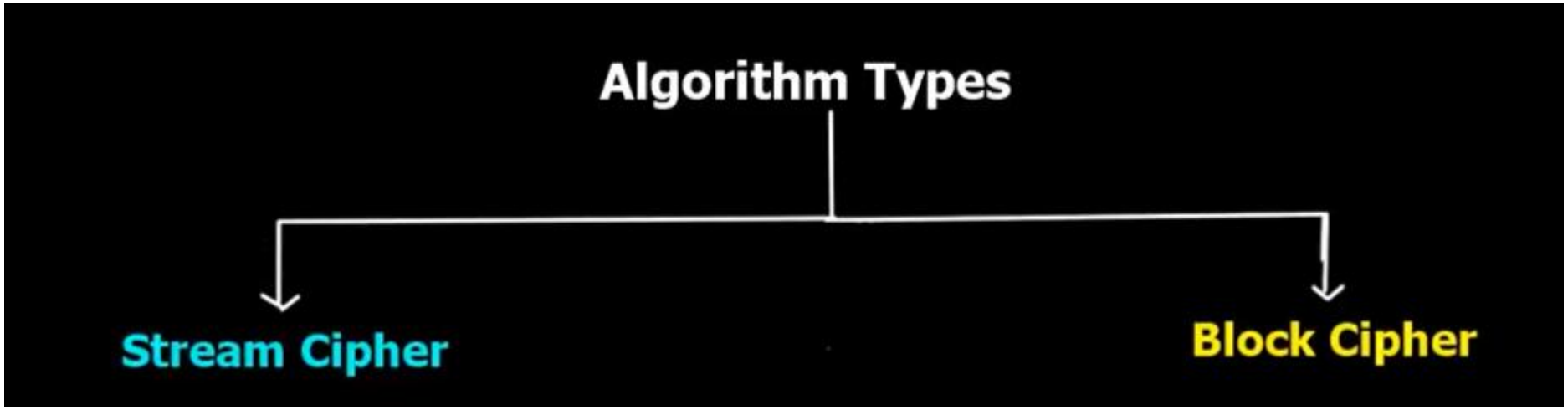
UNIT–II

Computer-based Symmetric Key Cryptographic Algorithms:

Algorithm Types and Modes, An overview of Symmetric Key Cryptography, DES, International Data Encryption Algorithm (IDEA), RC5, Blowfish, AES, Differential and Linear Cryptanalysis

Algorithm Types

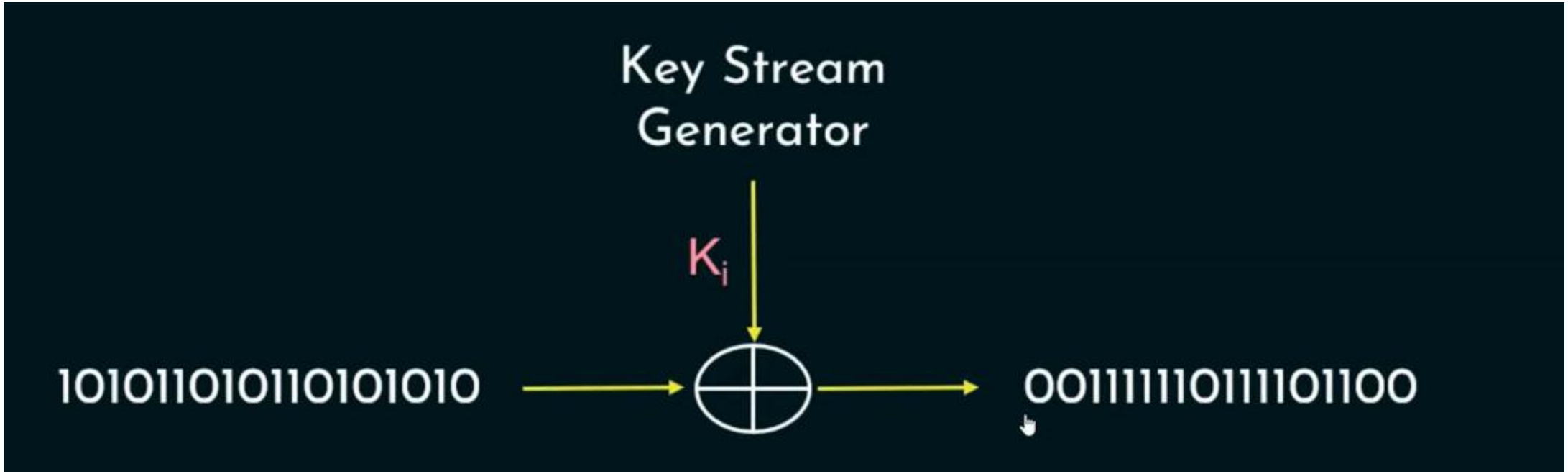


Algorithm Types

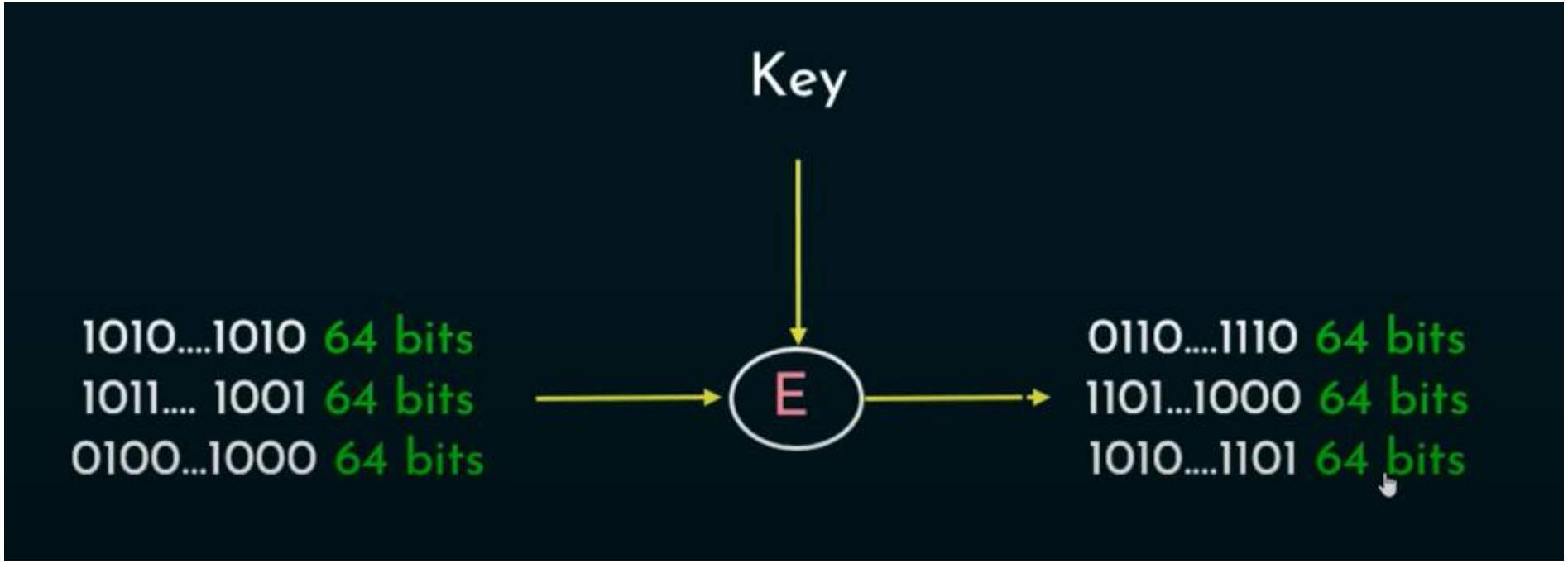
Stream Cipher -
Stream Cipher technique involves the encryption of one plain text bit at a time, the decryption also happens one bit at a time

Block Cipher -
Block Cipher technique involves encryption of one block of text at a time. Decryption also takes one block of encrypted text a time

Stream cipher

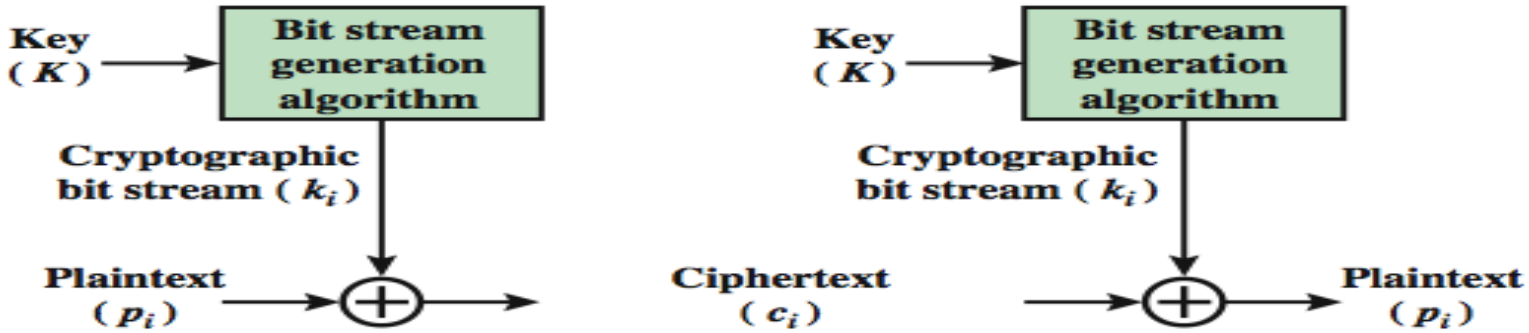


Block cipher

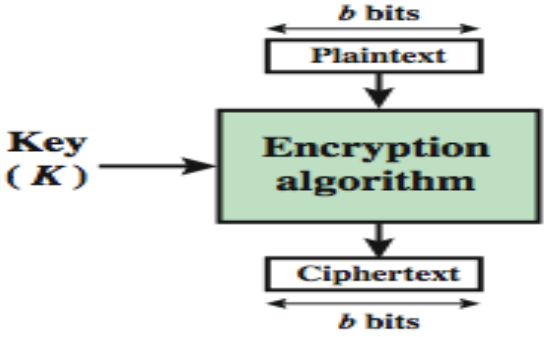


Algorithm Types

Block cipher VS Stream cipher



(a) Stream Cipher Using Algorithmic Bit Stream Generator

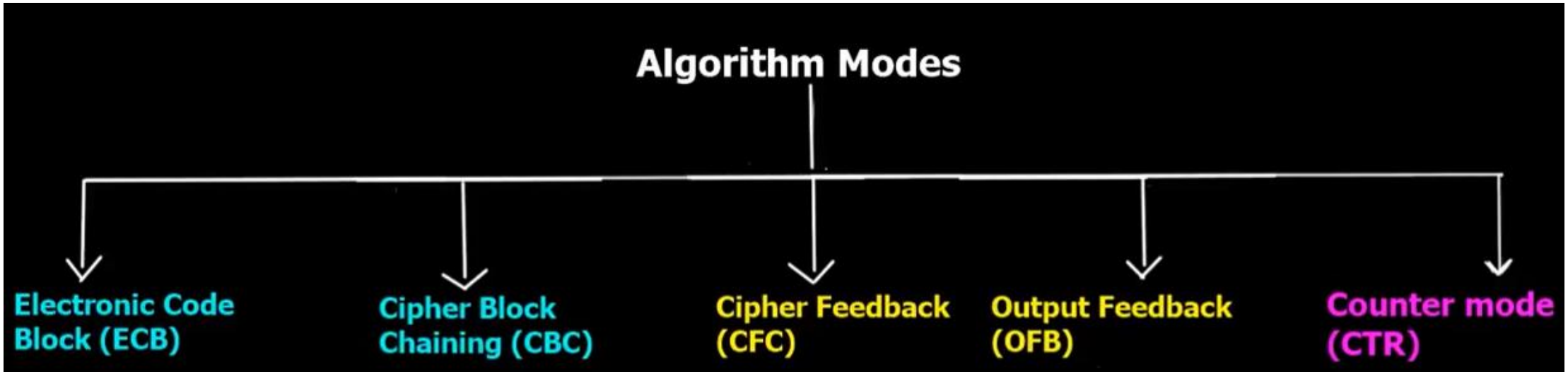


(b) Block Cipher

Algorithm Types

- There are two basic types of symmetric algorithms: block ciphers and stream ciphers.
- **Block ciphers** operate on blocks of plaintext and cipher text—usually of 64 bits but sometimes longer.
- **Stream ciphers** operate on streams of plaintext and cipher text one bit or byte (sometimes even one 32-bit word) at a time.
- With a block cipher, the same plaintext block will always encrypt to the same cipher text block, using the same key. With a stream cipher, the same plaintext bit or byte will encrypt to a different bit or byte every time it is encrypted.

Algorithm Modes



Algorithm Modes

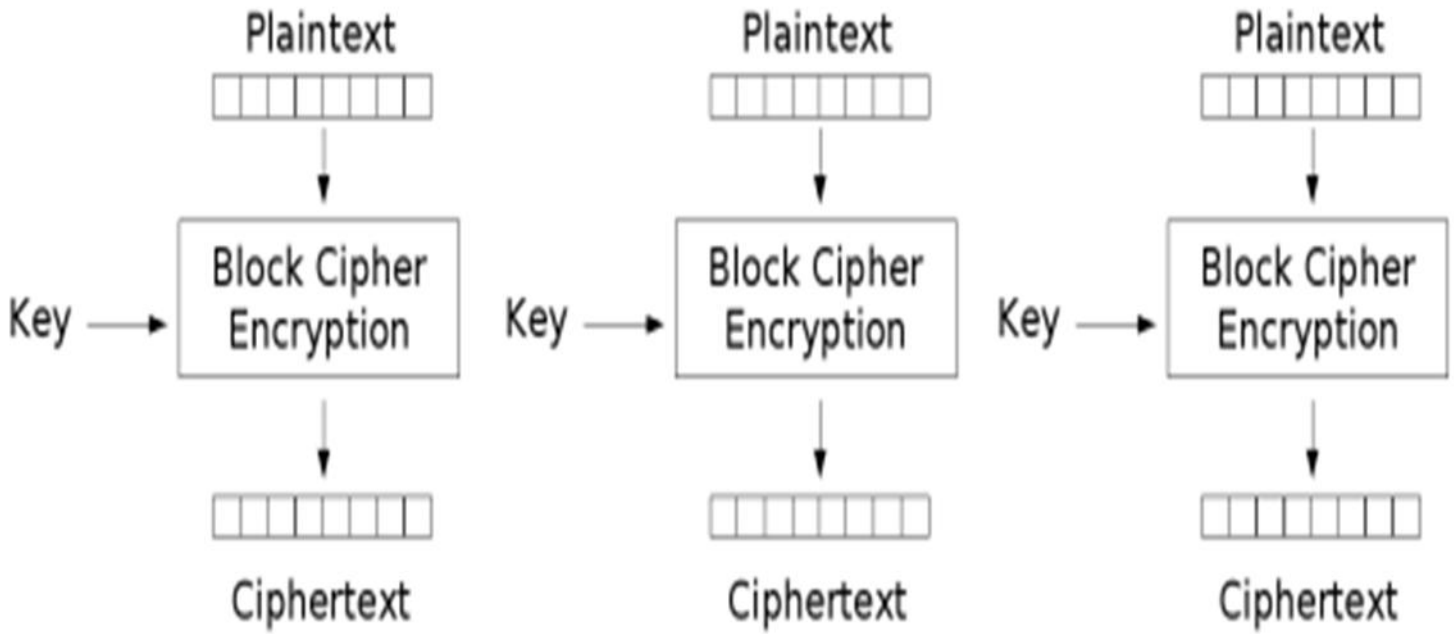
An Algorithm mode is a combination of a series of the basic algorithm steps on block cipher and some kind of feedback from the previous step.

A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block.

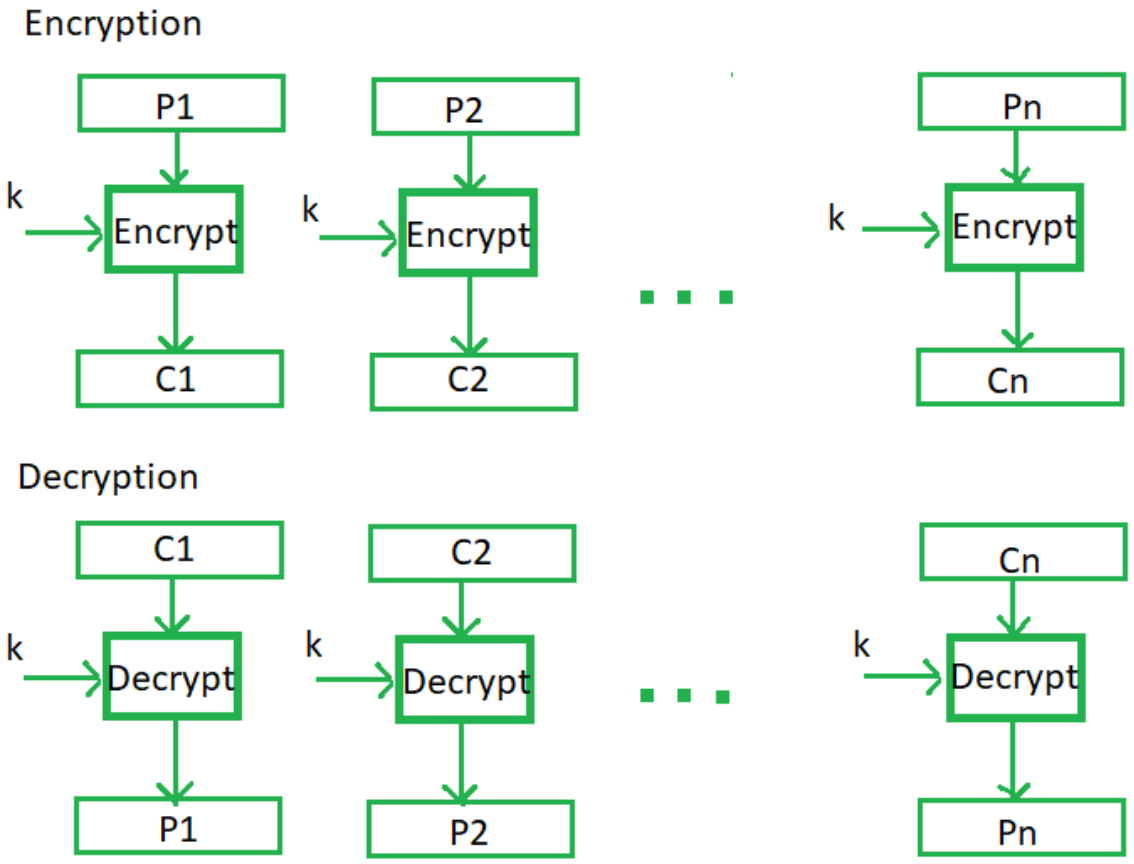
Electronic code book (ECB)

- Simplest mode of operation.
- Plain text message is divided into blocks of 64 bits each.
- Each block then encrypted independently of the other blocks.
- For each blocks same key used for encryption
- ECB is useful only for small message.
- Characteristics of ECB
  - The same b bit block of plaintext , if it appears more than once in message , always produce the same cipher text.

Electronic code book (ECB)



Electronic code book (ECB)

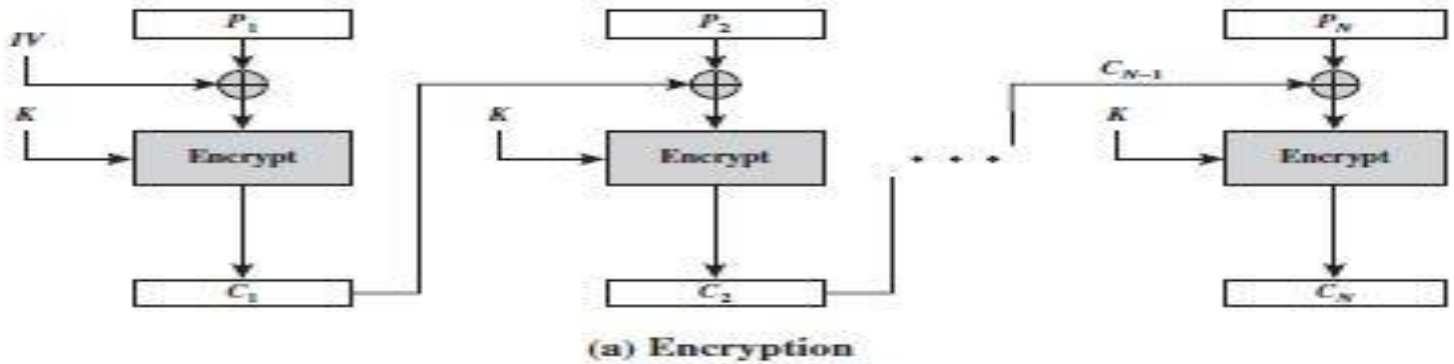


Cipher Block Chaining (CBC)

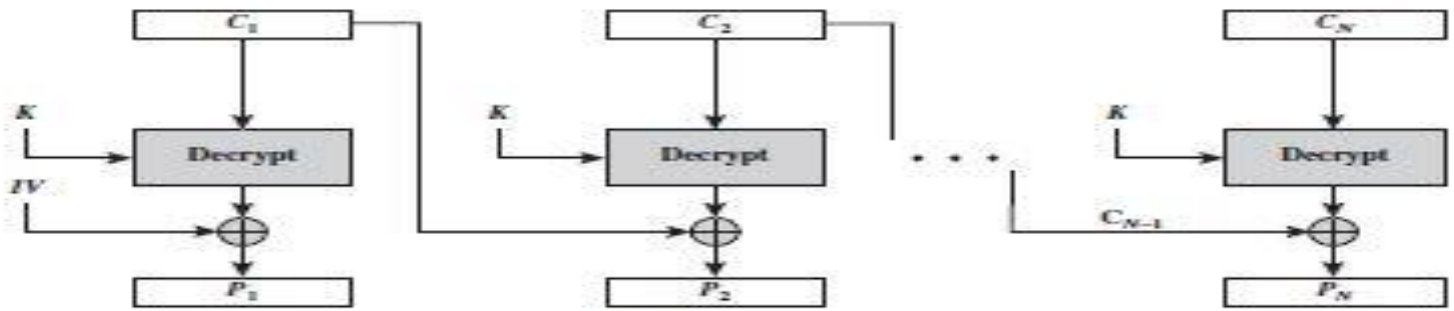
- In Cipher Block Chaining (CBC) message is broken into blocks linked together in encryption operation each previous cipher blocks is chained with current plaintext block, hence name use Initial Vector (IV) to start process
- uses: bulk data encryption, authentication

Cipher Block Chaining (CBC)

$$C_j = \mathrm{E}(K, [C_{j-1} \oplus P_j])$$



(a) Encryption



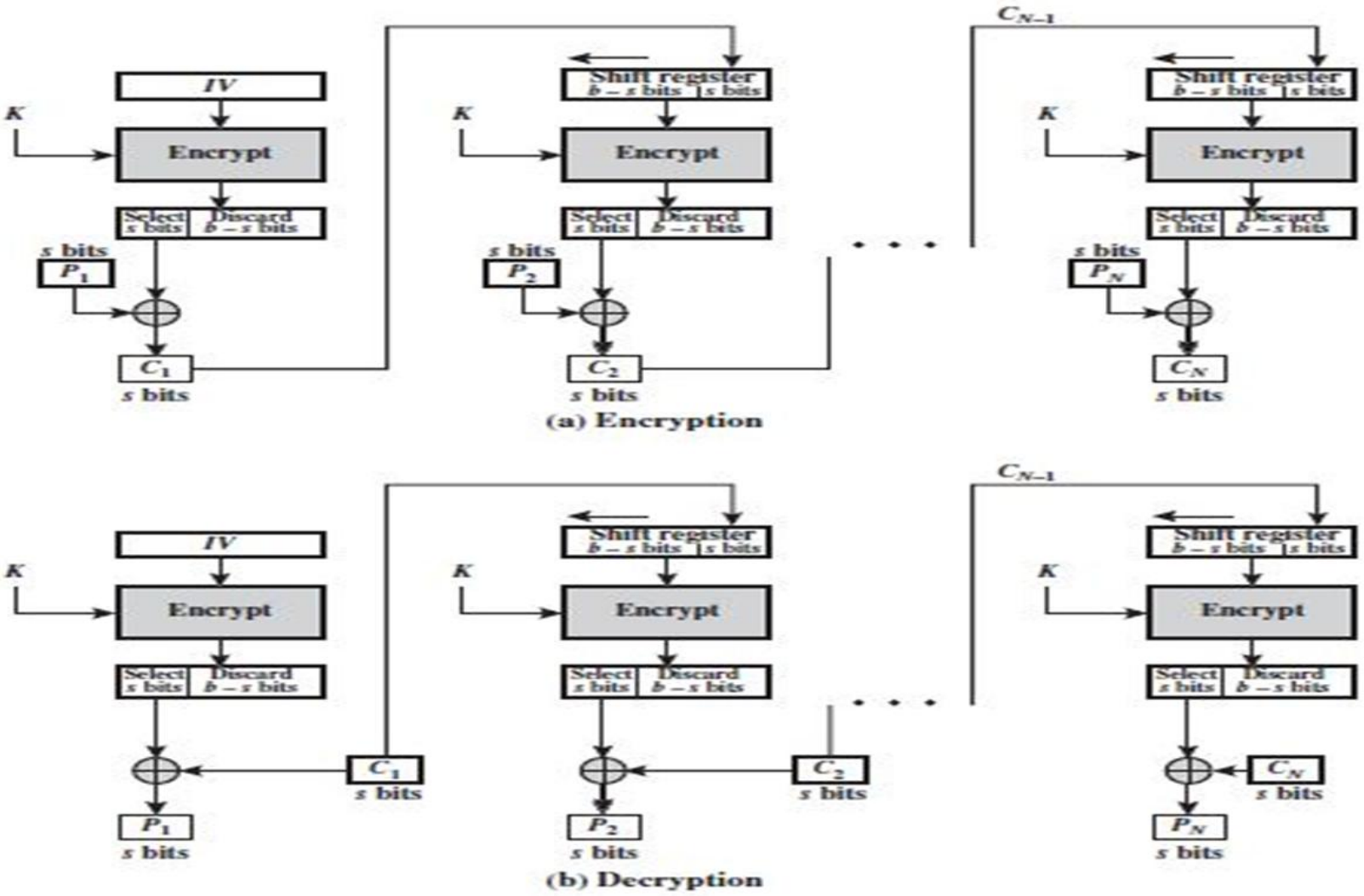
(b) Decryption

Figure 6.4 Cipher Block Chaining (CBC) Mode

Cipher feedback mode(CFB)

- In cryptography, cipher text feedback (CFB), also known as cipher feedback, is a mode of operation for a block cipher.
- Cipher text feedback uses an initialization vector (IV). CFB uses a block cipher as a component of a random number generator. In CFB mode, the previous ciphertext block is encrypted and the output is XORed with the current plaintext block to create the current cipher text block. The XOR operation conceals plaintext patterns.

Cipher feedback mode(CFB)



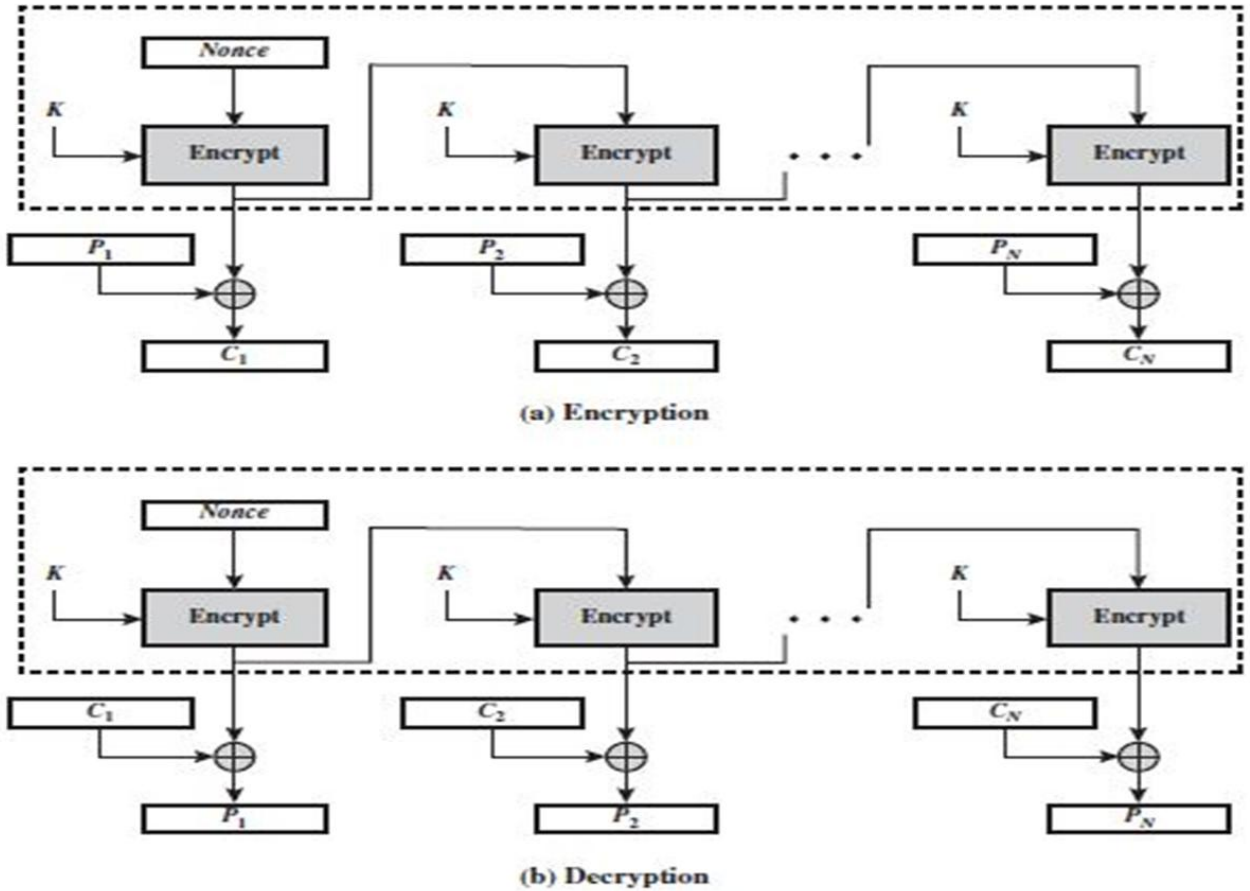
Cipher feedback mode(CFB)

- C1 = P1 (XOR) MSBs [E(k,IV)].
- P1 = C1 (XOR) MSBs [E(k,IV)].
- For DES, b = 64 bits.
- For AES, b = 128 bits.
- Initially S = 8 bits.

Output feedback mode(OFB)

- The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output.
- In output feedback mode, all bits of the block are sent instead of sending selected s bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases the dependency or relationship of the cipher on the plaintext.

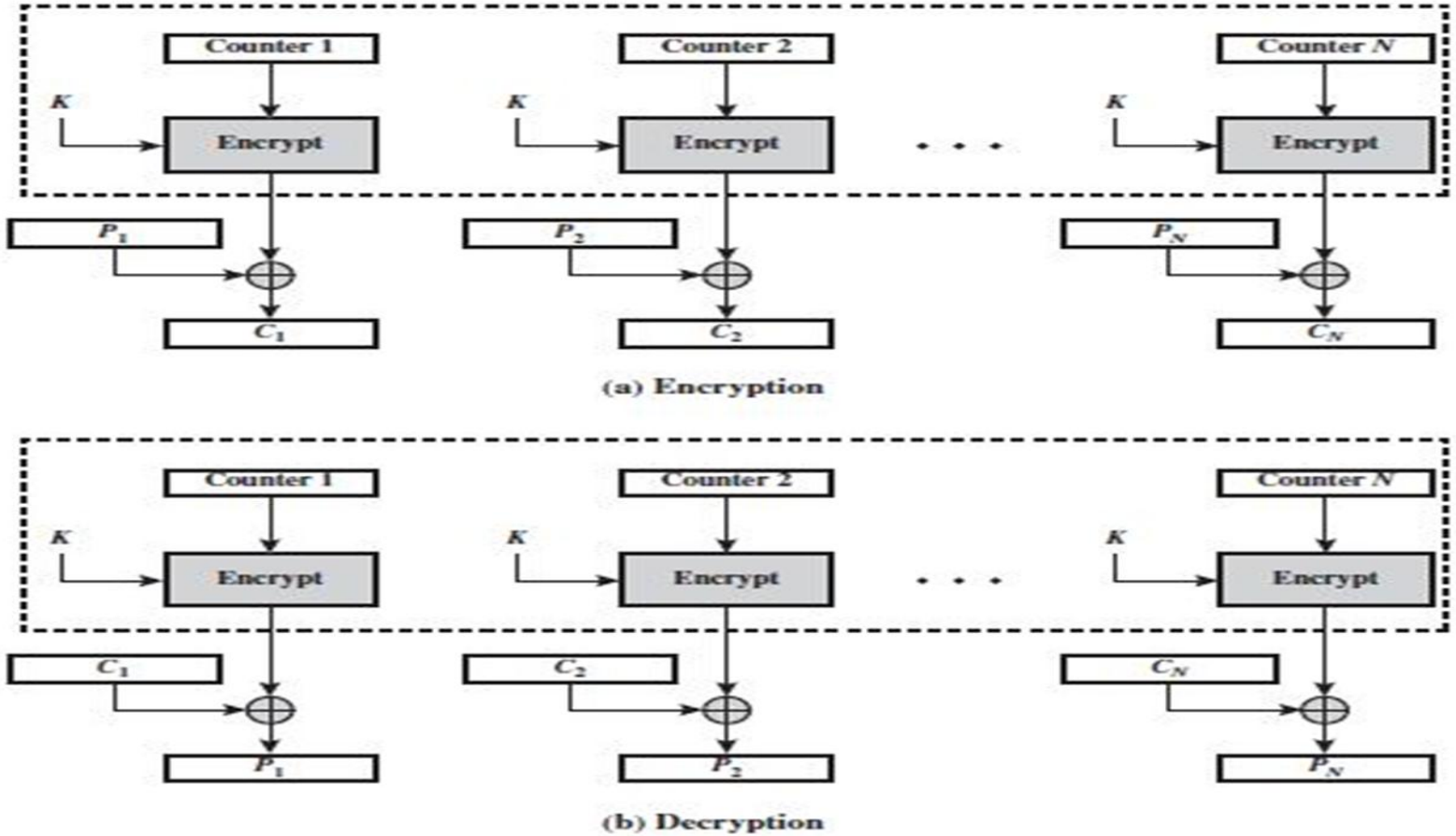
Output feedback mode(OFB)



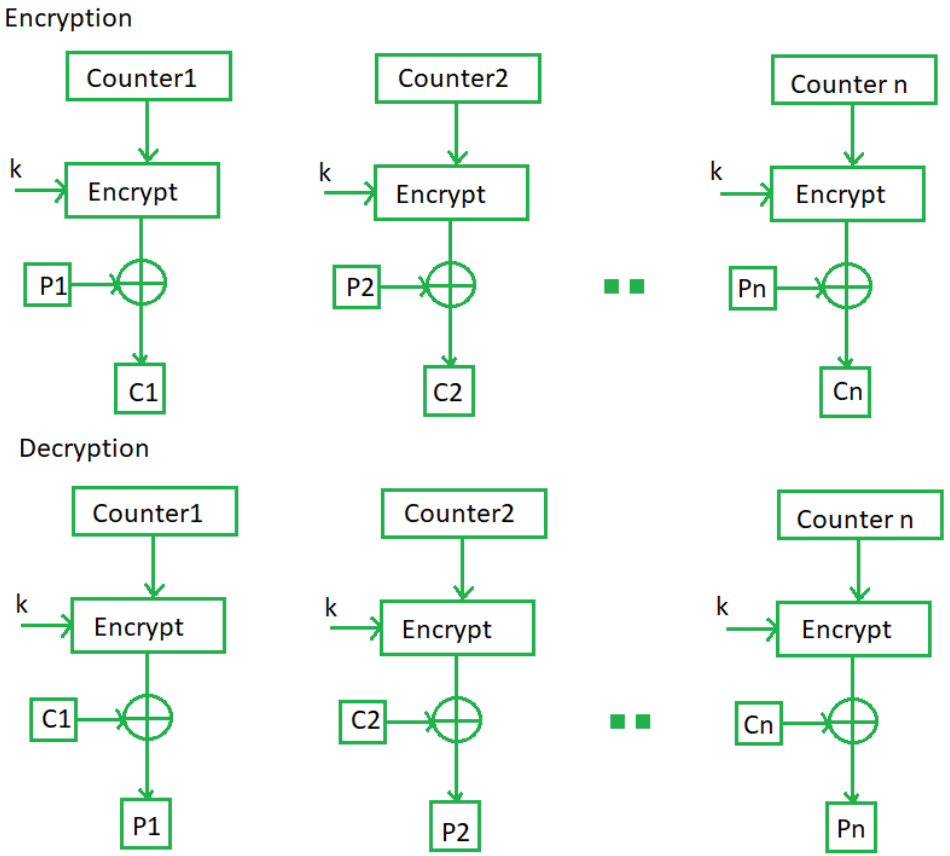
Output feedback mode(OFB)

- The Counter Mode or CTR is a simple counter-based block cipher implementation. Every time a counter-initiated value is encrypted and given as input to XOR with plaintext which results in cipher text block. The CTR mode is independent of feedback use and thus can be implemented in parallel.
- Extremely similar to the CFB.
- Only difference is that in the case of OFB, the output of the IV encryption process is fed into the next stage of encryption process

Counter Mode(CTR)



Counter Mode(CTR)



Counter Mode(CTR)

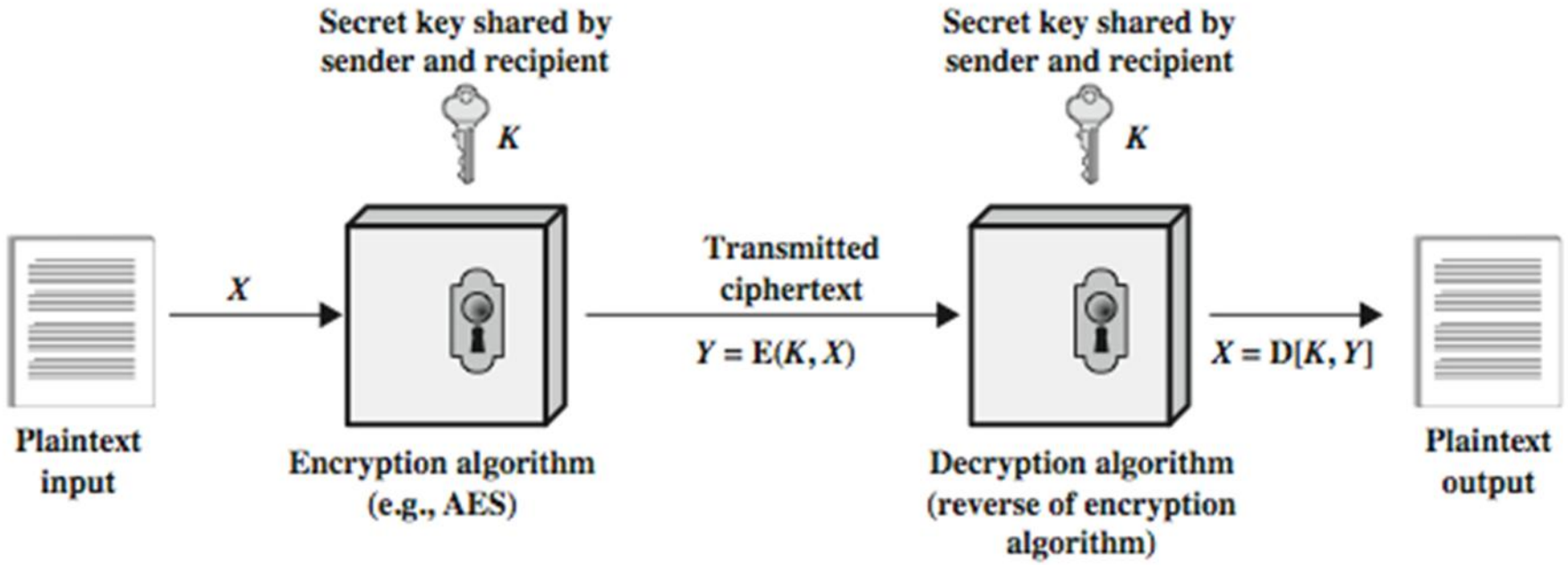
- Similar to the OFB with one variation.
- It uses sequence number called counters as the input to the algorithm.
- After each block is encrypted to fill the register, the next counter value is used.
- Size of counter value is same as plain text block.

Algorithm Modes

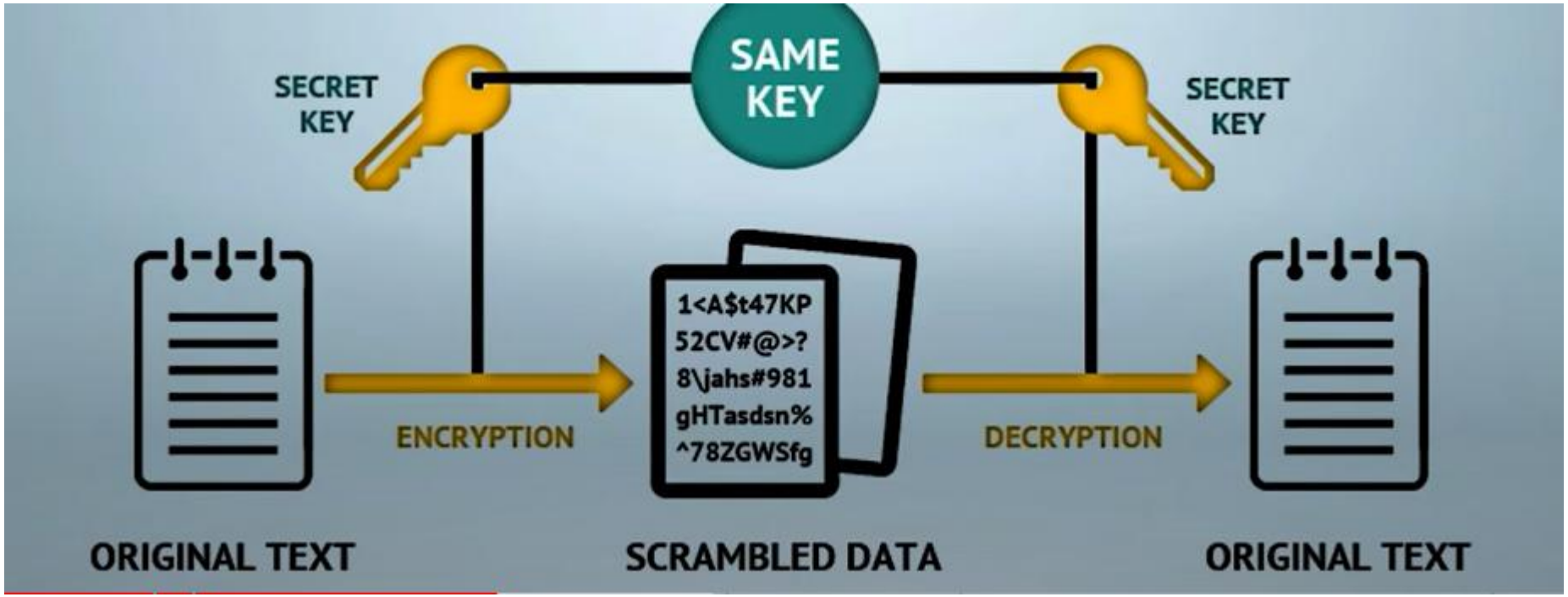
Algorithm Modes: Details and Usage

Algorithm mode	*Details*	*Usage*
Electronic Code Book (ECB)	The same key independently encrypts blocks of text, 64 bits at a time.	Transmitting a single value in a secure fashion (e.g. password or key used for encryption)
Cipher Block Chaining (CBC)	64 bits cipher text from the previous step and 64 bits plain text of the next step are XORed together.	Encrypting blocks of text Authentication
Cipher Feedback (CFB)	*K* bits of randomized cipher text from the previous step and *K* bits plain text of the next step are XORed together.	Transmitting encrypted stream of data Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption step is the preceding DES output.	Transmitting encrypted stream of data
Counter (CTR)	A counter and plain text block are encrypted together, after which the counter is incremented.	Block-oriented transmissions Applications needing high speed

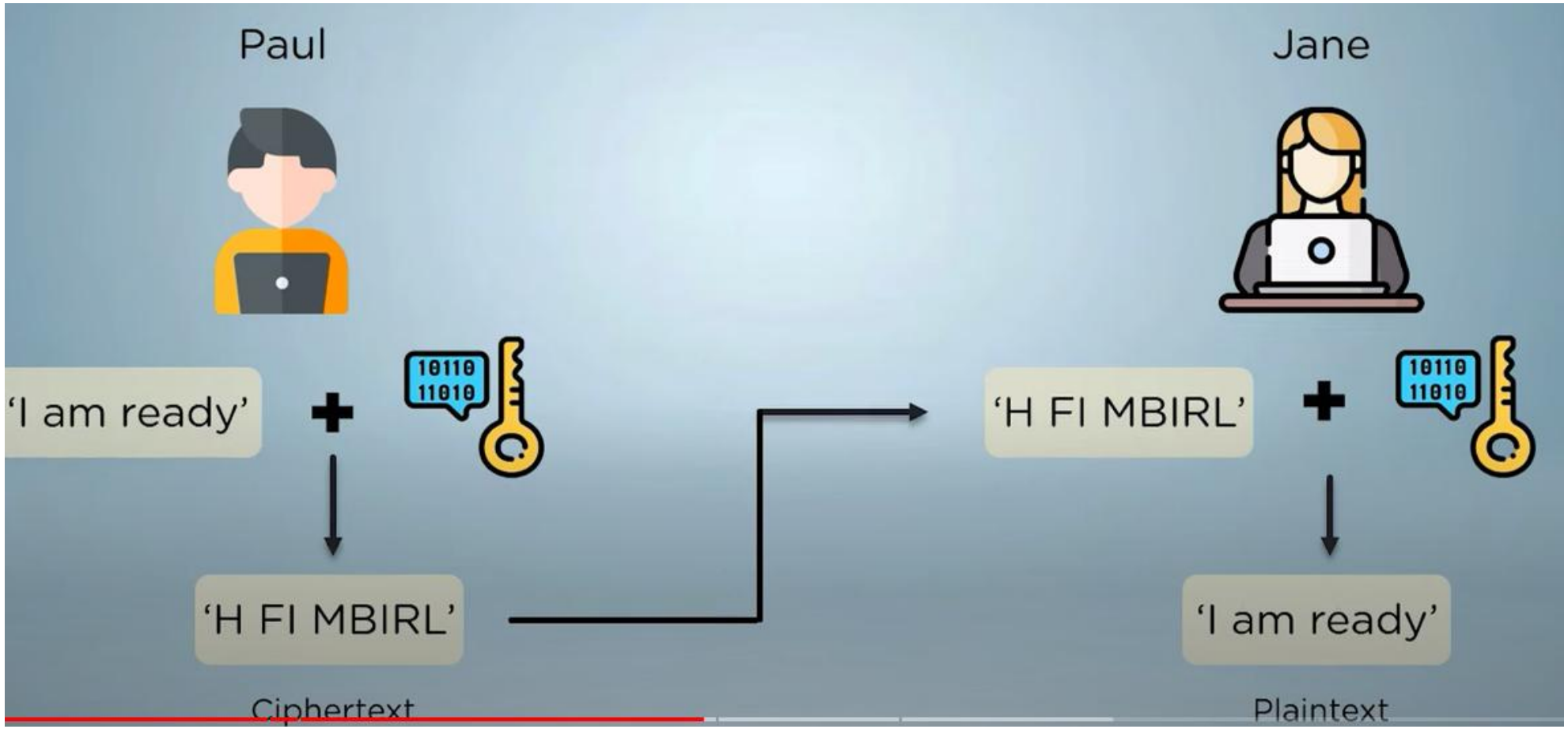
Symmetric Key Cryptography



An overview of Symmetric Key Cryptography



An overview of Symmetric Key Cryptography



An overview of Symmetric Key Cryptography

- Symmetric key cryptography involves using the same secret key to encrypt and decrypt the data. The encryption key is shared between the sender and the receiver of the message. This means that both the sender and receiver have the same key, and they use it to encrypt and decrypt messages. The main advantage of symmetric key cryptography is its speed, as it can encrypt and decrypt large amounts of data quickly. However, the main disadvantage is the challenge of securely sharing the key between the sender and receiver without it being intercepted by a third party.
- Since the same key is used to encrypt and decrypt, the system is also know as private-key encryption
- Symmetric key encryption uses shared secret keys also known as “private-key” encryption
- Primarily used for purpose of confidentiality and authentication
- *Advanced Encryption Standard (AES):* This is a widely used symmetric key encryption algorithm that uses a block cipher to encrypt data.
- *Data Encryption Standard (DES):* This is another popular symmetric key encryption algorithm that uses a block cipher. However, DES is considered less secure than AES and is no longer recommended for use.

Symmetric key distribution

- When two parties share the same key (i.e. symmetric key) that protect from access by others, the process between two parties that exchanges that key called as symmetric key distribution.

- If two person wants to communicates with each other via messages or exchange data without interference of other.

- Two parties/person A and B achieved the key distribution in various ways:

1. ***A** can select a key and physically deliver it to **B**.*
2. *A third party can select the key and physically deliver it to **A** and **B**.*
3. *If **A** and **B** have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.*

4. A trusted third party C delivers the key to A and to B using secure channels to A and to B.

Confusion and Diffusion

Confusion and Diffusion

Confusion

- ★ Making the relationship between the encryption key and the ciphertext as complex as possible.
- ★ Relationship between CT and PT is obscured.
- ★ Given CT, no info about PT, Key, Encryption algorithm etc.,
- ★ Example: Substitution.

Diffusion

- ★ Making each plaintext bit affect as many ciphertext bits as possible.
- ★ 1 bit change in PT, significant effect on CT.

Confusion and Diffusion

- Diffusion: dissipates statistical structure of plaintext over bulk of cipher text
- Confusion: makes relationship between cipher text and key as complex as possible

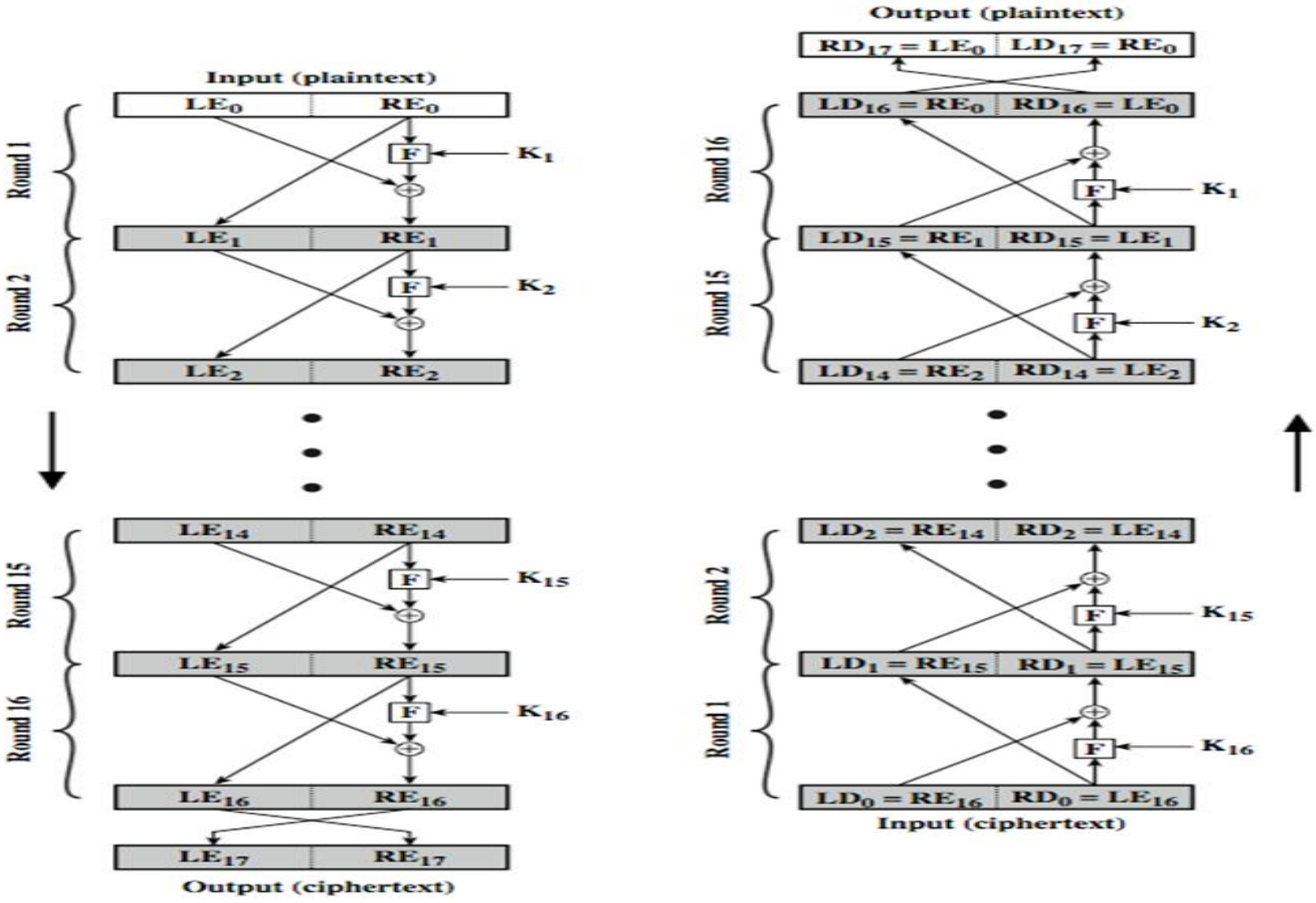
Feistel Cipher Structure

- Horst Feistel devised the Feistel cipher based on concept of invertible product cipher
- partitions input block into two halves
- process through multiple rounds which perform a substitution on left data half
- based on round function of right half & subkey then have permutation swapping halves

Feistel Cipher Structure steps

- block size
- key size
- number of rounds
- subkey generation algorithm
- round function
- fast software en/decryption
- ease of analysis

Feistel Cipher Structure



DES(Data Encryption standard) size

- Input : 64 bits.
- Output : 64 bits.
- Main Key : 64 bits.
- Subkey : 56 bits.
- Round key : 48 bits
- No. of rounds : 16 rounds.

DES Algorithm

The Data Encryption Standard (DES):

This algorithm adopted in 1977 by the National Institute of Standards and Technology (NIST). The algorithm itself is referred to as the Data Encryption Algorithm (DEA). For DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.

DES encryption algorithm:

The general structure of the DES consists of (1) key schedule, (2) round function and (3) initial and final permutation.

Step1: Plaintext is broken into blocks of length 64 bits.

Step2: The 64-bit block undergoes an initial permutation (IP) using initial permutation IP table, IP(M).

Step3: The 64-bit permuted input is divided into two 32-bit blocks: left (L) and right (R). The initial values of the left and right blocks are denoted L_0 and R_0.

Step4: There are 16 rounds of operations on the L and R blocks. During each round, the following formula is applied:

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \text{ XOR } F(R_{n-1}, K_n)$$

DES Block Cipher

Step5: The function **F(.)** represents the heart of the DES algorithm. This function implements the following operations:

1-Expansion: The right **32-bit** half-block is expanded to **48 bits** using the **expansion permutation** (**E**) table, $E(R_{n-1})$.

2-Key mixing: The expanded result is combined with a **subkey** using an XOR operation. Sixteen 48-bit subkeys (one for each round) are derived from the main key using the **key schedule**, $K_n + E(R_{n-1})$.

3-Substitution: After mixing in the subkeys, the block is divided into eight 6-bit pieces and fed into the substitution boxes (S-boxes), which implements nonlinear transformation. Each 6-bit piece uses as an address in the **S-boxes** where the first and last bits are used to address the i^{th} row and the middle four bits to address the j^{th} column in the S-boxes. The output of each **S-box is 4-bit length** piece. The output of all **eight S-boxes** is then combined into **32** bit section.

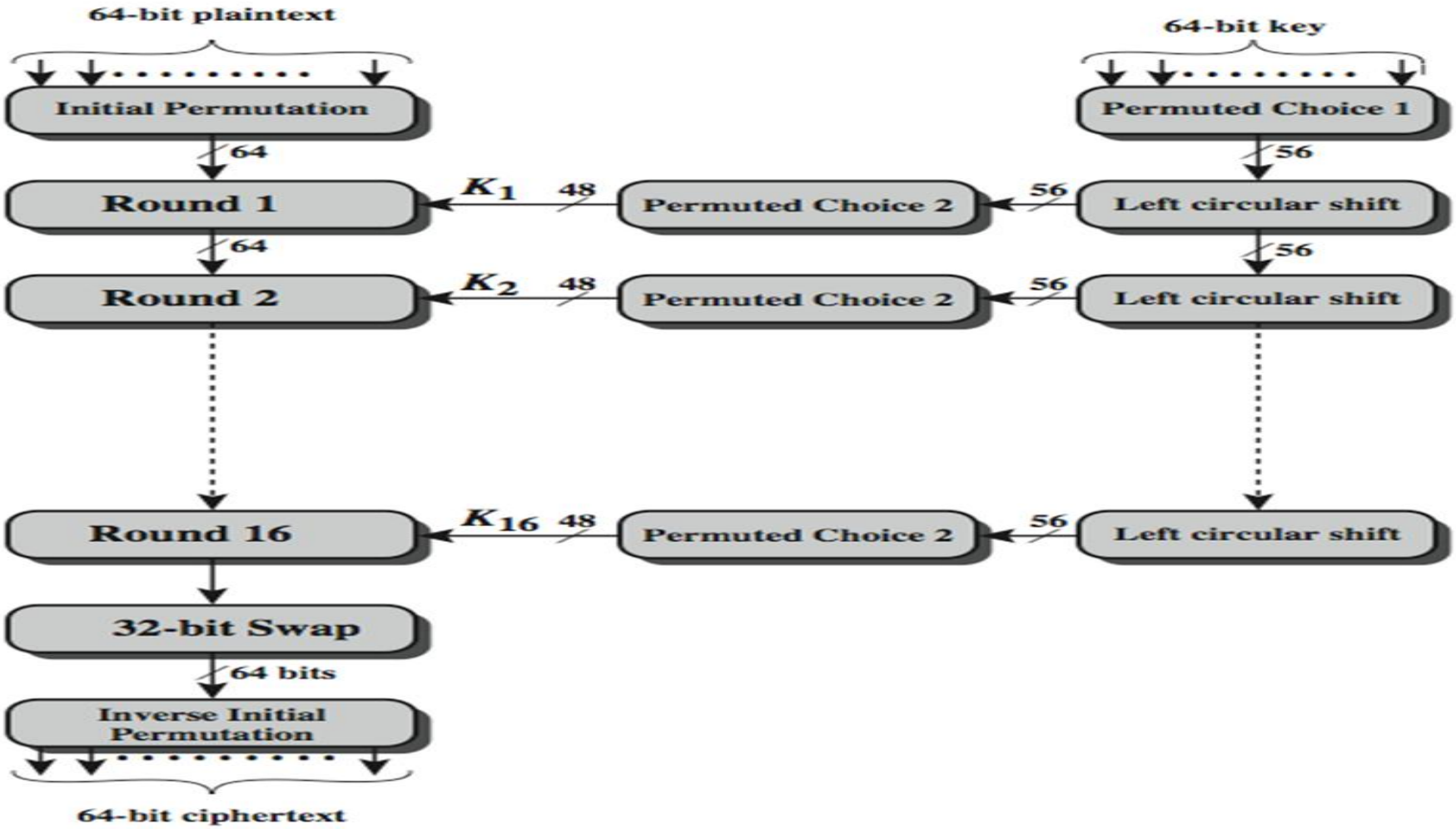
$K_n + E(R_{n-1}) = B_1B_2B_3B_4B_5B_6B_7B_8$

$S(Kn + E(Rn-1)) = S1(B_1)S2(B_2)S3(B_3)S4(B_4)S5(B_5)S6(B_6)S7(B_7)S8(B_8)$

4-Permutation: The **32** bits outputs from the S-boxes are rearranged using the **P-box**, $F=P(S(K_n + E(R_{n-1})))$

Step6: The results from the final DES round (i.e., L_{16} and R_{16}) are recombined into a 64-bit value and rearranged using an inverse initial permutation **(IP^{-1})** table. The output from IP^{-1} is the 64-bit ciphertext block.

Data Encryption Standard (DES)

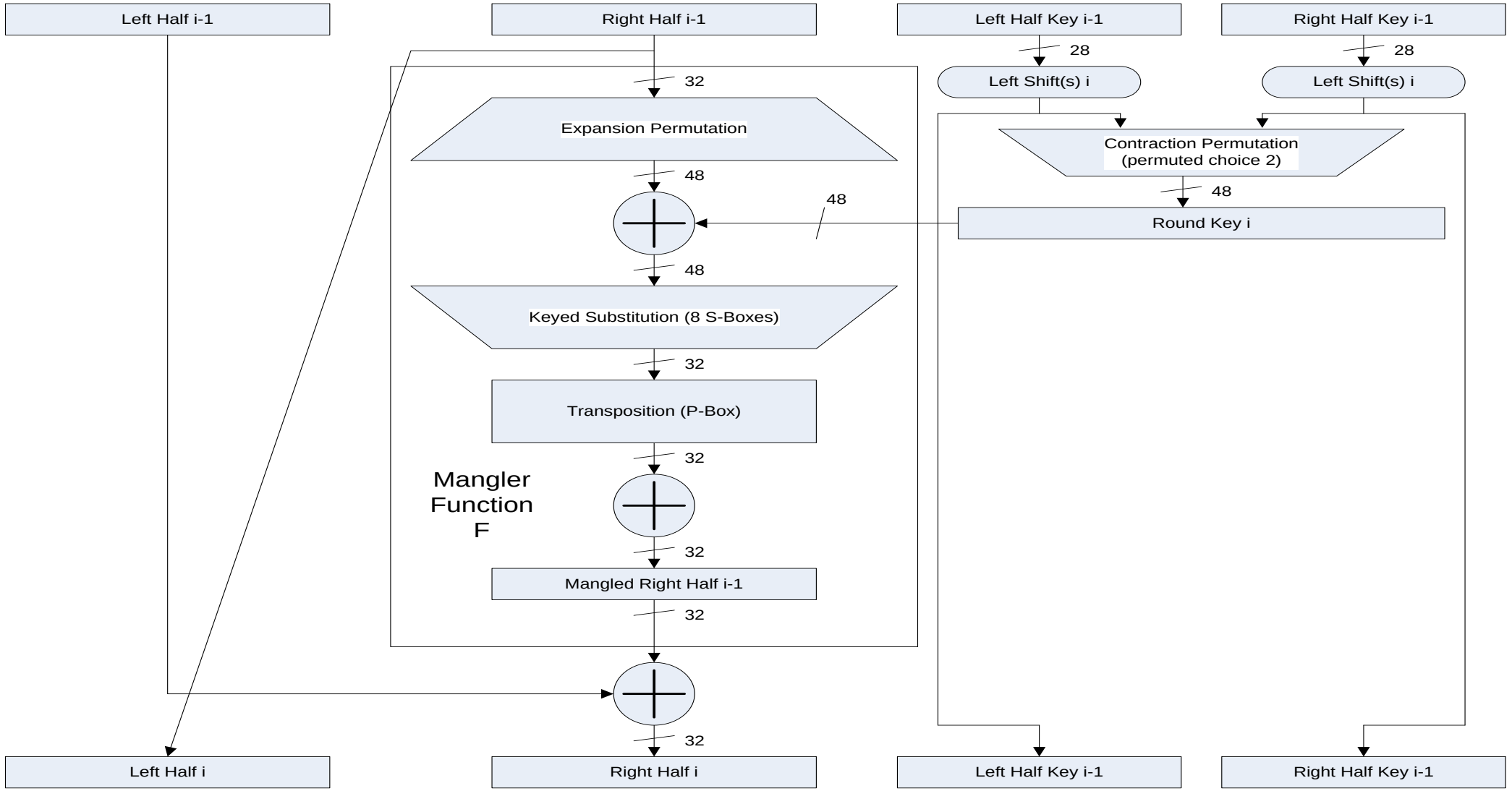


Initial Permutation

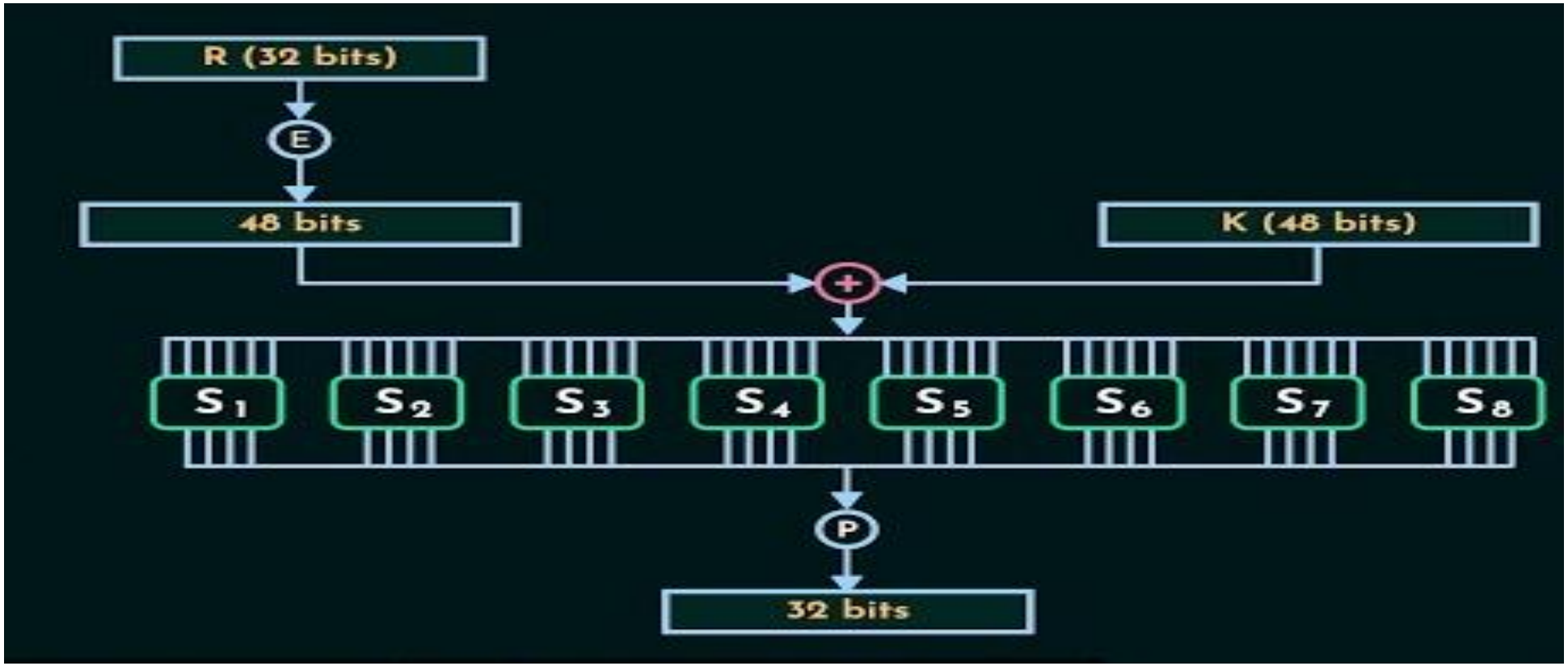
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

DES Round Structure



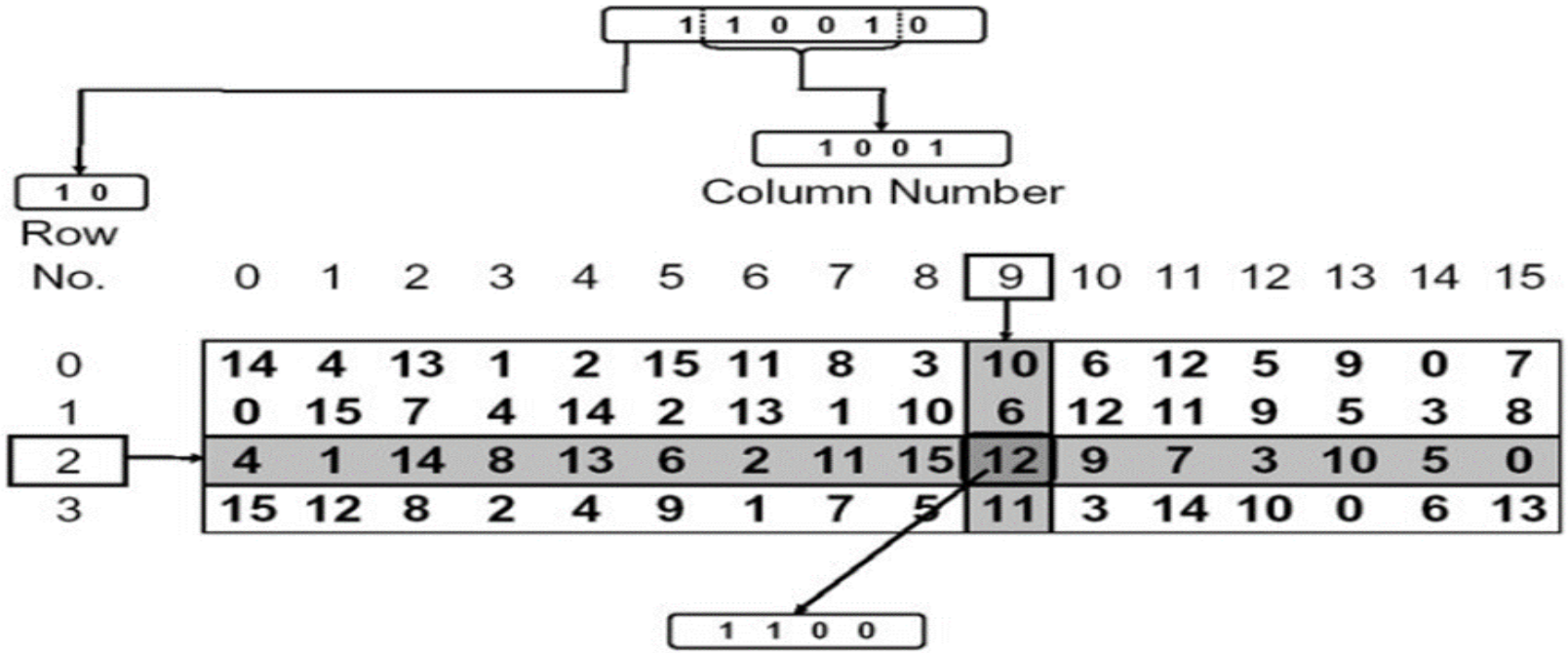
Mangler function F



The Expansion Permutation

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

S BOX


1 1 0 0 1 0
1 0 0 1
1 0
Row
Column Number
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

The DES S-Boxes

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_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_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_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

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_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_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_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

Tables used in DES key generator

(d) Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Key schedule (generator):

This algorithm generates the subkeys ($K \rightarrow K_1, K_2 \ldots K_{16}$).

1- The 56 bits of the key are selected from the initial 64 by Permuted Choice 1 (PC1) table.

2- The 56 bits are divided into two 28-bit halves.

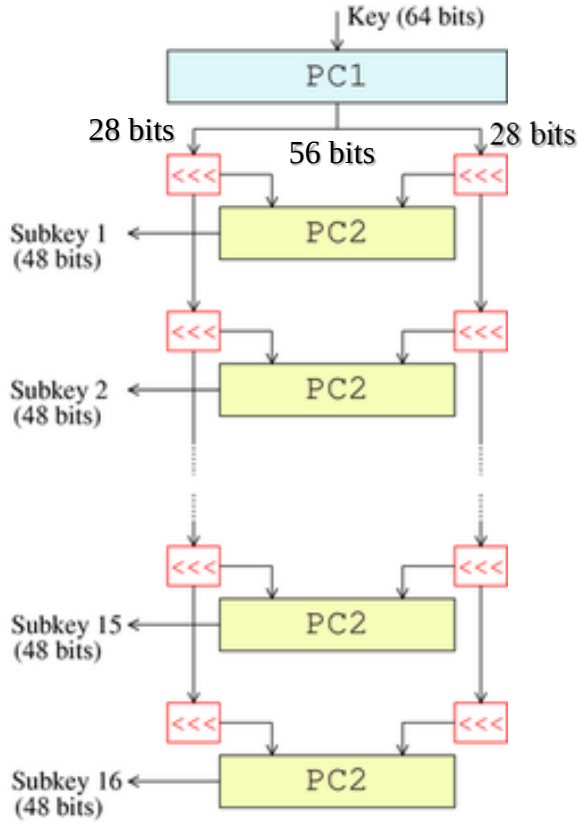
3- In each round, both halves are rotated left by one or two bits (specified for each round).

4- The 48 subkey bits are selected by Permuted Choice 2 (PC2) table (24 bits from the left half, and 24 from the right) and used in each round.

General remarks in the DES:

1- The S-boxes provide the core of the security of DES and the cipher would be linear, and trivially breakable without them.

2- The substitution and permutation in the DES provide confusion and diffusion.



Key schedule structure

Data Encryption Standard (DES)

DES uses a 56-bit key. Actually, The initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

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

Figure - discording of every 8th bit of original key

(a) Input Key

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

(b) Permuted Choice One (PC-1)

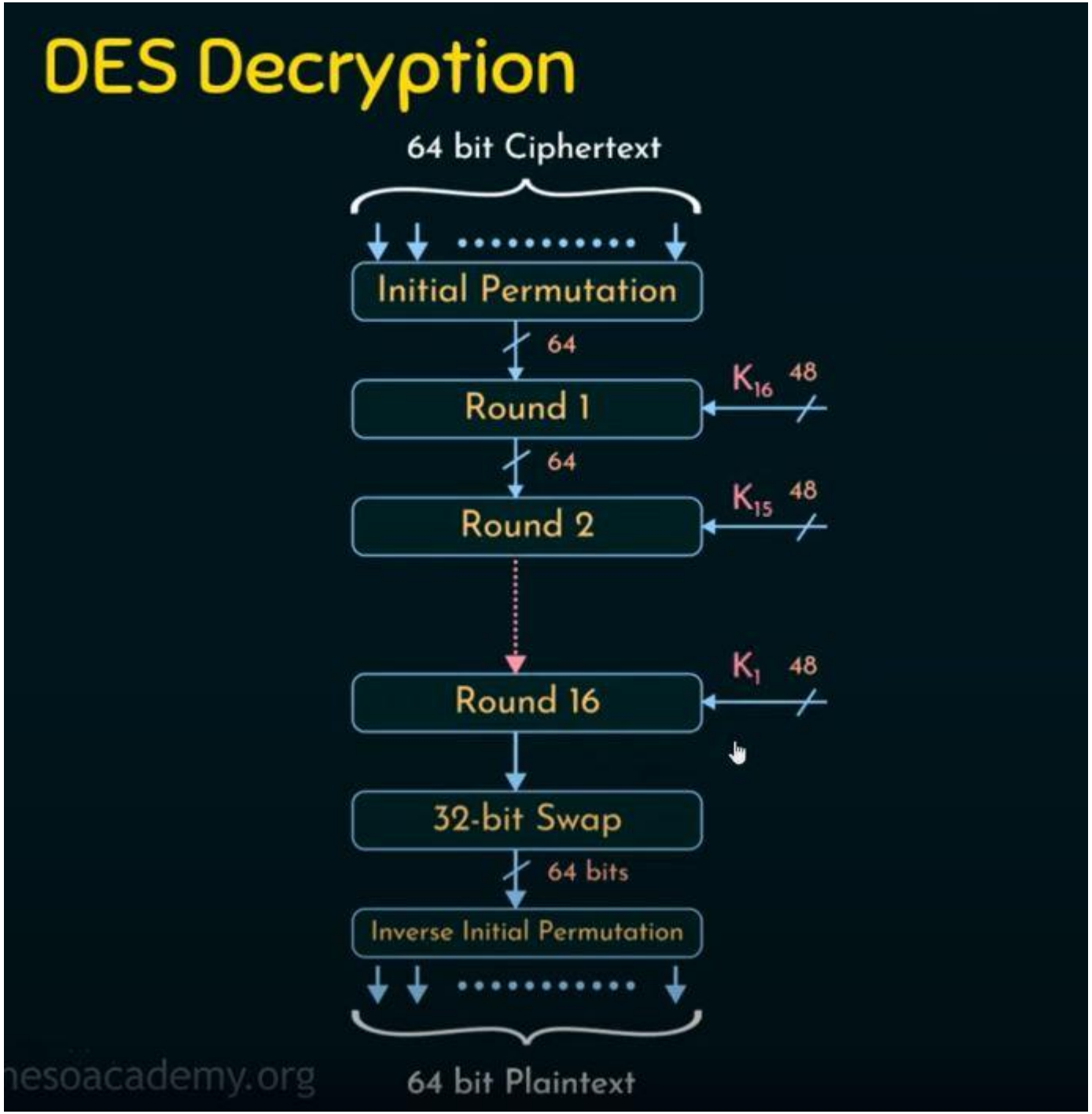
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

(d) Schedule of Left Shifts

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1


DES Decryption
64 bit Ciphertext
Initial Permutation
64
Round 1
K16 48
64
Round 2
K15 48
Round 16
K1 48
32-bit Swap
64 bits
Inverse Initial Permutation
64 bit Plaintext
nesoacademy.org

DES Block Cipher

DES decryption :

The decryption algorithm uses the same steps exactly as in the encryption algorithm except that the application of the subkeys is reversed (i.e. in round1 use K_{16}, round2 use K_{15} and so on).

Security and cryptanalysis:

The two most widely used attacks on block ciphers are linear and differential cryptanalysis. DES is also vulnerable to a brute-force (exhaustive search) attack.

Triple DES:

In cryptography, Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.

Therefore, Triple DES uses a "key bundle" that comprises three DES keys, , each of 56 bits.
The encryption algorithm is:

$K1, K2$ and $K3$

That is, DES encrypt with , DES *decrypt* with , then DES encrypt with .
Decryption is the reverse:

$$\text{ciphertext} = E_{K3}(D_{K2}(E_{K1}(\text{plaintext}))).$$

$K1$ $K2$ $K3$

That is, decrypt with , *encrypt* with , then decrypt with .
Each triple encryption encrypts one block of 64 bits of data.

$$\text{plaintext} = D_{K1}(E_{K2}(D_{K3}(\text{ciphertext}))).$$

$K3$ $K2$ $K1$