PAGE NO.:
DATE

Unit - 2

Symmetric key cryptography :

1. Block cipher Principles
2. Data Encryption Standard (DES)
3. Triple DES
4. Advanced Encryption standard (AES)
5. RC4 (Rivest Cipher)
6. Key Distribution.

PAGE NO.:
DATE

Unit - 2
Questions

Q1 :- Write an algorithm for DES and analyze it ?
(8M)

Q2 :- Explain block cipher principles ? what is difference bet° stream ciphers and block cipher ?
(6M)

Q3 :- Explain AES algorithm ? How is different from DES algorithm ? in details
(8M)

Q4 :- Short Note on

1. IDEA algorithm
2. key Distribution

(6M)

Q5 :- What are the Block cipher modes of operation of DES
(6M)

Q6 :- Differentiate public keys and convention encryption
(7M)

PAGE NO.:
DATE

Q7 :- what are the principle elements of public key cryptosystem (6m)

Q8 :- Differentiate bet^n

* Private vs Public key cryptography
or * conventional encryption vs. Public key encryption
or * symmetric cryptography vs. Asymmetric cryptography.

● Symmetric key :-

⇓

means

⇓

same key

⇓

(DES, 3DES, AES)

↓ ↓ ↓

56 bits | 192 bits | (128, 192, 256) bits bits bits

* DES → 64 bit's
* AES → minimum 128
maximum 256

PAGE NO.:
DATE

(III) DES :-

(i) DES stands for Data Encryption Standard.
(ii) key length is 64 bits (56 bits in each round)
(iii) DES involves 16 rounds of identical operations
(iv) the structure is based on Fiestal network.
(v) It is less secure.
It can be broken down (i.e., it is weak)
3DES more secure than DES
(6) Round in DES are :
Expansion, XOR operation with round key
Substitution and permutation.
(7) It can Encrypt 64 bits of plain text.
(8) It is derived from Lucifer cipher
(9) DES was designed by IBM.
(10) Brute force attack, Linear crypt-analysis and Differential crypt analysis
(11) It is comparatively slower.

PAGE NO.:
DATE

AES :- ADVANCED ENCRYPTION STANDARD

(1) AES stands for Advanced Encryption standard.

(2) Key length can be 128 bits, 192 bits or 256 bits.

(3) No. of round depends on the key length

round		bits
10	⟶	128
12	⟶	192
14	⟶	256

(4) The structure is based on the substitution Permutation network.

(5) AES is more secure than DES.

(6) Rounds in AES are :-
- byte substitution,
- Shift row,
- Mix column and
- key addition.

(7) It can encrypt 128 bits of plaintext (i.e., block size is 128 bits)

PAGE NO.:
DATE

(8) It is derived from square cipher

(9) No know attack.

(10) AES is faster.

(11) DES

(1) Data Encryption Standard

(2) DES basically Block cipher.

(3) DES follow symmetric key cryptography (Same key for encryption and decryption) ∵ Symmetric cipher

(4) It encrypt the data in blocks of size 64 bits each.

(5) 16 rounds each round is a fiestel round.

Steps :-

(i) initial permutation
(ii) 16 feestel rounds.
(iii) swapping
(iv) Final permutation

PAGE NO.:
DATE

Basic structure :-

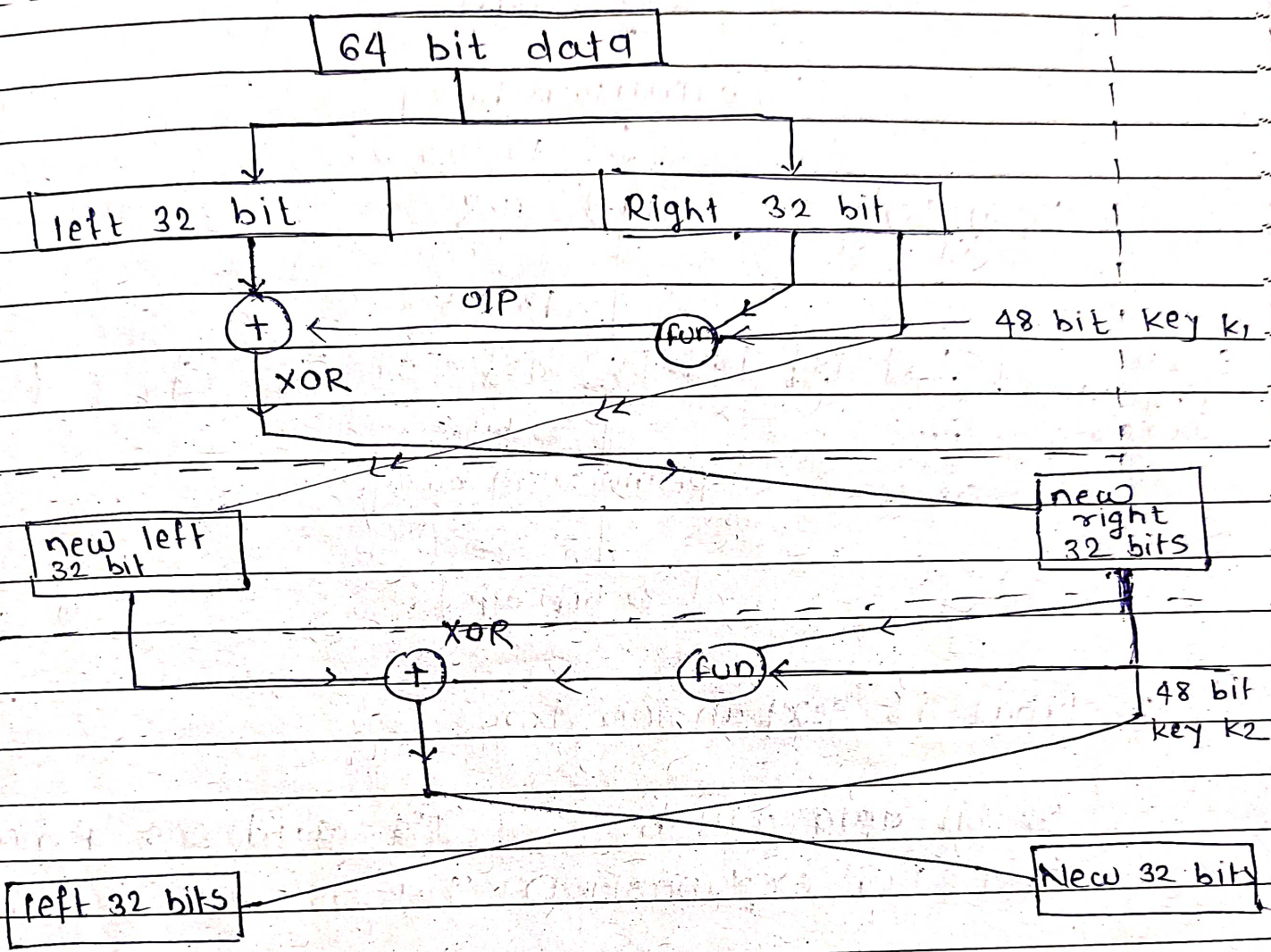
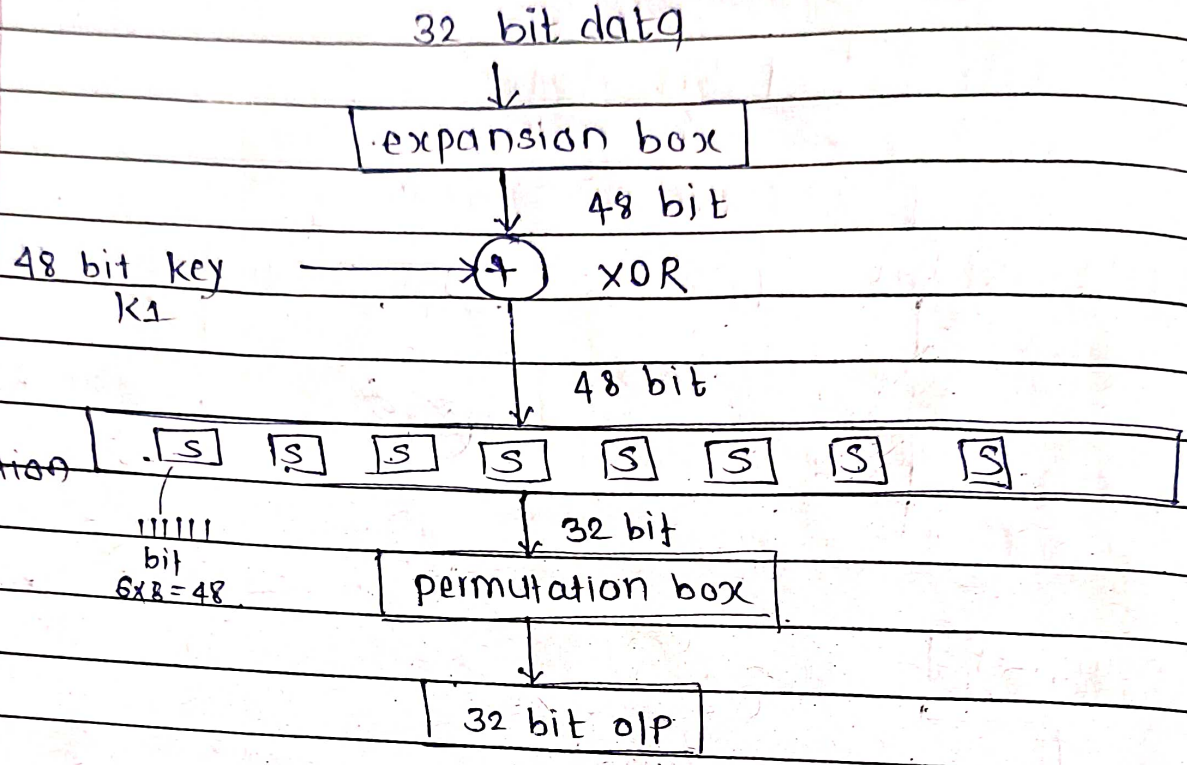


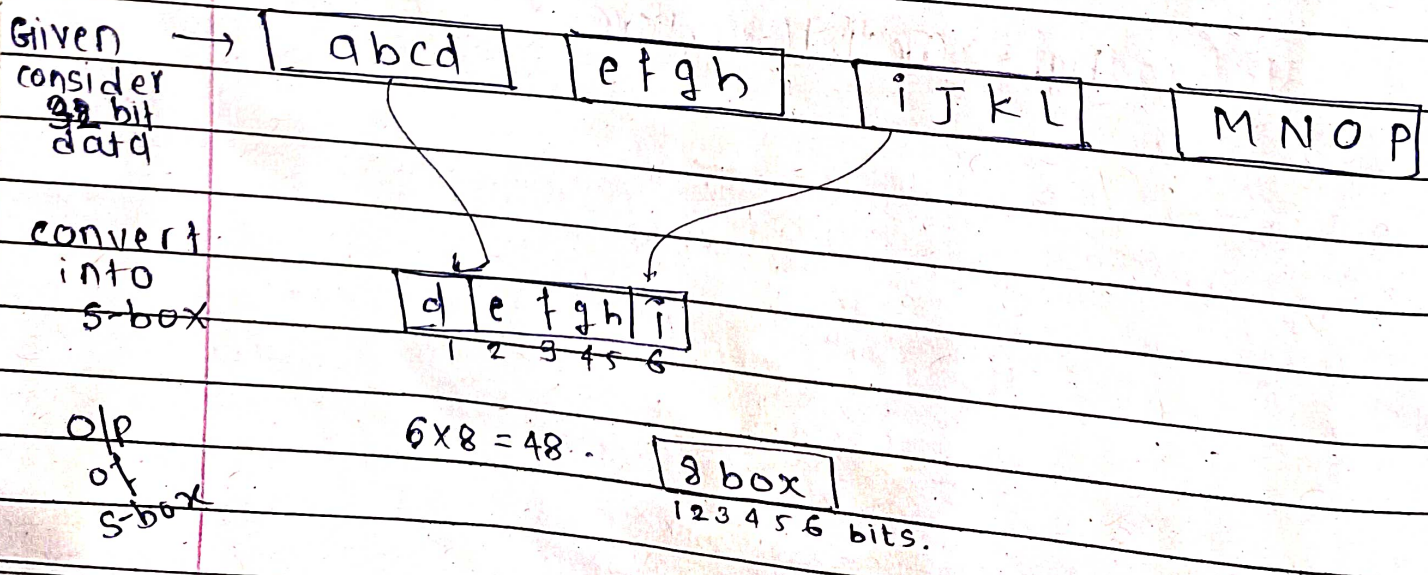
fig., → fiestel structure

function definition :-



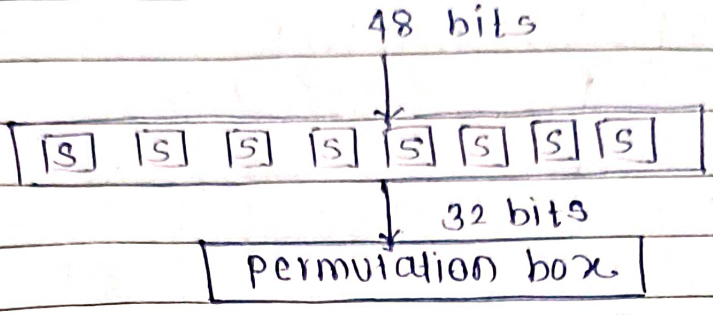
(1) What is expansion box :-

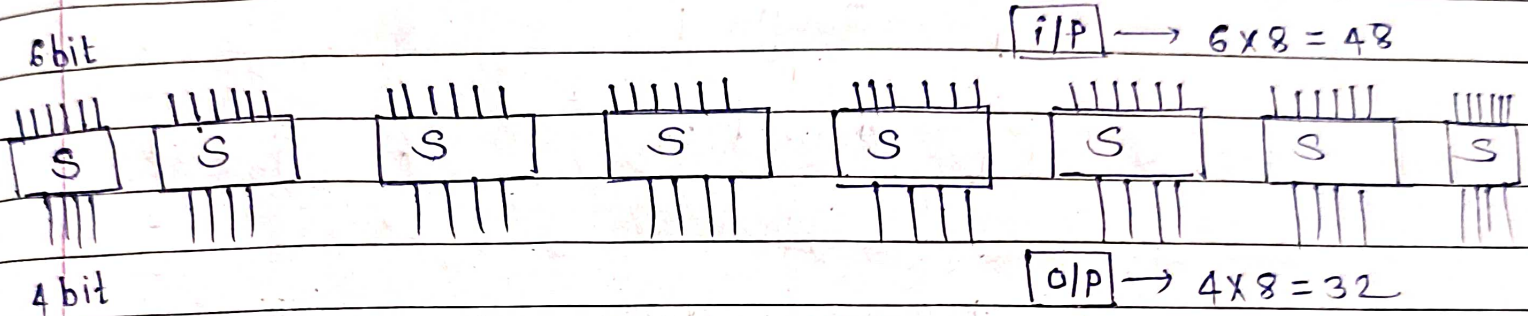
32 bit data will be → 1's and 0's form but for explanation let us consider a text



PAGE NO.:
DATE

(III) Convert 48 bit into 32 bit.



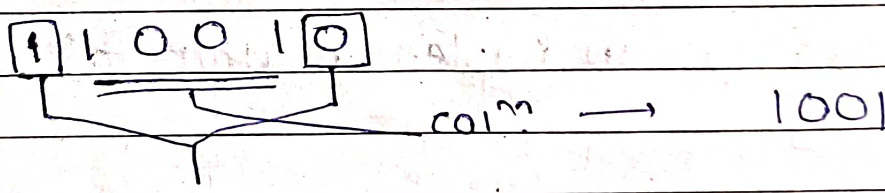


these 32 bits will go into Permutation box.

for each an every S-box you will have a separate diffierent table

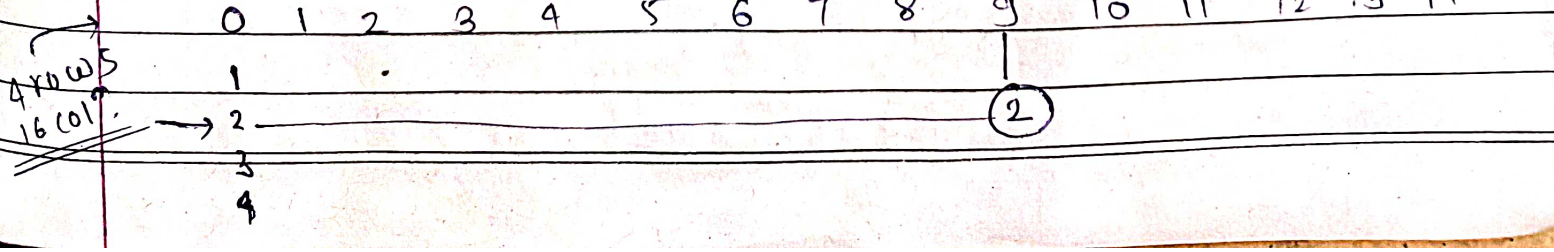
(III) How 6 bit converted into 4 bits ?

eg.,



8 4 2 1
1 0 ⇒ 2 ⇒ 2nd row

8 4 2 1
1 0 0 1 ⇒ 9 ⇒ 9th colm.



XOR

1 0 → 1
0 1 → 1
0 0 → 0
1 1 → 0

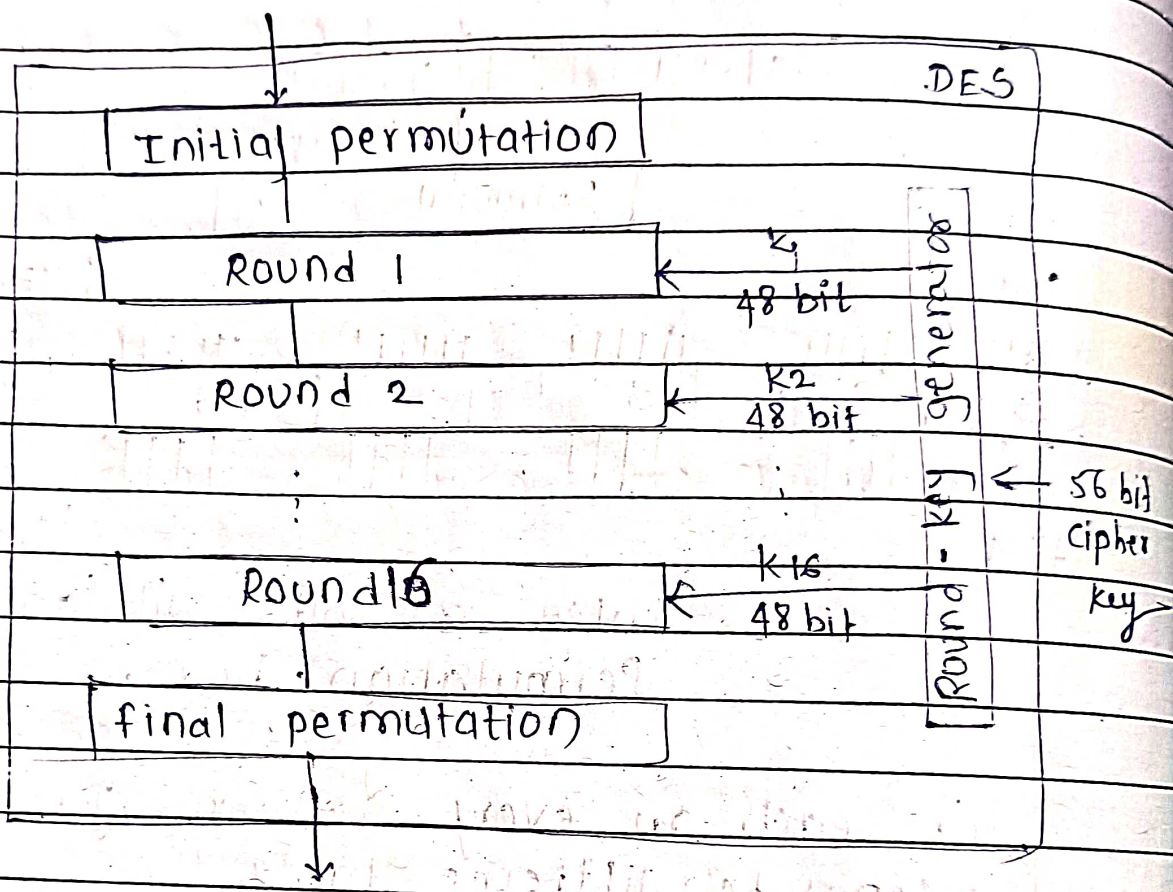


fig:→ General structure of DES.

DES is an implementation of feistel cipher.

PAGE NO.:
DATE

note

RC4 Algorithm :-
- Stream Cipher Algorithm

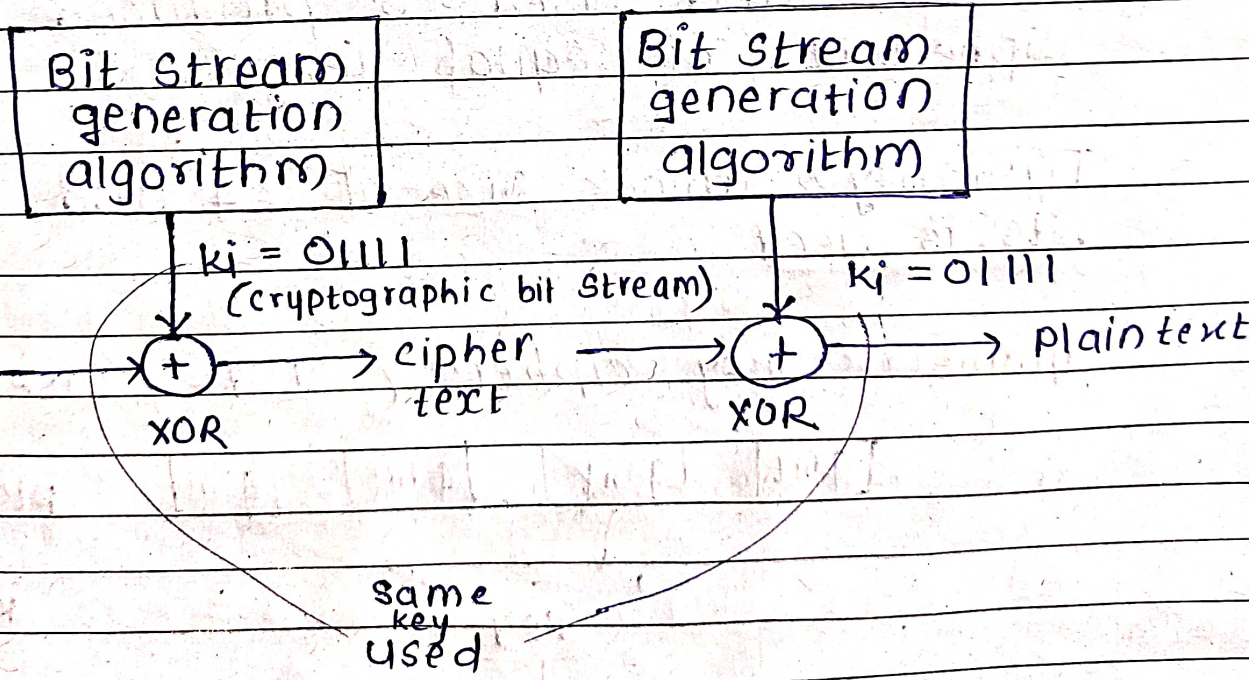
Stream and Block Cipher :-

Both Stream and Block Cipher used to convert plain text into Cipher text.

① Stream Cipher :-

- It is the one that encrypts a digital data (010110) stream one bit or 1 byte at a time
- It is a symmetric key cipher (i.e., 1 key for encryption and decryption)

generally key in the form of bits



XOR (⊕)

1	0	→ 1
0	1	→ 1
1	1	→ 0
0	0	→ 0

Eg.,

```
  1 0 1 1 0 1 1 0   (message from sender side)
⊕ 0 1 0 1 0 1 0 1   → key
-----------------
  1 1 1 0 0 0 1 1   → cipher.
```

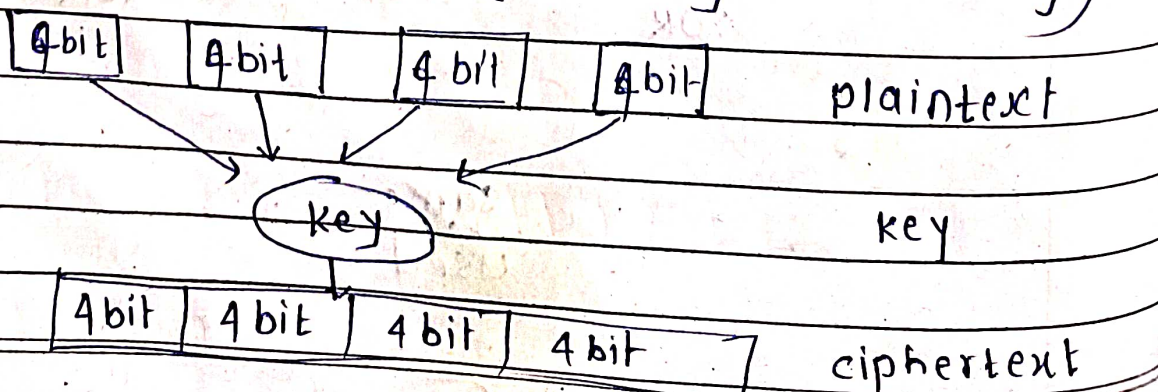
To decrypt,

```
  1 1 1 0 0 0 1 1   → cipher
⊕ 0 1 0 1 0 1 0 1   → key
-----------------
  1 0 1 1 0 1 1 0   → Plaintext
```

---

(2) Block cipher :-

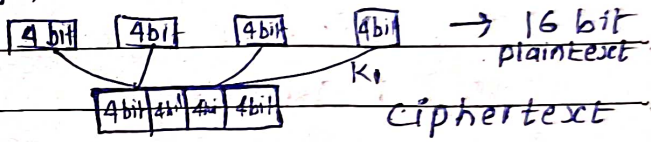
- In this a block of paintext is treated as a whole and used to produced the ciphertext of equal length.
- Typically a block size of 64 and 128 bits is used.
- Symmetric key cipher (1 key used only)



e.g., of Block cipher :-

DES (64 bit block size) cipher and Plaintext

Q., Difference between stream and Block cipher.

Stream cipher	Block cipher
① 1 bit or 1 byte of plain text is converted into plaintext.	① Plaintext is converted into ciphertext by taking Plaintext block at a time for eg., 
② Stream cipher uses 8 bits	② It uses 64 bits or more
③ complexsity of Stream cipher is more complex.	③ Complexsity of block cipher is simple
④ uses only confusion Concept	④ uses confusion as well as diffusion concept.
⑤ Reverse encrypted text is easy	⑤ In this reverse encrypted text is hard.

(6) CFB (cipher feedback) OFB (output feedback) algorithmic modes used.	(6) ECB (Electronic code book) CBC (cipher Block chaining) algorithmic modes are used.

Q., Difference bet^n confusion and Diffusion

confusion :-

It is used to ensure that cipher text doesn't give a clue about Plaintext.

(key not mentioned here)

eg., HELLO ⟶ LIPPS
(Plaintext) (ciphertext)

- Achieved with the help of Substitution
- used in both Block and Stream cipher

Diffusion :-

Diffusion increases Plaintext redundancy

- Achieved With the help of Transposition

Eg., HELLO ⟶ HOELL

- used in Block cipher

PAGE NO.:
DATE:

IMP

(III) Modes of operation in Block cipher :-

① Need of block cipher mode is basic building block for providing data security.
In block cipher rather than encrypting one bit at a time, block of bits is encrypted at a time.

② There are 5 modes of operation for block cipher that may be used in a wide varity of appl^n. like symmetric key cryptography algorithm.

③ These mode defines how data encrypted and decrypted.

Block cipher Mode operations

Electronic Code Book (ECB) mode	Cipher Block Chaining (CBC) mode	Cipher Feedback (CFM) mode	o/p feedback mode (OFB)	Counter CTR mode

Work as a block cipher

Work as block cipher but acting as stream cipher