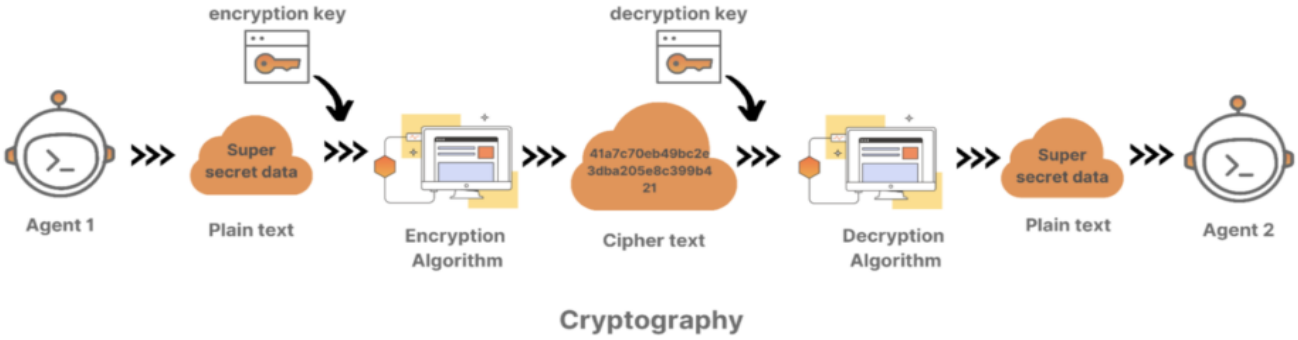
CRYPTOGRAPHY:

- The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.

OR

Cryptography is the science of using mathematics in writing the secret code i.e. to encrypt (data is transmitted into unreadable format) and decrypt (unreadable data reverse transmitted into readable format) the data.

- The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing.
- Cryptography is a need while communicating over an untrusted medium such as a network or the internet.



Cryptography

SHIFT CIPHER/ CAESAR CIPHER:

The Caesar Cipher is named after its inventor Julius Caesar. Shift Ciphers work by using the modulo operator to encrypt and decrypt messages. The Shift Cipher has a key X, which is an integer from 0 to 25. We will only share this key with people that we want to see our message.
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25.
Encryption and Decryption is represented using mathematical equation involving modular arithmetics:

For Encryption,

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

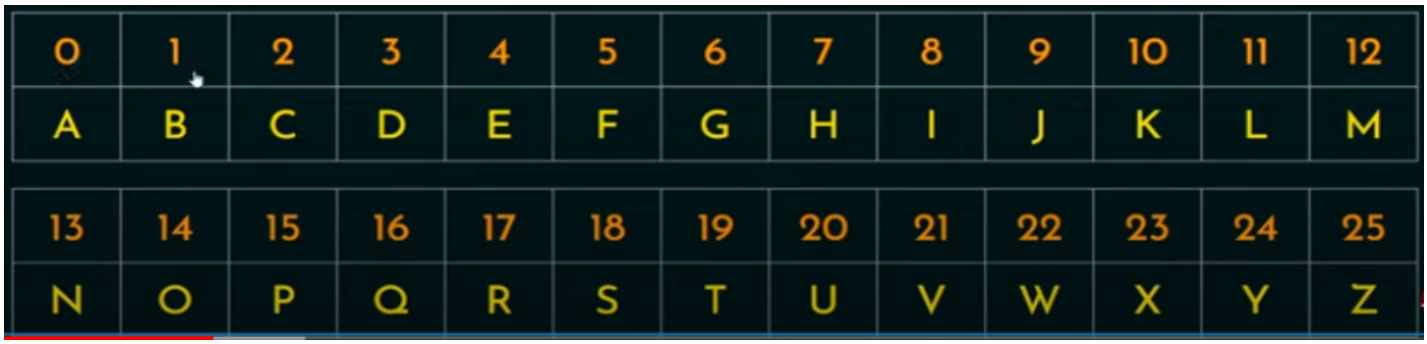
For Decryption,

$P = D(X,C) = (C-X) \bmod 26$

Where,
C= Cipher Text,
P= Plain Text,
E and D= Encryption and Decryption,
X= Key used in the process,
Modulo= Remainder of the number when divided by the modulo number,
26= Total number of alphabets.

(Question format asked in exam and solution should be written in tabular format as mentioned below.
NOTE- If key is not mentioned consider X= 3)

Q1. Encrypt the Plain Text "FIVE" using Caesar Cipher with a given encryption key X= 3.
Solution:
Reference table-



Encryption,

Plain Text	(P + X) mod 26	Cipher Text
F	(5+3) mod 26 = 8 mod 26= 8	i
I	(8+3) mod 26= 11 mod 26= 11	l
V	(21+3) mod 26= 24 mod 26= 24	y
E	(4+3) mod 26= 7 mod 26= 7	h

Decryption,

Cipher Text	(C- X) mod 26	Plain Text
i	(8-3) mod 26 = 5 mod 26= 5	F
l	(11-3) mod 26= 8 mod 26= 8	I
y	(24-3) mod 26= 21 mod 26= 21	V
h	(7-3) mod 26= 4 mod 26= 4	E

PRACTICE:

Q2. Encrypt the Plain Text "TREATY IMPOSSIBLE" using Caesar Cipher Technique.

Q3. Encrypt the Plain Text "meet me after the toga party" using Caesar Cipher with a given encryption key X= 3.

****

[**NOTE-** Some Mathematical concepts related to mod- https://modulocalculator.com/7-mod-26
STEPS: Calculate the mod

1. **Start by choosing the initial number** (before performing the modulo operation). Let's say it is 52. This is our dividend.
2. **Choose the divisor.** Let's pick 6. The operation we want to calculate is then `52 mod 6`.
3. **Divide one number by the other, rounding down:** `52 / 6 = 8.66666`**.** This is the quotient.
4. **Subtract this number from your initial number -> `8.66666- 8= 0.66666`**
5. **Multiply the divisor by the quotient.** So it's `0.66666 * 6 = 4` in our example.
6. **The number you obtain is the result of the modulo operation.** We can write it down as `52 mod 6= 4`.

For practice purposes find out: **7 mod 26** using above steps.]

****

ENCRYPTION BASICS:

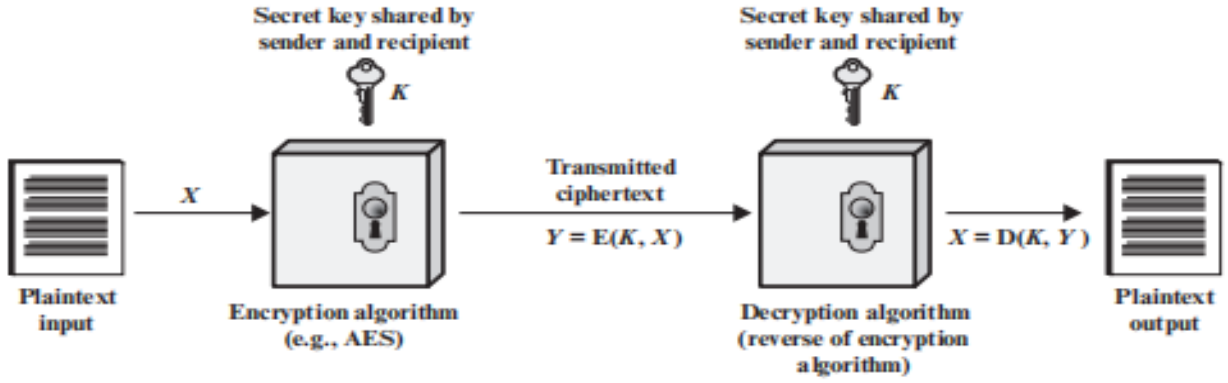
1. Plaintext: The original message without any encryption techniques.

2. Encryption Algorithm: Technique used to convert plaintext to encrypted text.
3. (Secret)Key: The input for the encryption algorithm.
4. Cipher Text: Output of encryption algorithm.
5. Decryption Algorithm: The encryption algo to be run in reverse.

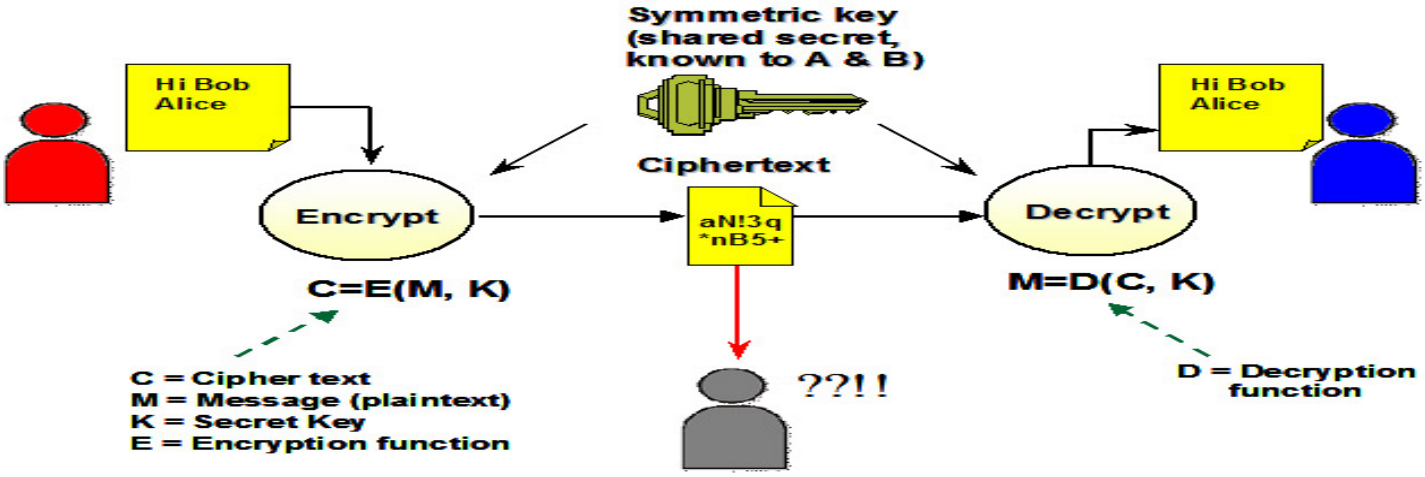
TYPES OF ENCRYPTION:

1. **Symmetric Encryption Technique** (Same Key is used in Encryption and Decryption)
2. **Asymmetric Encryption Technique** (Different Keys are used in Encryption and Decryption)

SYMMETRIC CIPHER MODEL:



Example of Bob and Alice for above concept:



SUBSTITUTION TECHNIQUE IN ENCRYPTION:

1. **Monoalphabtic Cipher:**

Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process.
For E.g.
If 'A' is encrypted as 'D' , for any number of occurrences in that plain text 'A' will always get encrypted to 'D'.

Plain Text: **A B** C D **A** F X **B** Q **A** S
Cipher Text: **D M** F C **D** R T **M** O **D** P

2. **Caesar Cipher/ Shift Cipher:**

E.g.

```
plain:  meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

```
plain:  a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

[**NOTE:** Rules:

1. *During the decryption process, if you get a negative value then add it with 26.*

   Eg. (-2)mod 26 = (-2+26) mod 26= 24 mod 26= 1
2. *During the Encryption process, if you get a number greater than 26 then subtract it with 26.]*

Disadvantages:

- Simple structure usage.
- Can only provide minimum security to the information.
- Frequency of the letter pattern provides a big clue in deciphering the entire message.

3. **Playfair Cipher:**

In playfair cipher, unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

➔ More than one character is used for encryption and decryption.Hence it is called a Multiple Substitution Cipher.
➔ Input of this technique are Keyword and Plaintext.
➔ Keyword(Key) is a string.

E.g.

1. **P.T. :** HEYA ——→ HE YA

2. **P.T. :** HELLO ——→ HE LL O ✗

HE LX LO ✓

Two similar letters cannot be together. When two similar letters are grouped we group one of them by 'X'.

3. **P.T. :** HELLOE ——→ HE LX LO E

So, in such case where alphabet is alone we use 'Z' to group with that alphabet.

HE LX LO EZ

4. **P.T.** HEXXOE ——→ HE XZ XO EZ

Steps to perform encryption using playfair cipher technique:

(Steps and examples solved during lecture. Refer to your class notebook.)

Some concepts related using the table (5 x 5)

A	B	H	I/J	C
D	E	F	G	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

1. If both the alphabets are in the **same row**, **replace them** with alphabets to their **immediate right**.

   P.T – FG ——→ GK **P.T** – UQ ——→ QR

2. If both the alphabets are in the **same column, replace them** with alphabets **immediately below them**.

   P.T – BM ——→ ER **P.T** – RW ——→ WB

3. **If not in same row/column**, **replace them** with alphabet in the **same row respectively, but at other pair of corners**.

   P.T- QW ——→ RV **P.T**- FL ——→ DN

4. Vigenere Cipher:

- Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets .The encryption of the original text is done using the Vigenère square or Vigenère table.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.

- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.

- The alphabet used at each point depends on a repeating keyword.

Method- 1 (When table is given)

keyword \ plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Method – 1 (When table is given….)

Plaint Text : GIVE MONEY
Key : LOCK

Encryption and Decryption :

Plain Text	G	I	V	E	M	O	N	E	Y
Key	L	O	C	K	L	O	C	K	L
Cipher Text	R	W	X	O	X	C	P	O	J
Key	L	O	C	K	L	O	C	K	L
Plain Text	G	I	V	E	M	O	N	E	Y

Method-2 (Table is not given. Make the following table.)

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

Encryption

The plaintext(P) and key(K) are added modulo 26.

$C_i = E_i = (P_i + K_i) \bmod 26$

Decryption

$D_i = (E_i - K_i + 26) \bmod 26$

Example :

Plaint Text : SHE IS LISTENING
Key : PASCAL

0	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
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Plaint Text : SHE IS LISTENING
Key : PASCAL ⟶ **Key Stream :** 15, 0, 18, 2, 0, 11

P.T.	S	H	E	I	S	L	I	S	T	E	N	I	N	G
P's value	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Key Stream	15	0	18	2	0	11	15	0	18	2	0	11	15	0
C's value	7	7	22	10	18	22	23	18	11	6	13	19	2	6
C.T.	H	H	W	K	S	W	X	S	L	G	N	T	C	G
P's value	18	7	4	8	18	11	8	18	19	4	13	8	13	6
P.T.	S	H	E	I	S	L	I	S	T	E	N	I	N	G

Calculating D's Value : (Decryption)

$$D_i = (E_i - K_i + 26) \bmod 26$$

Cipher Text : H
Key Value : 15
= (7 – 15 + 26) mod 26
~~= -8 mod 26 = -8~~ *If get negative value then add it with 26.*
= (-8 + 26) mod 26 = 18
If get negative value then add it with 26.

Key Stream	15	0	18	2	0	11	15	0	18	2	0	11	15	0
C's value	7	7	22	10	18	22	23	18	11	6	13	19	2	6
C.T.	H	H	W	K	S	W	X	S	L	G	N	T	C	G
P's value	18	7	4	8	18	11	8	18	19	4	13	8	13	6
P.T.	S	H	E	I	S	L	I	S	T	E	N	I	N	G

5. Vernam Cipher-

- Also called as One Time Pad or the Perfect Cipher. Here plaintext is combined with a

random key. The Key must be at least as long as the plaintext. Each key is used only once and the sender receiver must destroy the key after use. There should be only two copies of the keys,1 with the sender and the other with the receiver.

Rules of Encryption:

1. Assign a number to each character in ABC series -

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

2. Assign no. to each character of plaintext and key according to the table from the previous slide.

Plain Text : HELLO

Key : baxyc

Encryption :

P. T.	H	E	L	L	O
P's Value	7	4	11	11	14
Key	b	a	x	y	c
Key Stream	1	0	23	24	2

3. Add the values of plaintext(pt) and key:

P. T.	H	E	L	L	O
P's Value	7	4	11	11	14
Key	b	a	x	y	c
Key Stream	1	0	23	24	2
P.T. + Key	8	4	34	35	16
P.T. - 26	8	4	(34 – 26) = 8	(35 -26) = 9	16
C.T.	I	E	I	J	Q

Where here the number is GREATER THAN 26 in next step we need to subtract that number with 26.

4. Decryption:

Decryption :

0	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
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**

C.T.	I	E	I	J	Q
C's Value	8	4	8	9	16
Key	b	a	x	y	c
Key Stream	1	0	23	24	2
C.T – Key	7	4	-15	-15	14
C.T + 26	7	4	(-15 + 26) = 11	(-15 +26) = 11	14
P.T.	H	E	L	L	O

Where here the number is NEGATIVE so add that number with 26

****

TRANSPOSITION TECHNIQUES IN ENCRYPTION:

Columnar Technique:

Rail Fence Technique:

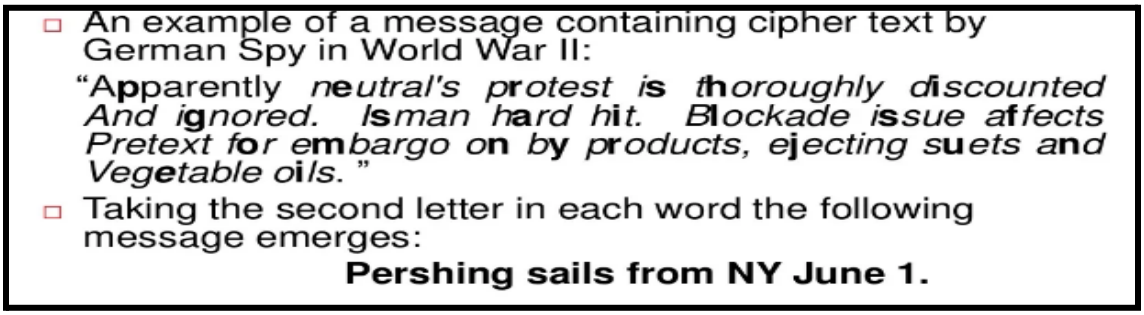
****

STEGANOGRAPHY:

- Steganography is defined as the study of invisible communication. Steganography usually deals with the ways of hiding the existence of the communicated data in such a way that it remains confidential. It maintains secrecy between two communicating parties.
- Steganography is a Greek word which means concealed writing. The word “steganos” means “covered “ and “graphical “means “writing” .
- Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data.
- Steganography hides the secret data in another file in such a way that only the recipient knows the existence of the message.
- In ancient time, the data was protected by hiding it on the back of wax, writing tables, stomach of rabbits or on the scalp of the slaves. But today’s most people transmit the data in the form of text, images, video, and audio over the medium.
- In order to safely transmit confidential data, multimedia objects like audio, video, images are used as a cover source to hide the data.

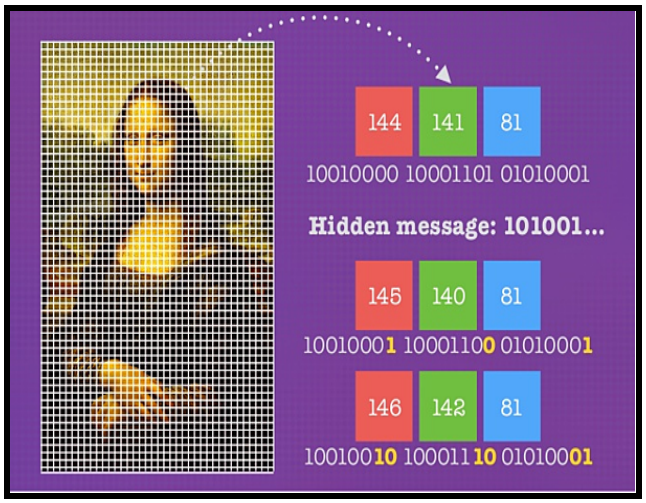
1. TEXT STEGANOGRAPHY:

It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every word of text message.



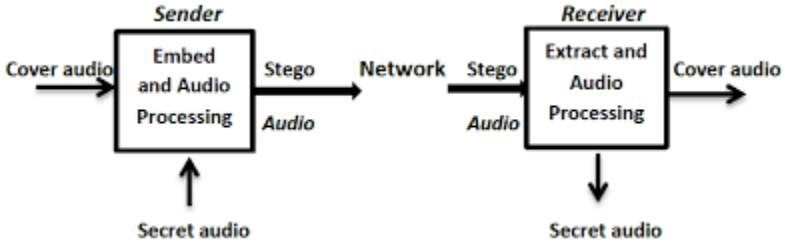
2. IMAGE STEGANOGRAPHY:

Hiding the data by taking the cover object as an image is referred to as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used as cover sources because there are a number of bits present in digital representation of an image.



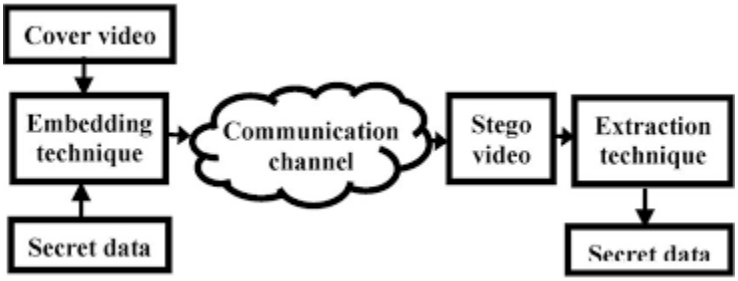
3. Audio Steganography:

It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files.It is a technique used to secure the transmission of secret information or hide their existence. It also may provide confidentiality to secret messages if the message is encrypted.



4. Video Steganography:

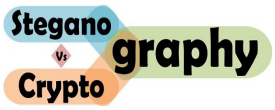
It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as a carrier for hiding the data.



5. Network or Protocol Steganography:

It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. In the OSI layer network model there exist covert channels where steganography can be used.

****



Difference between Cryptography and Stegnography:

CRYPTOGRAPHY	STEGANOGRAPHY
1. Cryptography means secret writing.	1. Steganography means covered writing.
2. Goal of cryptography is Data Protection.	2. Goal of steganography is Secret Communication.
3. It takes a file and transforms it into a new file known as cipher text using a key.	3. It hides a file within another file.
4. It supports security principles such as Confidentiality, Data- integrity, Authentication and Non- Repudiation.	4. It supports security principles such as Confidentiality and Authentication.
5. Implemented on only text files.	5. Implemented on text, audio, video, image files.
6. No one would be able to know what the message says unless there's a key to code.	6. The hidden message is imperceptible to anyone.
7. Involves the use of number theory and mathematics to alter data.	7. Mathematical transformations are not much involved.
8. Drawback- No matter how unbreakable it is, it will arouse suspicion.	8. Advantage- Hidden messages do not attract attention.