Q1) Discuss the term Cryptography & Stegnography?

Ans -:

**Cryptography** -: Cryptography is technique of securing information & communications through use of codes so that only those person for whom the information is intended can be understand it & process it. Thus preventing unauthorized access to information. The prefix "crypt" means hidden & suffix graphy means writing.

**Features** -:

① Confidentiality

Information can only be accessed by the person for whom it is intended & no other person except can access it.

② Non - repudiation

The sender of info. cannot deny his or her intension to send info. at later stage.

③ Integrity

Information cannot be modified in storage or tra between sender or transition between sender & intended receiver without any addition to info. being detected.

④ Authentication

Identities of sender & receiver are confirmed

Steganography :-

It is the art of hiding the existence of a message rather than its meaning. It is currently a very HOT topic as one subdivision of Steganography is digital water marking, a technique used to copyright & to protect digital images, music & software.

Types of Steganography :-

1. Low tech Steganography
2. High tech Steganography
3. Anaglyphic Steganography.

It deals with breaking of the cryptography text or the cipher text whereas, cryptography deal with the encryption of plaintext into cipher text.

Q2) Distinguish between active & passive security attacks. Give some examples of both types of attack?

Ans :- Active Attacks :-

An active attack is one in which an unauthorized change of network messages is attempted

(a) Masquerade Attack :-

It relates to an entity taking on a false identity in order to acquire information, & in effect achievement an unwaranted privilege status.

(b) Traffic Analysis -:
It is the process of intercepting & examining message in order to deduce information from pattern in communication.

(c) Brute force Attack -:
It is an attempt to break a cipher keys, a brute force or exhaustive search attack.

(d) Algebraic Attack -:
It writes the cipher as a system of equations & solve for the key.

Q3) What is monoalphetic cipher ? How is it different from Caesar cipher.

The caesar cipher uses only 26 rotation out of 26 Permutation on alphabet. The monoalphetic cipher uses them all. A key K is an arbitrary permutation of the alphabet. The size of key space is $|K| = 26! > 2^{74}$, which is too large for a successful brute force attack. However, monoalphetic ciphers can be readily broken using letter frequency analysis, given a long enough message. Because each occurence of a letter a in the msg is replace by same letter K|d| the most frequently occuring ~~msg~~ ~~will~~ letter of m is corresponding to most frequently occuring letter C.

(b) Message replay -:
It involves the reuse of captured data at a later time of benefit to the attacker then originally intended, inorder, to repeat some action

(c) Message Modification
Modify a packet header address for the purpose of directing it to an unintended destination or modifying the user data.

(d) DOS attack
This attack prevents the normal use or mangement of communication service & may take the form of either a targeted attack on a particular service or a broad, incapicitating attack.

Passive attacks -:
A passive attack is one on which the attacker only eave drop. He may see messages he do not suppose to see & monitor the network traffic but he does n alter messages.

Types -:
(a) Release of message contents.
In release of message contents the attacker gains the knowledge of confidential message being transfere from sender to receiver.

while she may not know what the most frequently occuring letter of m is, if the message is long enough & she knows that it's english, then it is quite likely that most most frequently occuring letter in m is one of the most frequently occuring letters in english (e or t) She can assume that most frequent letter $b_1$ in C is the 'e' the next most frequent letter $b_2$ is t & so forth. Of, course not all the guesses are right but the no. of likely candidate for each ciphertext letter is greatly reduced.

Moreover, many wrong guesses can be quickly discarded even without constructing the entire trial key because they lead to unlikely letter combinations

More generally could use a more complex equation to calculate the ciphertext letter for each plaintext letter $E_{(ab)}$: $i \longrightarrow a.i+b \bmod 26$, 'a' must not divide 26 otherwise cipher is not reversible

eg:- $\alpha = a$ & $\alpha = 0, b = 1, c = 2, \ldots y = 24, z = 25.$

eg:- $E_{(5,7)}$ $i \longrightarrow 5.i + 7 \bmod 26.$

Q4) What is transposition cypher? Illustrate with an example?

Ans:- Transposition cypher hide the msg content by rearranging the order of letters. Scytable cipher.

## Reverse Cipher

Write a message backwards

Plain :- I CAME I SAW I CONQUERED

Cipher :- DEREUQ ONOCIWASIE MACI

## Rail Fence Cipher

- Write a message with letters on alternate rows.
- Read off cipher row by row.

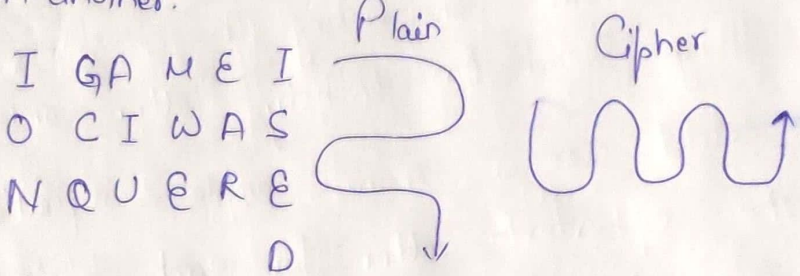
Plain :- IAESWCNURD

CMIAIOQEE

Cipher - IAESW CNURD CMIAI OQEE

## Geometric Figure

- Write message following one pattern & read out with another.




## Row transposition Cipher

- In general write in a number of columns & th some rule to read off from these columns.
- Key could be a series of number being the to: read of the cipher; or write in the plainte

Plain : THE SIMPLESTPOSSIBLETRANSPOSITION

Key (R) : 25413

Key (W) : 41532

THESI STIEH
MPLES ENSLP
TPOSS STSOP
IBLET EITLB
RANSP SRPNA
OSITI TOIIS
ONSXX XOXSN

Cipher : STIEH ENSLP STSOP EITLB SRPNA TOIIS XOXSN

Plain: ACONVENIENT WAYTO EXPRESS THE PERMUTATION

Key (W) : COMPUTER

Key (W) : 14358726

ANOVINCE
EW TAOTNY
HEPR TUEH
AOINXXTX

Cipher Text : ANOVINCEEW TAOTN YHEPR TUENA OINZZT

(05) Difference between Security mechanism & Security Services

Ans :- Security Services :-

(1) Confidentiality

It keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy. It could be achieved by physically securing t use of mathematical algo for data encryption.

(2) Data Integrity

The data may get modified by an unauthorized

entity intentionally or ~~unin~~ accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user.

(3) Authentication

It provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified & verified sender.

(4) Non Repudiation

Ensure that the entity cannot refuse the ownership of a previous commitment or an action.

## Security Mechanism

(1) Encipherment

This hiding data that provides confidentiality.

(2) Digital Integrity

The data integrity mechanism appends to the data a short check value that has been created by specific process from the data itself.

(3) Digital Signature

A Digital Signature means by which the sender can electronically sign the data & the receiver can electronically verify the signature.

(4) Authentication Exchange

(5) Traffic padding

(6) Routing Control

Q6) Differentiate between Symmetric key & Assymmetric key Cryptography.

Ans:- Symmetric Key Cryptography

It provides secure communication for a pair of communication partners.

Definition:- A symmetric key encryption scheme consist of a map

$$\mathcal{E} = M \times K \longrightarrow C,$$

such that for each $K \in K$ the map

$$E_K : M \to C, m \longrightarrow \mathcal{E}(K, m)$$

is invertible; The elements $m \in M$ are the plain texts & also called messages.

C is the set of ciphertext or cryptographs.

$K \in K$ are the keys

$D_K = E_K^{-1}$ is called the decryption function. It is assumed that efficient algo to compute $E_K$ & $D_K$ exist.

Assymmetric Key Cryptography

Each person's key is separated into 2 parts a public key for encryption available to everyone & a secret key for the decryption which is kept secret by the owner.

It is used for secure distribution of secret

key between a ~~pair of users~~, & at least some important forms of authentication & non-repudiation also require public key methods, such as digital signatures.

There is no shared secret key between a pair of users. Each user has a pair of keys, a secret key SK known only to him & public key PK known to everyone.

Q7) Describe Hill Cipher with an example.

Ans The Hill Cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical to operate one more that 3 symbols at once.

Exam A hill cipher uses $K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$ for encipherin the message

$\Rightarrow K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$

Decryption Key $= K^{-1}$

$KK^{-1} = I$

$K^{-1} = I/K$

$\Rightarrow \begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix}$

$K^{-1} \Rightarrow \frac{1}{K} \begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix}$

$\Rightarrow a_{11}a_{22} - a_{12}a_{21}$

$\Rightarrow 3 \times 7 - 2 \times 5 = 1$

$\Rightarrow K^{-1} = \frac{1}{11} \begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix}$

08) Discuss Shannon's theory of confusion & diffusion.

In Shannon's theory, Confusion refers to make the relationship between the key & the ciphertext as complex involved as possible; diffusion refers to the property that, redundancy in the statistics of the plain text is dissipated in the statistics of ciphertext.

Diffusion is associated with dependency of bits of the output on bits of the input. In a cipher with good diffusion, flipping an input bit should change each output bit with a probability of one half.

Substitution (Confusion)

Transforming a message by replacing the values of its elements according to some rule; for example, $C(i) = S(P(i))$ over all i in the message, where S is a substitution table indexed over the elements of the alphabet used

Transposition (Diffusion)

Transforming a message by placing its elements in different locations within the message, for example, $C(T(i)) = P(i)$ over all i in the message, where T is a transposition table indexed overall the character positions in the message.

09) Describe triple DES.

Triple DES uses 3 keys for the encryption. Here, firstly the DES encryption is done using key 1,

then DES decryption using key 2 & finally DES encryption using key 3 to obtain the cipher text.

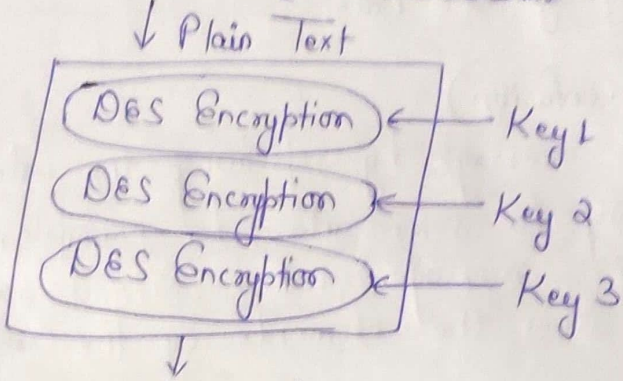
Encryption → Triple DES uses a "key bundle" which comprises 3 DES keys $K_1, K_2, K_3$ each of 56-bits

The Encryption Algo is :-

Ciphertext = $E_{K3}(D_{K2})(E_{K1}(\text{Plaintext}))$.

i.e. DES encrypts with $k_1$, DES decrypts with $K_2$, then DES encrypts with $K_3$.

Plaintext → DES $E_{K_1}$ → DES $D_{K_2}$ → DES $E_{K_3}$ → Ciphertext




Decryption → Plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{Ciphertext}))$

i.e. decrypt with $K_3$, encrypt with $K_2$, & then decrypt with $K_1$.

Ciphertext → DES $D_{K3}$ → DES $E_{K2}$ → $D_{K1}$ → Plaintext.

(10) Discuss the strength of IDEA.

In cryptography, block ciphers are very important in the designing of many cryptographic algos &

are widely used to encrypt the bulk of data in chunks. By Chunks, it means that the cypher takes a fixed size of the plaintext in the encryption process & generates a fixed size ciphertext using a fixed-length key. An algo. strength is determined by its key length.

IDEA (Simplified International Data Encryption Algorithm) is a key block cypher that -:

→ Use a fixed-length plain text of 16 bits &
→ Encrypts them in 4 chunks of 4 bits each.
→ Produce 16 bits Ciphertexts
→ The length of key is used is 32 bits
→ The key is also divided into 8-blocks of 4 bits each.