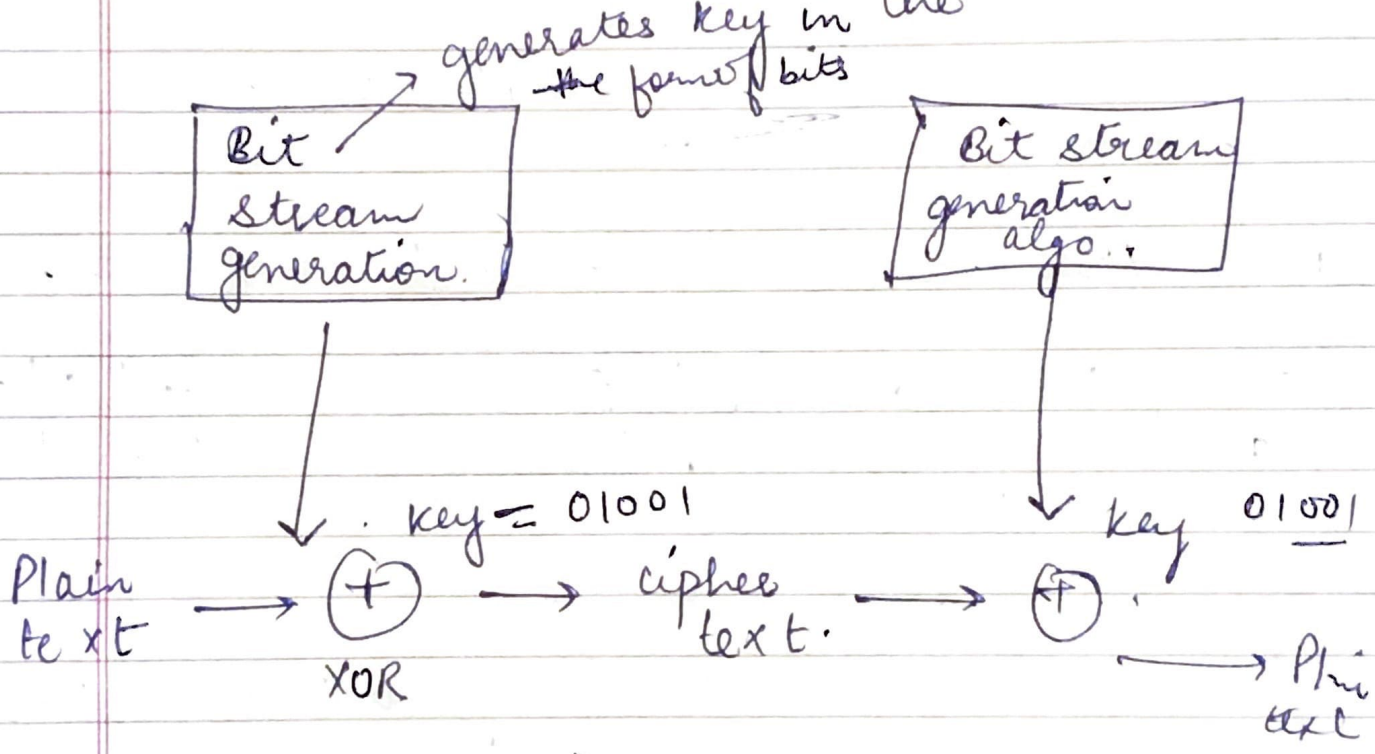
Cipher → LIPPS

* Stream & Block Ciphers :-

Stream Cipher :-

It is the one that encryptes a digital data stream one bit or 1 byte at a time .



→
```
  1 0 1 1 0 1 0
  0 1 0 1 0 1 1      key
-----------------
  1 1 1 0 0 0 1 1
-----------------
```

```
1  0 → 1
0  1 → 1
0  0 → 0
1  1 → 0.
```

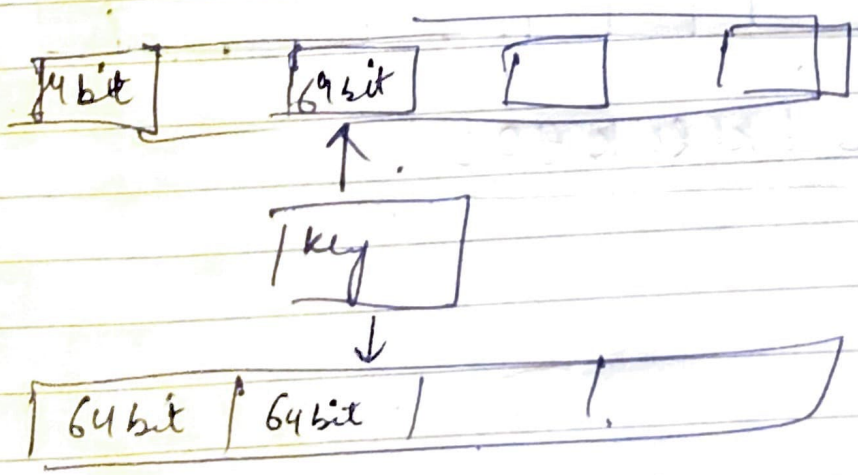
To decrypt :-

```
  1  1  1  0  0  0  1  0
  0  1  0  1  0  1  0  1   key.
-------------------------
  1  0  1  1  0  1  1  0
-------------------------
                    → Plain text.
```

2) Block cipher :-

In this, a block of plain text is treated as a whole and used to produce the cipher text of equal length (means fixed sized blocks)

* Typically, a block size of 64 and 128. key will be applied on each block.

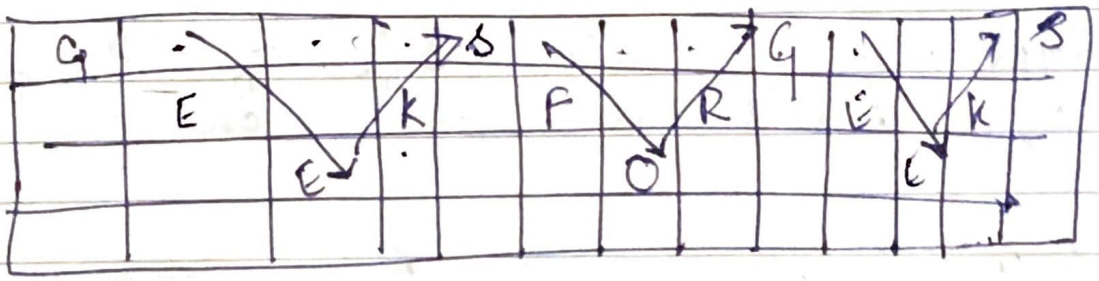


Ex! DES (64 bit block size)

Block cipher	stream cipher
(1) Block cipher converts the plain text into cipher text by taking plaintext block at time.	Steeam cipher converts the plain text into cipher text by taking 1 byte of plain text at a time.
→ 64 bits or more	Steeam cipher uses 8 bits.

Transposition Ciphers

Rail fence algo (3).



G S G S E K F R E K E O E

Columnar Transposition Cipher :-

Given a plain-text message and a numeric key / cipher / de-cipher the given text using columnar Transposition cipher

given text = GeeksforGeeks.
keyword = HACK.

1	2	3	4	5
G	E	E	K	S
F	O	R	G	E
E	E	K	S	

key = ~~3452+~~ 43512 (Random arrangement of column indexes provided no digit is greater than 5).

C = KGSERK SE GFEEOE

* The columnar Transposition cipher is a form of transposition ciphers like Rail Fence Cipher.

* Columnar Transposition involves writing the plaintext out in rows, and then reading the cipher text off in columns one by one.