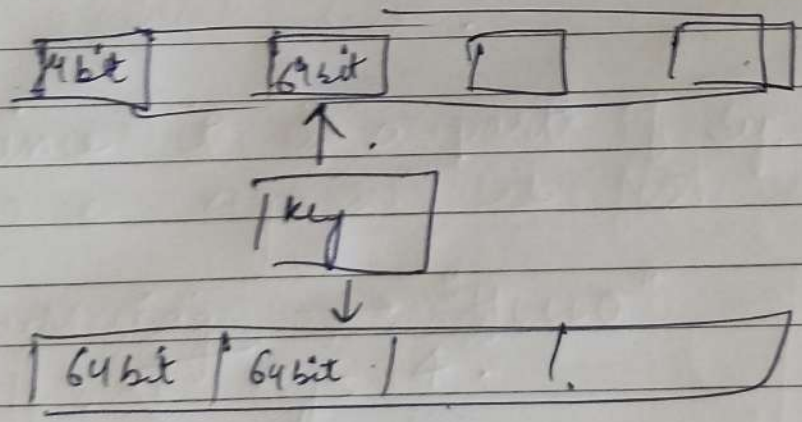
To decrypt :-

```
  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.

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



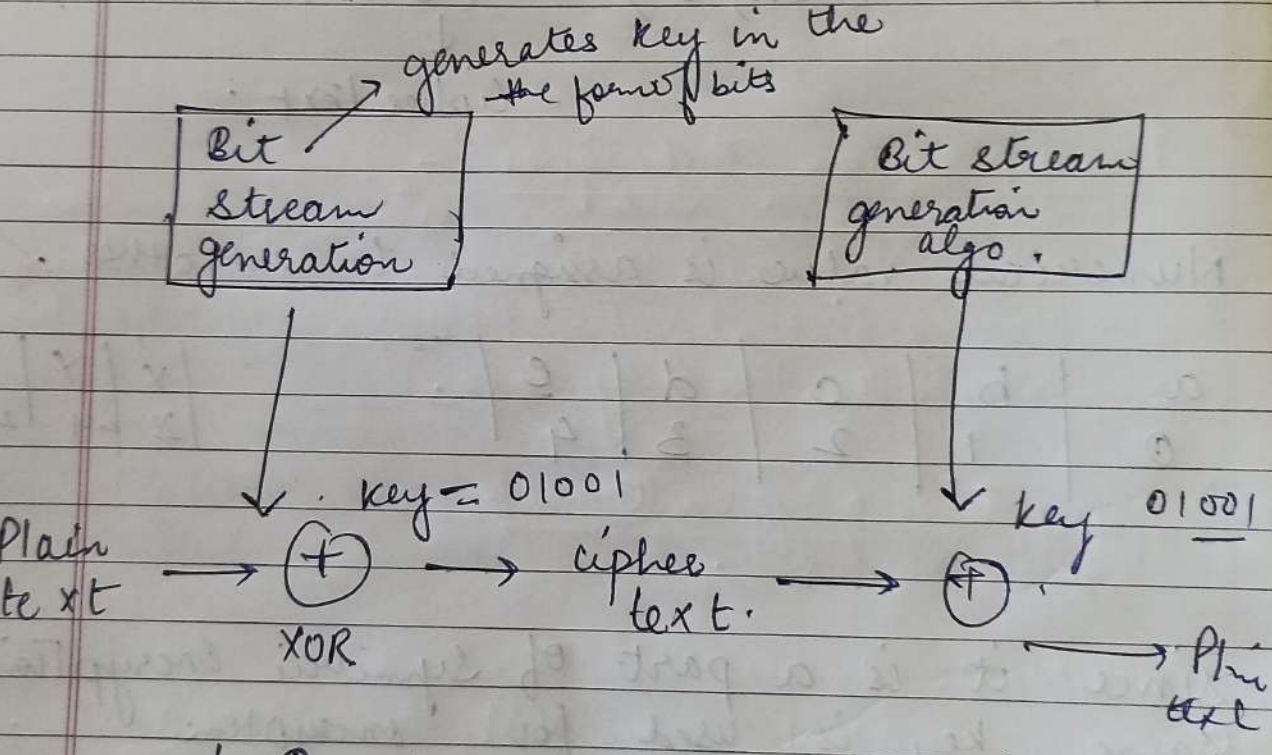
Ex: DES (64 bit block size)

Cipher → LIPRS

* Stream & Block Ciphers :-

Stream Ciphers :-

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



→ 1 0 1 1 0 1 1 0
0 1 0 1 0 1 0 1 key
1 1 1 0 0 0 1 1

1 0 → 1
0 1 → 1
0 0 → 0
1 1 → 0.

Cipher Text :- message.

$C = E(k, P) = (P + k) \bmod 26.$

k → key, P → plain text } encryption

For decryption:-

$P = D(K, c) = (c - k) \bmod 26.$

c → Cipher text.

Numerical value is assigned to each other.

a	b	c	d	e	----	x	y	z
0	1	2	3	4		23	24	25

Since it is a part of symmetric encryption same key is used for encryption

eg: Message → "HELLO"
let key = 4.

$C(H) = (P + k) \bmod 26.$
$(7 + 4) \bmod 26 = 11 = L$

$C(E) = (E + k) \bmod 26 = 8 = I$
$4 + 4 \bmod 26$

L
I
PP
S

FREEMIND

Date

Page

Caesar Cipher

* It is also called shift cipher / additive ciphers.

* Each letter in the plaintext is replaced by a letter corresponding to a no. of shifts in the alphaset.

shift key = 3.

Plain:- A B X C
D E A F

Julius Caesar used an additive cipher to communicate with his officers. For this reason additive ciphers are sometimes called Caesar Ciphers.

A → D
B → E
C → F
D → G
E → H
F → I

x
y
z

FREEMIND

Date

Page

A B C
↓
B C D.

ift Letters.

A B C D ----- X Y Z
↓ ↓ ↓ ↓
M x Z A

Cipher text.

* Transposition Techniques :-

performing some sort of permutations on the plaintext letters.
ie reorders the symbols.

i.e :- rearrangement of the letters of the plain text. *

eg:- NAME :- 4! 4x3x2x1.
EAMN, AENM or MNEA etc.

Types of Transposition ciphers
- keyless.
- keyed.

- Rail fence
- Columnar
- Double transposition

Monoalphabetic substitution cipher

FREEMIND

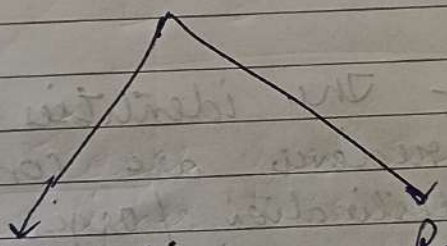
Date

Page

* Substitution Cipher :-

is a method of cryptography which converts standard language or plaintext into coded language or cipher text by replacing units of plaintext in accordance with fixed set of rules.

→ The plaintext units may be individual letters or characters, letter, pairs triplets or other combinations.



Mono Alphabetic cipher (Single)
↓
one to one

Poly Alphabetic cipher.
↓
one to many.

Plaintext
e.g. P A R R O T
cipher C B Q Q A L

eg. P A R R O T
C B Q S A L

→ Additive cipher (Shift cipher)
→ Multiplicative Cipher
→ Affine Cipher.

→ Autokey cipher
→ Vigenere cipher

shift

*

Tra

FREEMIND

Date

Page

Features of Cryptography

* Confidentiality :- Information can only be accessed by the person for whom it is intended and no other except him can access it.

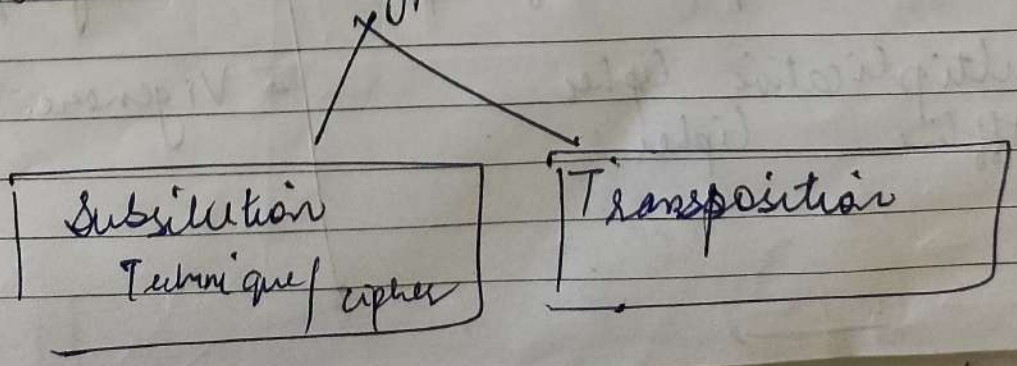
* Integrity :- Information can't be modified in storage or transition between senders and intended recieves.

* Non-repudiation :-

* Authentication :- The identities of sender and reciever are confirmed. As well as destination / orgin of information is confirmed.

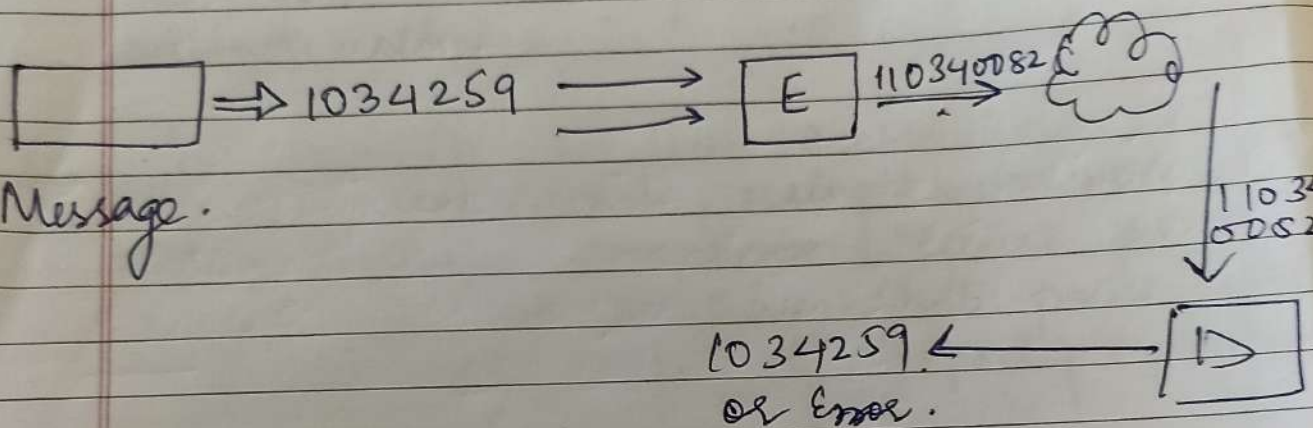
Encryption Algorithms :-

Symmetric encryption also reffered to as conventional encryption



Cryptography :- Plain to cipher text → cipher text to Plain text.

Cryptography is the practice & study of techniques for securing comm. & data in the presence of adversaries.



So, to protect this message, Andy first convert his readable message to unreadable form. Here, he convert the message to some random numbers. After that he uses a key to encrypt his message in Cryptography ; we call this ciphertext