• Cryptography :

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

'Crypt' means hidden and 'graphy' means writing.
So, cryptography means 'secret writing'.

Cryptography is most often associated with scrambling plain text into ciphertext (called encryption) then back again to plain text (called decryption).

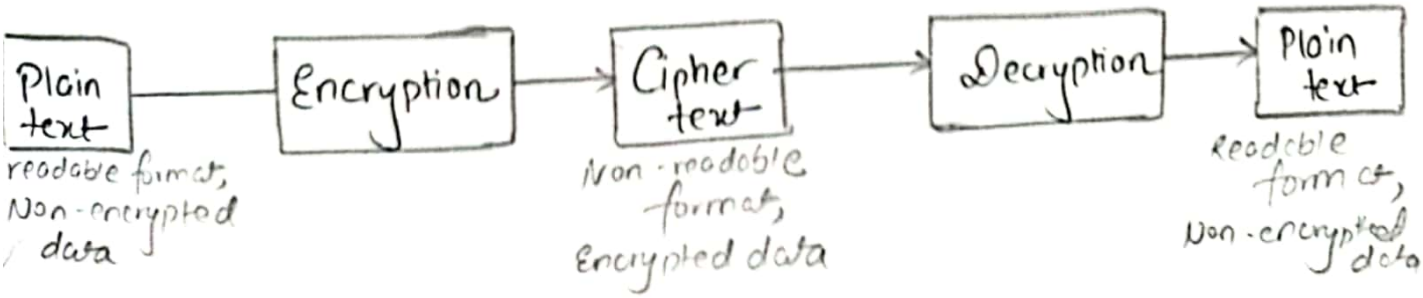
Modern Cryptography concerns itself with the following objectives:

1) Confidentiality: the information cannot be understood by anyone for whom it was unintended.

2) Integrity: the information cannot be altered by anyone except sender & intended receiver.

3) Authentication: the sender and receiver can confirm each other's identity and the origin of the information.

Cryptography



- **Cipher Text:**

Cipher is an algorithm which is applied to plain text to get ciphertext. Ciphertext is not understandable until it has been converted into plain text using key. There are many types of ciphertext and ceaser cipher is one, also known as substitution cipher.

- **Shift Cipher (Ceaser Cipher in Cryptography):**

Shift Ciphers work by using the modulo operator to encrypt and decrypt messages. It is one of the earliest and simplest method of encryption technique.

The shift cipher has a key 'K' which is an integer from 0 to 25. and it is the deciding factor for encryption & decryption among two communicators.

- **Encrypt:**

It is the process of converting every letter of message into the number that matches its order in the alphabet. starting from 0, call this number 'X'.

Now,

Calculate $Y = (X+K) \text{ MOD } 26$

Then, Convert the number 'Y' into a letter that matches its order in the alphabet starting from 0.

- **Decrypt:**

Convert the letter into the number that matches its order in the alphabets starting from 0, and call this number 'Y'.

Now,
Calculate: $X = (Y - K) \bmod 26$

Then, convert the number 'X' into a letter that matches its order in the alphabet starting from 0.

↳ The table is included below:

A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

↳ Key starts from 1 and ends with 26 unlike the encryption and decryption alphabets which start from 0 and end with 25.

↳ Anyone who doesn't have a key, cannot decode the message.

- Shift Cipher Insecurity:

A cipher should prevent an attacker, who has a copy of the cipher text but does not know the key, from discovering the contents of the message.

Since there are only 26 choices for the key, someone can easily try all of the 26 keys, one by one, until they recover the message.

This type of attack is called Brute Force Attack.

↳ Exercises:

Encryption:

1) TODAY IS SUNDAY AND IIT CLASS IS FIRST
Key = 2

Ans: (19, 14, 3, 0, 24) (8, 18) (18, 20, 13, 3, 0, 24) (0, 13, 3) (8, 8, 19) (2, 11, 0, 18, 18) (8, 18) (5, 8, 17, 18, 19)

Now, Adding Key = 2,

(X+K) =

(21, 16, 5, 2, 26) (10, 20) (20, 22, 15, 5, 2, 26) (2, 15, 5) (10, 10, 21) (4, 13, 2, 20, 20) (10, 20) (7, 9, 19, 20, 21)

Using Y = (X+K) MOD 26

(21, 16, 5, 2, 0) (10, 20) (20, 22, 15, 5, 2, 0) (2, 15, 5) (10, 10, 21) (4, 13, 2, 20, 20) (10, 20) (7, 9, 19, 20, 21)

= VQFCA KU UWPFCA CPF KKV ENCUU KU HKTQV

- Decrypt :

1) WIGXMSR E GSRXEMPW KSSH WX4 HIRXW
GSQTEVIH XS SXLIV WIGXMSRW

Key-4

Ans Here,

(22, 8, 6, 23, 12, 18, 17) (4) (6, 18, 14, 23, 4, 12, 17, 22)
(10, 18, 18, 7) (22, 23, 24, 7, 8, 17, 23, 22)
(6, 18, 16, 19, 4, 21, 8, 7) (23, 18) (18, 23, 11, 8, 21)
(22, 8, 6, 23, 12, 18, 17, 22)

Now,

Using $X = (Y-K) \text{ MOD } 26$.

(18, 4, 2, 19, 8, 14, 13) (0) (2, 14, 13, 19, 0, 8, 13, 18)
(6, 14, 14, 3) (18, 19, 20, 3, 4, 13, 19, 18)
(2, 14, 12, 15, 0, 19, 4, 3) (19, 14)
(14, 19, 7, 4, 17) (18, 4, 2, 19, 8, 14, 13, 18)

= SECTION A CONTAINS GOOD STUDENTS COMPARED TO OTHER SECTIONS

---

2) Se irgyy ixokbj tgsh oy ysxozo kn xkyzng (key=6)

Ans (18, 4) (8, 17, 6, 24, 24) (11, 23, 14, 10, 19, 9)
(19, 6, 18, 10) (14, 24) (24, 18, 23, 14, 25, 14)
(24, 13, 23, 10, 24, 25, 13, 6)

Now,

$X = (Y - K) \text{ MOD } 26$

(12, 24) (2, 11, 0, 18, 18) (5, 17, 8, 4, 13, 3)
(13, 0, 12, 4) (8, 18) (18, 12, 17, 8, 19, 8)
(18, 7, 17, 4, 18, 19, 7, 0)

= MY CLASS FRIEND NAME IS SMRITI SHRESTHA

---

3) Dywybbyg sc ryusnki (Key = 10)

→ Here,

(3, 24, 22, 24, 1, 1, 24, 6) (18, 2) (17, 24, 21, 18, 13, 10, 8)

Now,

$X = (Y - K) \text{ MOD } 26$

(19, 14, 12, 14, 17, 17, 14, 22) (8, 18) (7, 14, 11, 8, 3, 0, 24)

= Tomorrow is holiday