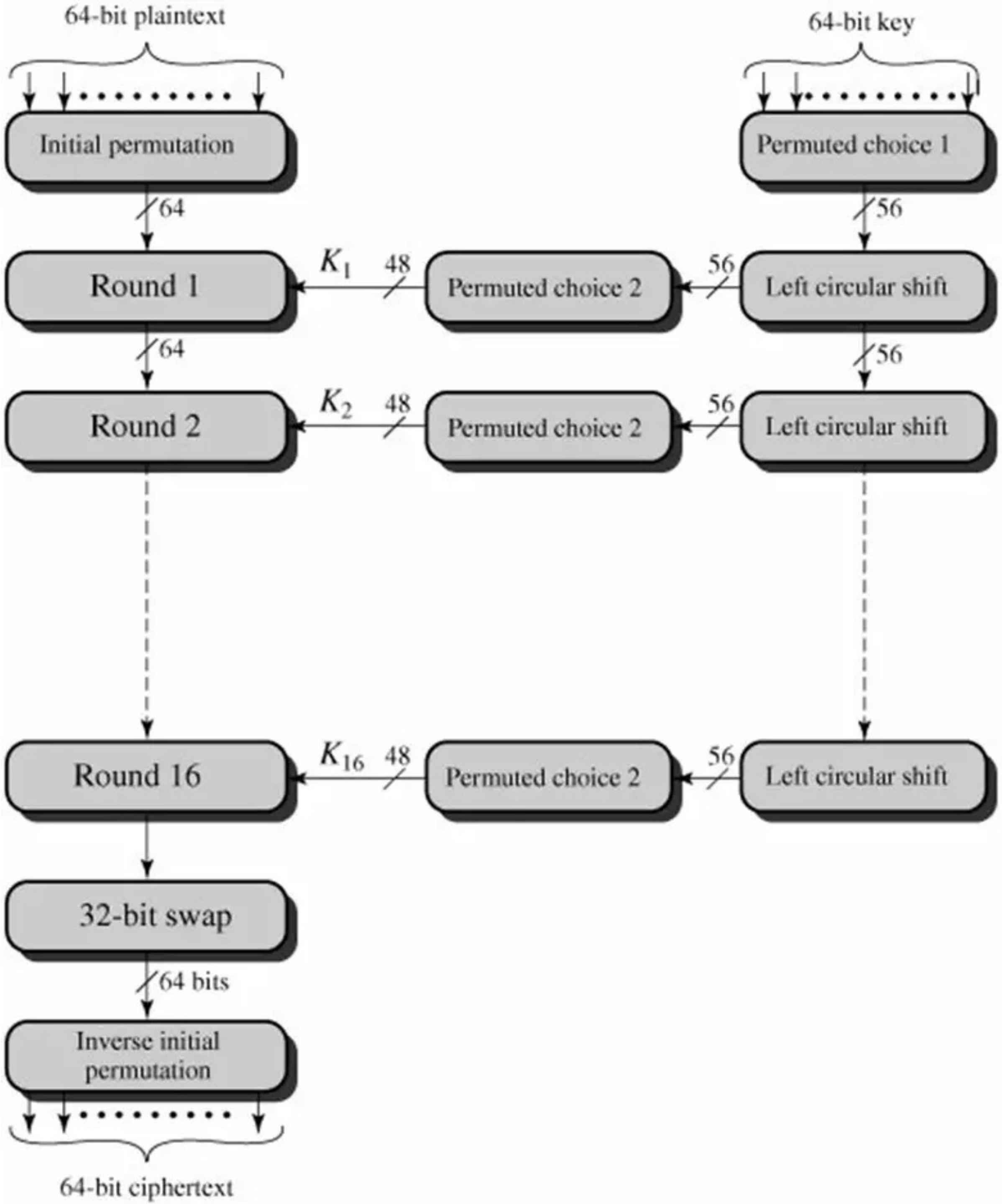
Each round uses a **different key** for encryption, and that same key is used for the decryption process.

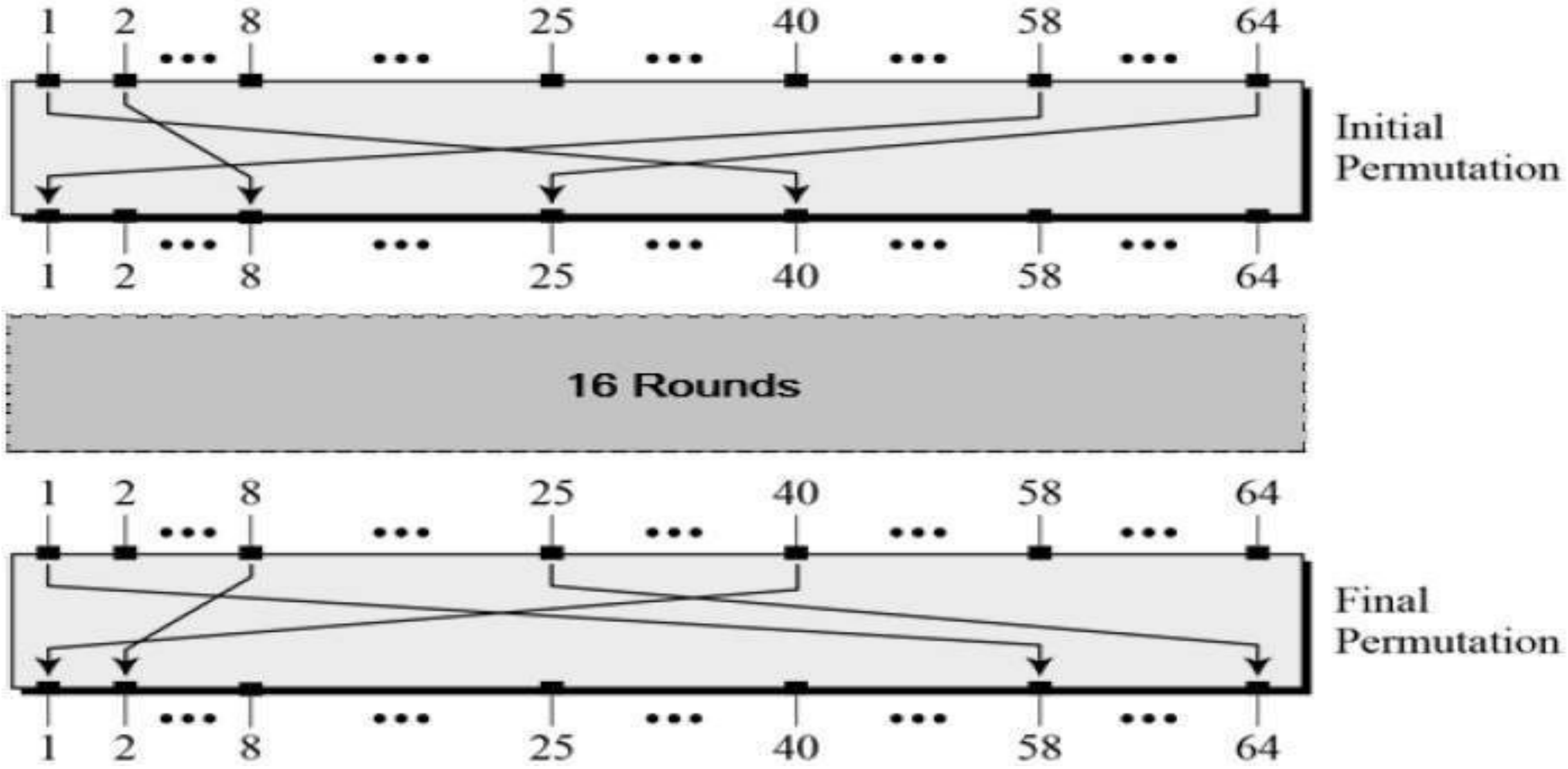

Input (plaintext)
LE0 RE0
Round 1
F K1
LE1 RE1
Round 2
F K2
LE2 RE2
LE14 RE14
Round 15
F K15
LE15 RE15
Round 16
F K16
LE16 RE16
LE17 RE17
Output (ciphertext)
Output (plaintext)
RD17 = LE0 LD17 = RE0
LD16 = RE0 RD16 = LE0
Round 16
F K1
LD15 = RE1 RD15 = LE1
Round 15
F K2
LD14 = RE2 RD14 = LE2
LD2 = RE14 RD2 = LE14
Round 2
F K15
LD1 = RE15 RD1 = LE15
Round 1
F K16
LD0 = RE16 RD0 = LE16
Input (ciphertext)

- Feistel cipher structure has the following five components:
- **Number of rounds:** The greater the number of rounds used for the encryption/decryption process, the higher the complexity; hence, the security of the block cipher.
- **Sub key generation algorithm:** Complex algorithms make it difficult for intruders to crack the key.
- **Encryption function:** Complex functions enhance the security of the block cipher, making them difficult to crack.
- **Block size:** The larger the size of the block, the more secure and complex the block cipher is. However, a larger block size reduces the execution speed of the encryption and decryption process.
- **Key size:** A large size key increases the security of the block cipher. However, it also makes the encryption and decryption process slow.

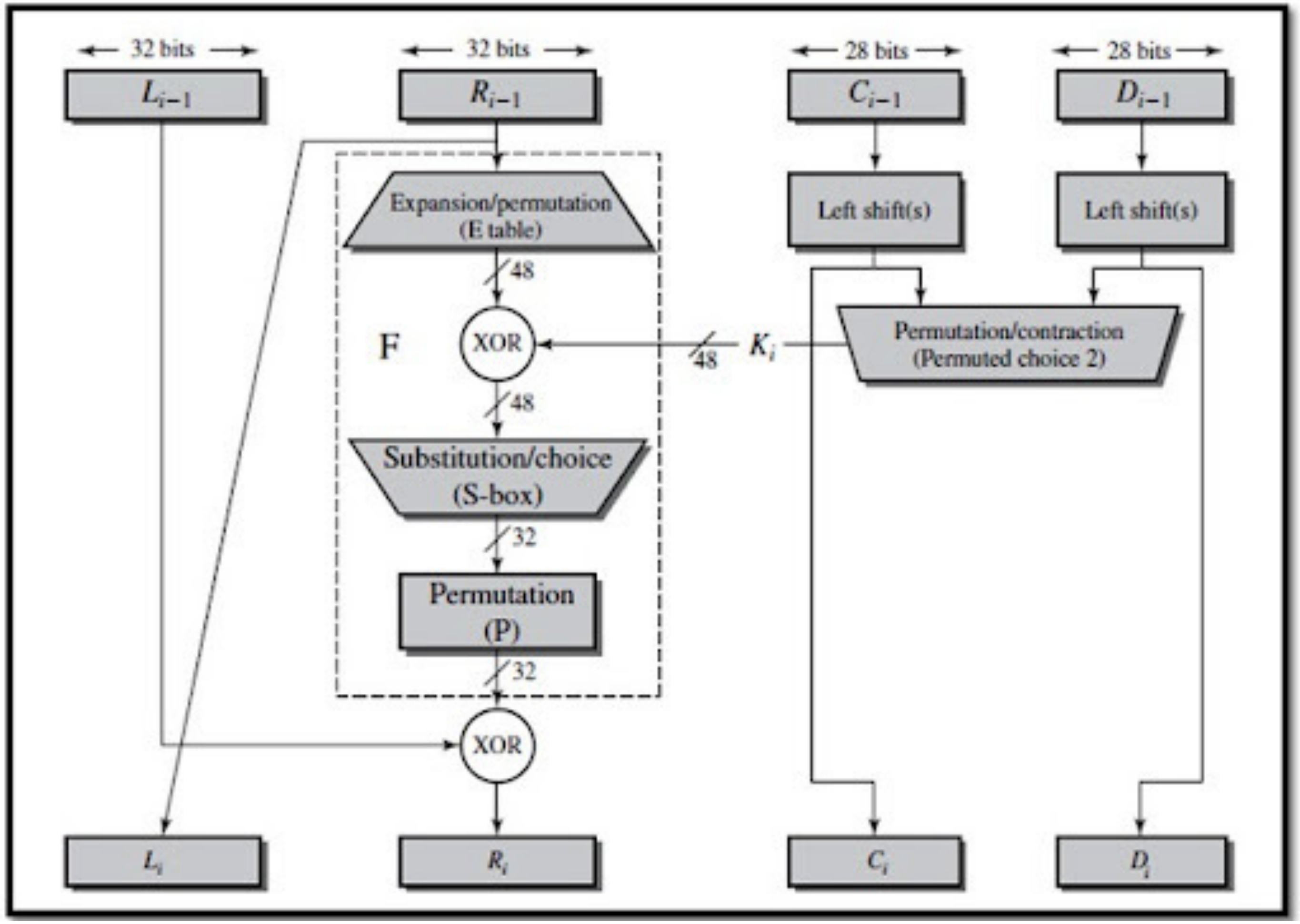
Data Encryption Standard

- The Data Encryption Standard (DES) is a **symmetric-key** block cipher published by the National Institute of Standards and Technology (NIST).
- DES is an implementation of a Feistel Cipher.
- It uses **16 round** Feistel structure.
- The **block size** is **64-bit.**
- Though, key length is 64-bit, DES has an **effective key length of 56 bits**, since 8 of the 64 bits of the key are not used by the encryption algorithm


64-bit plaintext
64-bit key
Initial permutation
Permuted choice 1
64
56
Round 1
K_1
48
Permuted choice 2
56
Left circular shift
64
56
Round 2
K_2
48
Permuted choice 2
56
Left circular shift
Round 16
K_{16}
48
Permuted choice 2
56
Left circular shift
32-bit swap
64 bits
Inverse initial permutation
64-bit ciphertext

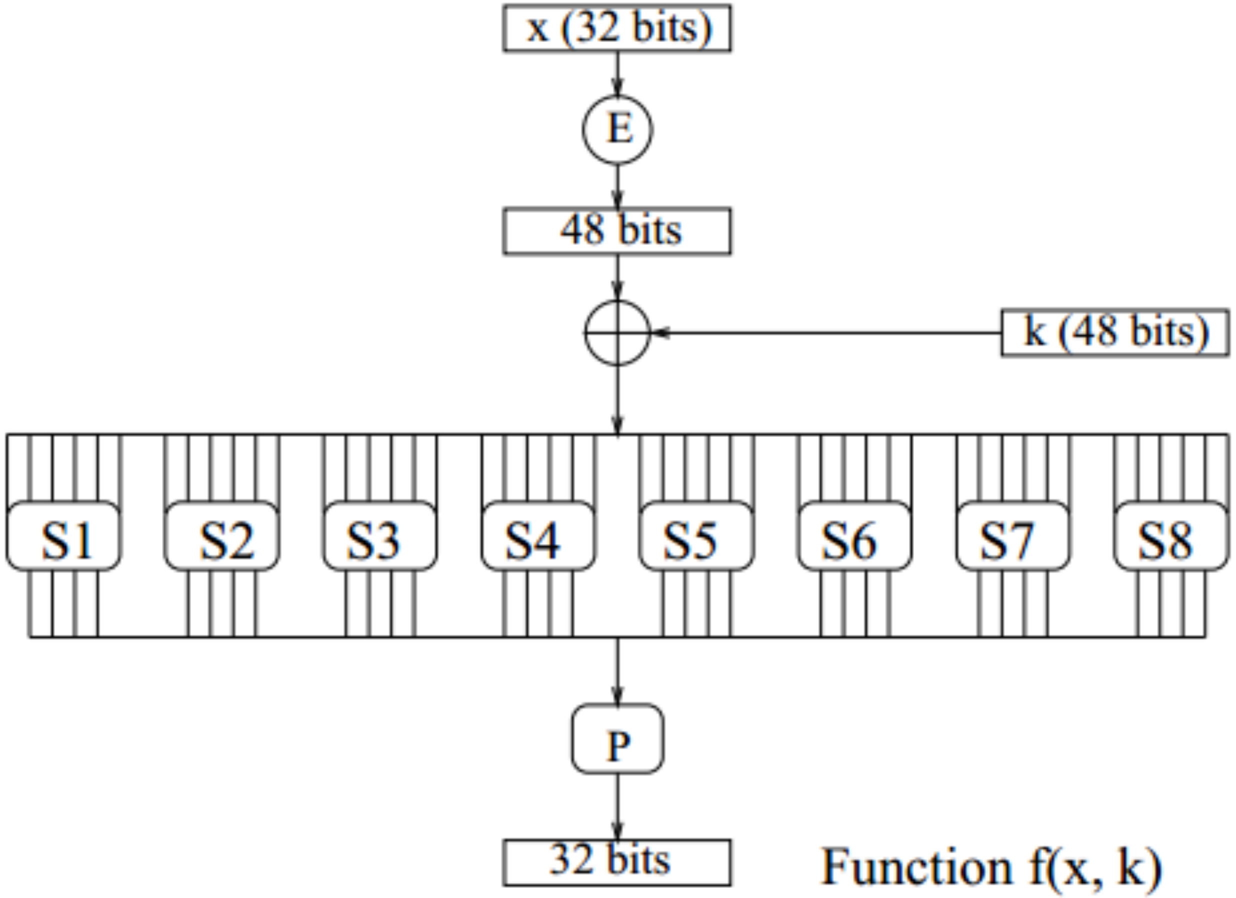

1
2
8
25
40
58
64
Initial
Permutation
1
2
8
25
40
58
64
16 Rounds
1
2
8
25
40
58
64
Final
Permutation
1
2
8
25
40
58
64

Single Round of DES



Li=Ri-1

Ri=Li-1 XOR F(Ri-1,Ki)



Function f(x, k)

Multiple Encryption

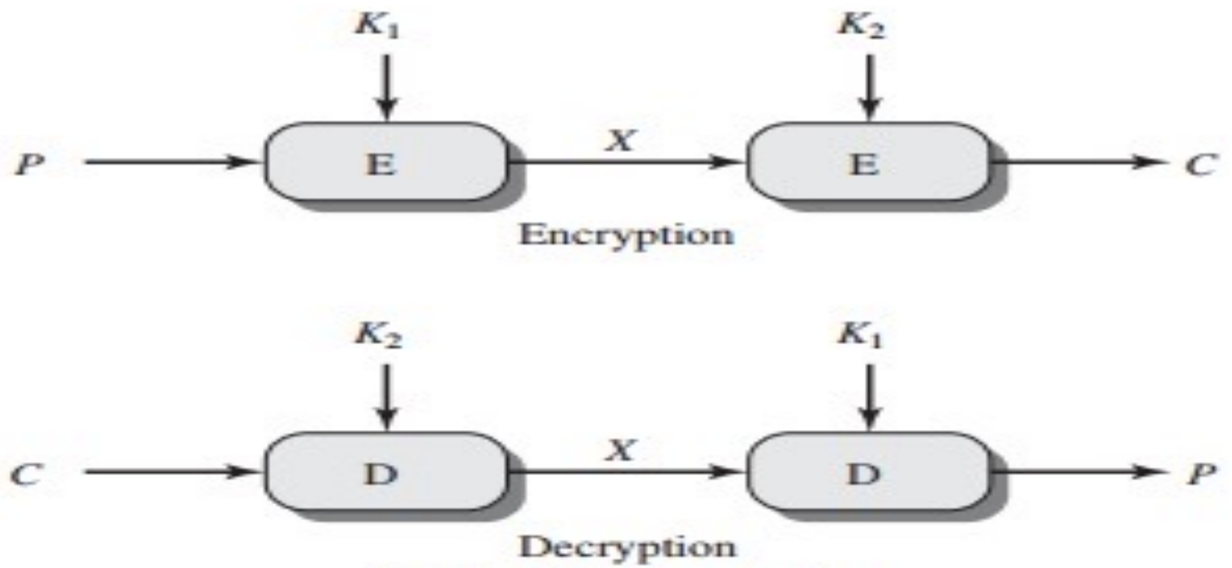
Multiple encryption is a technique in which an encryption algorithm is used multiple times.

Double DES

- The simplest form of multiple encryption has **two encryption stages and two keys** Given a plaintext P and two encryption keys $K1$ and $K2$, ciphertext C is generated as
  - $C = E(K2, E(K1, P))$
- Decryption requires that the keys be applied in reverse order:
  - $P = D(K1, D(K2, C))$
- For DES, this scheme apparently involves a key length of 56 * 2 = 112 bits, resulting in a dramatic increase in cryptographic strength.

$$C = E(K2, E(K1, P))$$

$$P = D(K1, D(K2, C))$$

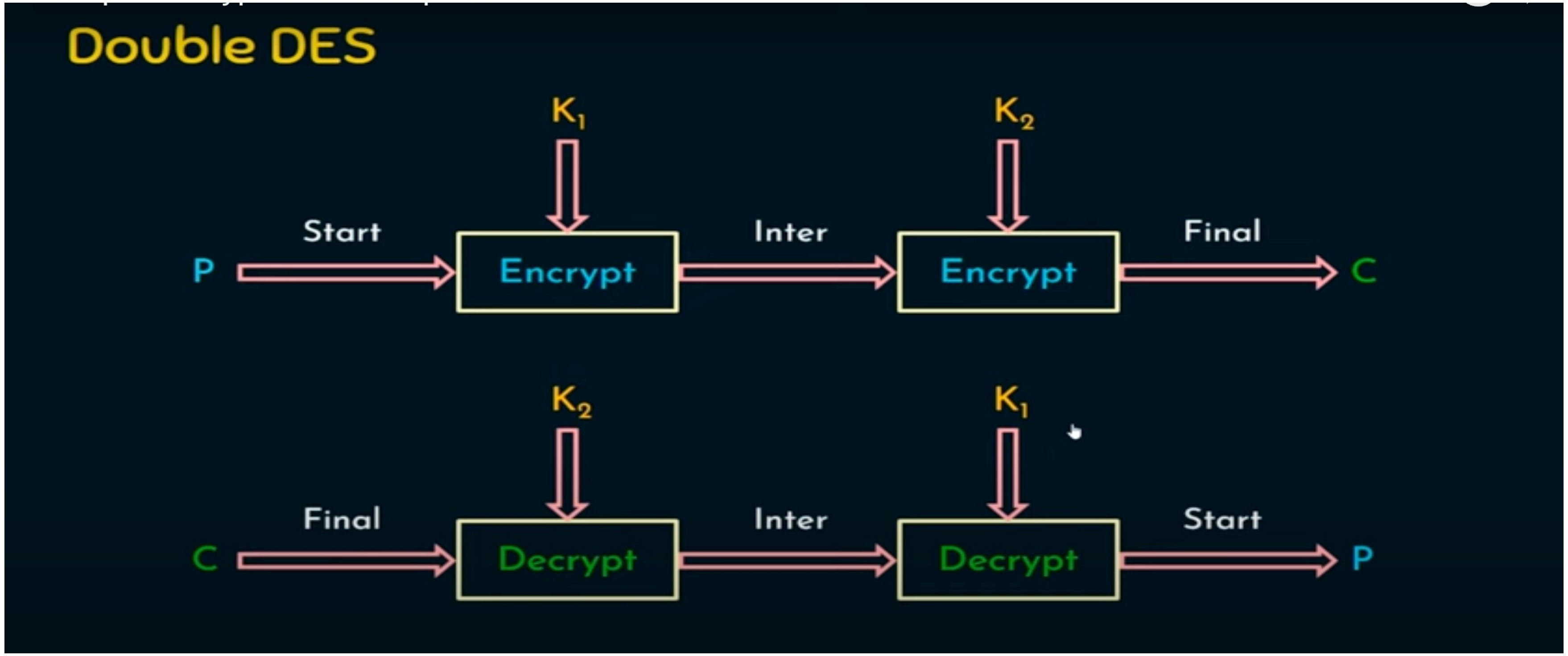


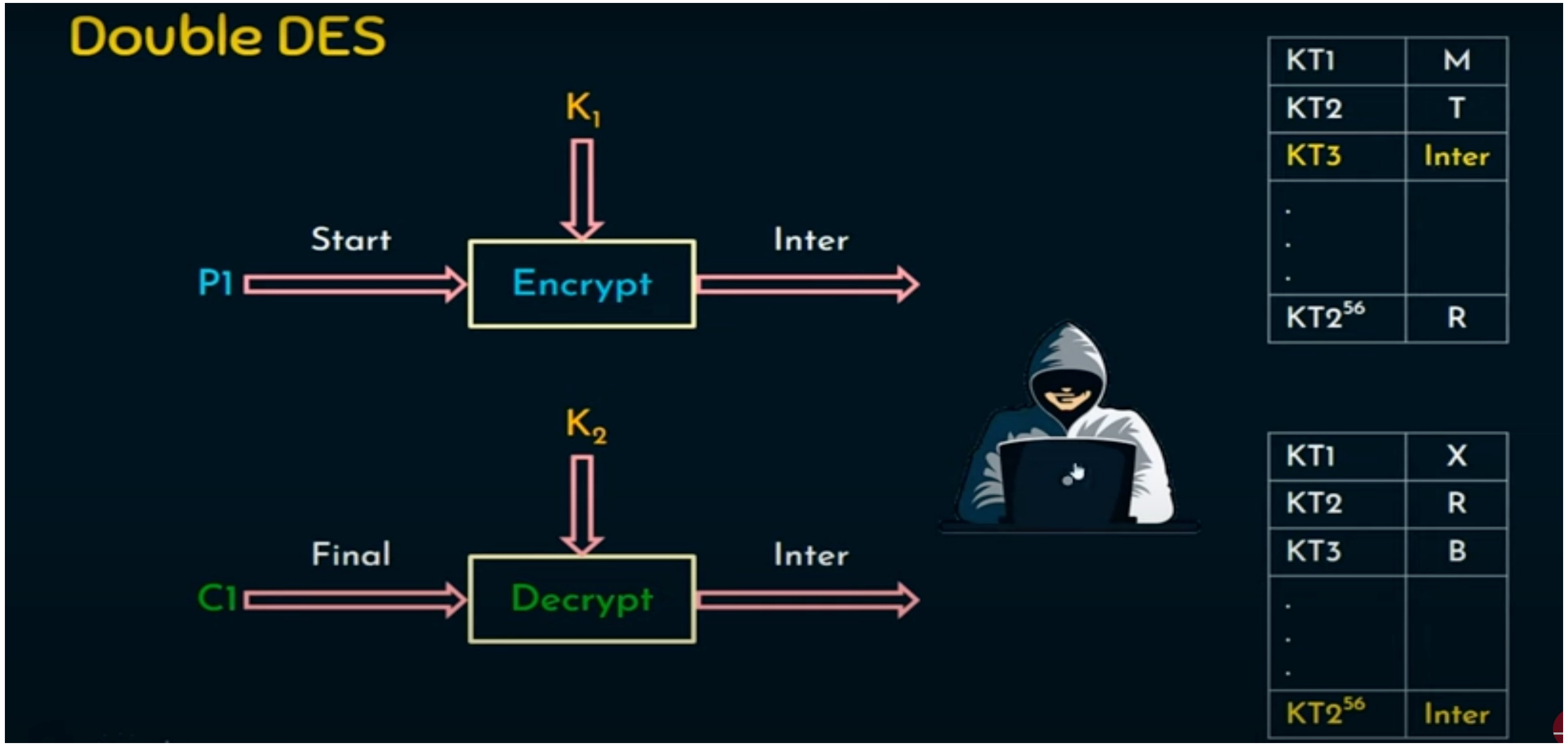
(a) Double encryption

Meet in the Middle Attack

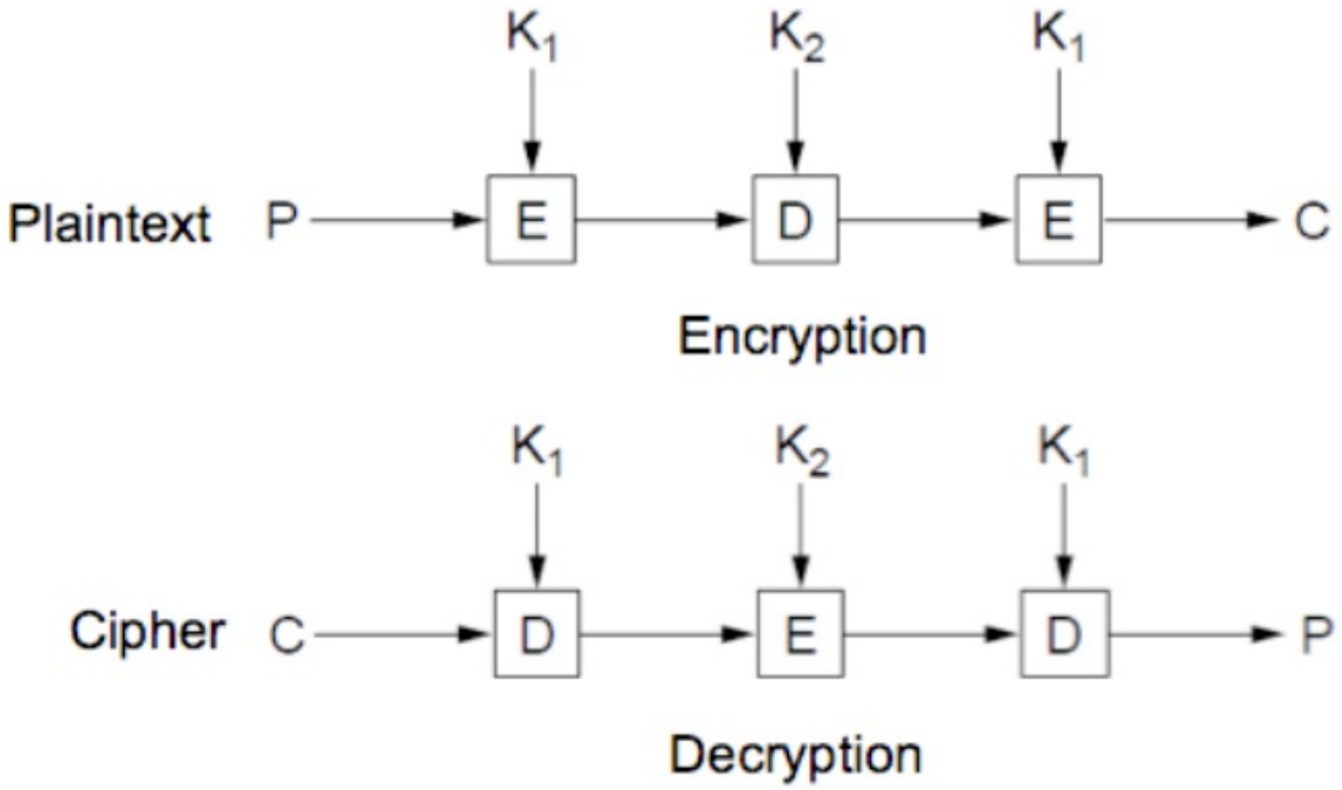
- Given a known pair, (P, C), the attack proceeds as follows.
- First, encrypt P for all 2^{56} possible values of $K1$.
- Store these results in a table
- Next, decrypt C using all 2^{56} possible values of $K2$.
- As each decryption isproduced, check the result against the table for a match.
- If a match occurs, then test the two resulting keys against a new known plaintext–ciphertext pair.

Plain Text:Start
Cipher Text: Final

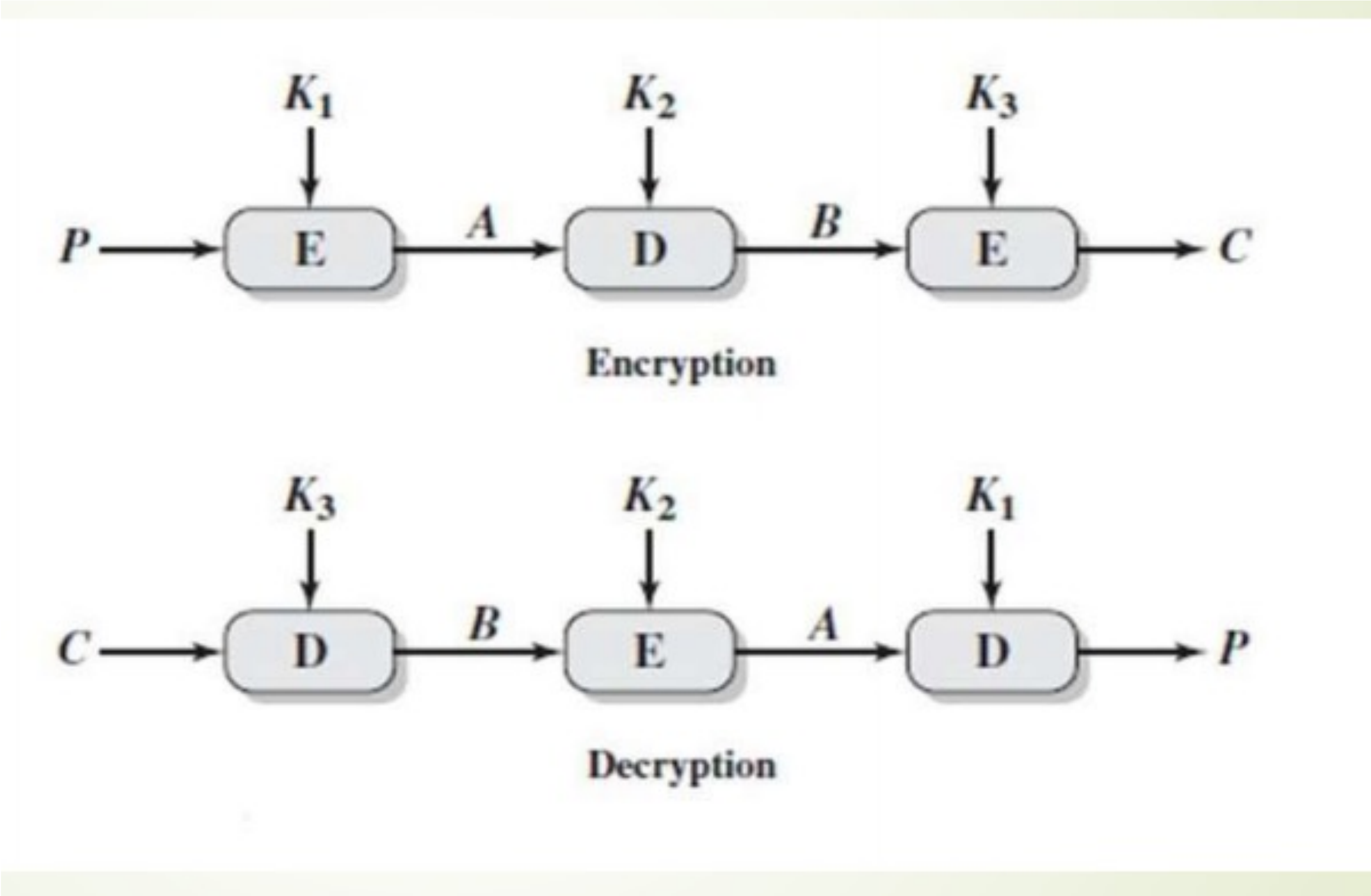



Double DES
K1
Start
P1
Encrypt
Inter
K2
Final
C1
Decrypt
Inter
KT1 M
KT2 T
KT3 Inter
KT2^56 R
KT1 X
KT2 R
KT3 B
KT2^56 Inter

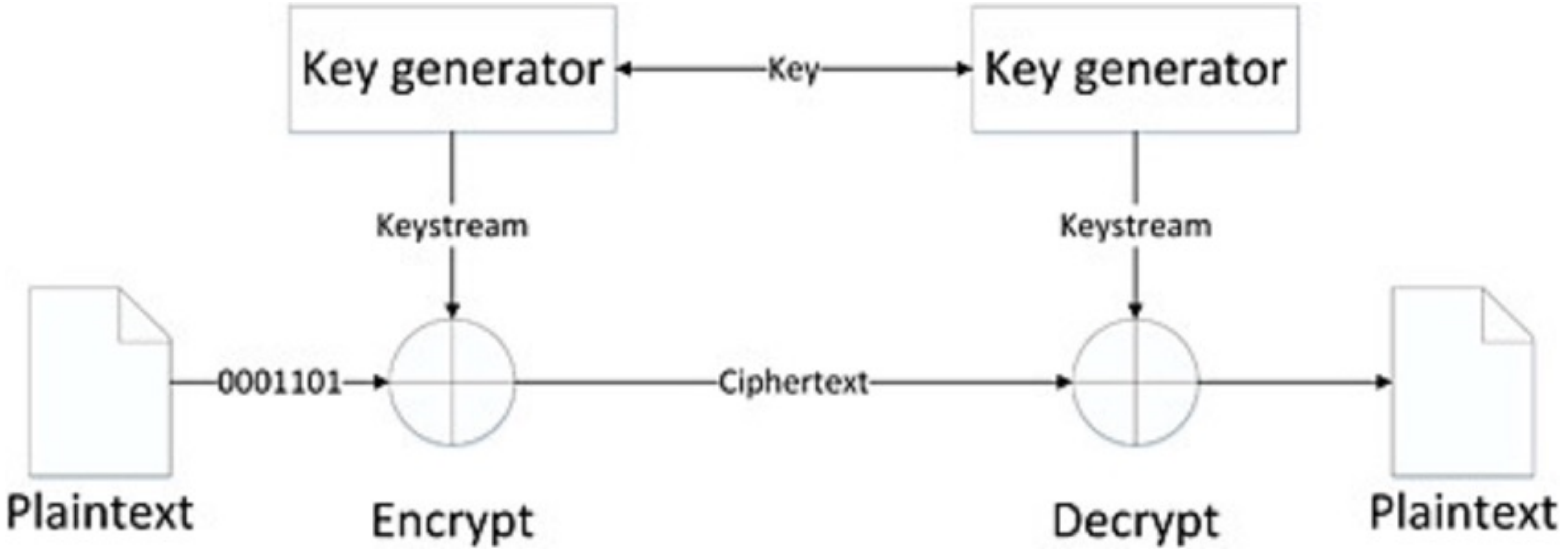
Triple DES with 2 Keys



Triple DES with 3 Keys



Stream Cipher



- A typical stream cipher encrypts plaintext one byte at a time,
- A Key stream is one that is generated by an algorithm but is unpredictable without knowledge of the input key.
- The output of the generator(**keystream**), is combined one byte at a time with the plaintext stream using the bitwise exclusive-OR (XOR) operation

RC4 Algorithm

RC4 is a stream cipher designed in 1987 by Ron Rivest

1.Uses an array State vector S of length 256(0 to 255)

2.Uses a key array of length 256(0 t0 255)

3.Key encoded with ASCII

Steps in RC4

1.Key Scheduling

2.Key Stream Generator

3.Encryption and Decryption

Key Scheduling

- No.of Iterations=Size of S array
- A temporary vector, T, is also created
- If the length of the key K is 256 bytes, then K is transferred to T

Algorithm

```
/* Initial Permutation of S */
 j = 0;
for i = 0 to 255 do                     S[i]=state vector
 j = (j + S[i] + T[i]) mod 256;         T[i]=key array
Swap (S[i], S[j]);
```

S array=[0 1 2 3 4 5 6 7]

Key array=[1 2 3 6]

Plain text=[1 2 2 2]

Initialise T array with key

T =[1 2 3 6 1 2 3 6]

Key Stream Generation

Once the S vector is initialized, the input key is no longer used

No.of Iterations=Size of Key

```
/* Stream Generation */
i, j = 0;
 while (true)
 i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 256;
 k = S[t];
```

New Key is generated

Encryption/Decryption

To encrypt, XOR the value k with the next byte of plaintext.

To decrypt, XOR the value k with the next byte of ciphertext

11001100 plaintext !

XOR

01101100 key stream

10100000 ciphertext