UNIT – 1

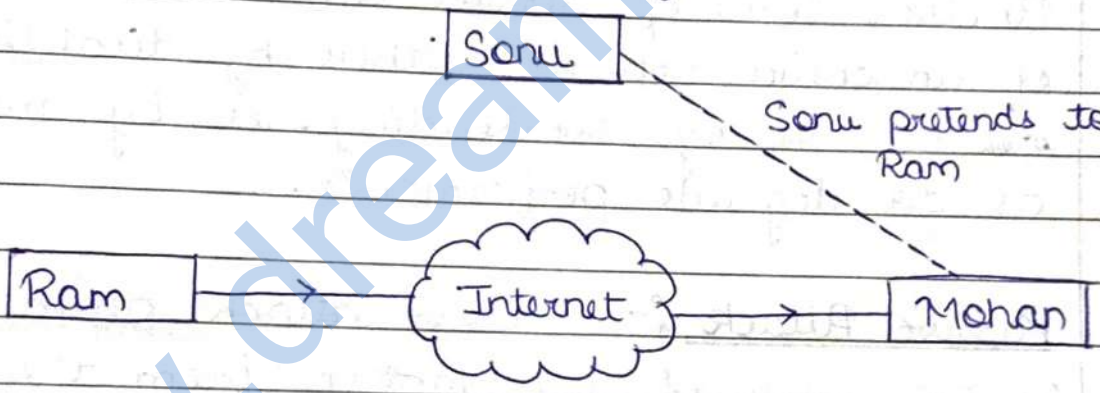
Introduction

★ **Attacks :-**

(1.) **Active attack** – An active attack attempts to alter system resources or affect their operations. Active attack involve some modification of data stream or creation of false statement.

Types of active attacks are as follows –

1- **Masquerade** – This attack takes place when one entity pretends to be different entity.



2- **Modification of messages** – It means that some portion of a message is altered or that message is delayed or recorded to produce an unauthorised effect.
For example – "Mohan is allowed to read confidential file x" is modified as "Sonu is allowed to access confidential file x".

3- **Repudiation** – This attack is done by either sender or receiver. The sender or receiver can deny later that he or she has send or receive a message.

Example – Customer ask his bank "to transfer an amount to someone" and later on the sender (customer) deny that he had made such a request. This is repudiation.

4- Replay – It involves the passive capture of a message and its sub-sequent the transmission to produce an authorised effect.

5- Denial of Service – It prevents normal use of communication facilities. This attack may have a specific target.
Example- An entity may suppress all messages directed to a particular destination.
Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it by messages so as to degrade performance.

(2) Passive Attack :- Passive attack attempts to learn or make use of information from the system but does not affect system resources.
Passive attacks are in the nature of monitoring of transmission. ~~The release~~

1- The release of message content – Telephonic conversation, e-mail message or a transfered message contain sensitive or confidential information. We would like to prevent an opponent from learning the content of these transmissions.

2- Traffic analysis – We had to make encryption of

information so that the attacker even if captured, the ~~message~~ attacker could not extract any information from the message.

The opponent could determine the location and identity of communicating host, and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

★ **Security Services** :- Security services are the methods used to enhance the security of the network. It helps in implementing security policies and uses various security mechanisms. A security mechanism is a method which is used to protect your message from unauthorised entity. There are four types of security services -

1- **Authentication** - Authentication ensures that the entity sending or receiving the messages is the one, It is actually pretending to be. Two types of authentications mainly used in network are -

(i) Peer entity authentication used in association with a logical connection to provide confidence in the identity of the entities connected.

(ii) Data origin authentication, in a connectionless transfer, provides assurance that the source of received data is as claimed.

2- **Access Control** - Access control prevents the unauthorized use of resources. This service control who can have

access to a resource, under what conditions access can occur and what those accessing that resource are allowed to do.

In other words, access control can be defined as the ability to permit or deny the use of something by someone.

3- **Data confidentiality** — Data confidentiality avoids unauthorized access by ensuring that the data is being received safely by the original receiver, for whom it was actually meant for. Various types of confidentiality are as follow -

(i) **Connection Confidentiality** - The protection of all user data on a connection.

(ii) **Connectionless Confidentiality** — The protection of all user data in a single data block.

(iii) **Selective field Confidentiality** — The confidentiality of selected fields within the user data on a connection or a single data-block.

(iv) **Traffic flow Confidentiality** — The protection of the information that might be derived from observation of traffic flow.

4- **Data Integrity** — Data integrity ensures that data received is exactly the same as sent by an authorised entity (i.e. contains no modification, insertion, deletion or replay).

* **Security Mechanism :-** Security mechanism deals with identification of any break in security and also helps in removing it. It is different from security services. Security mechanisms are also used to identify and recover from various security attacks.

Security mechanisms are as follows -

1- **Encipherment :** Encipherment is also known as encryption. It is the process of using mathematical formulas, algorithms and the keys to transform the simple message into a message that is not easily understood by each and everyone.

2- **Digital Signatures :** These are similar to signatures on paper done in real life but these are done in computer documents and in cryptographic format to ensure the source and integrity.

3- **Access Control :** Access control includes variety of techniques used to avoid unauthorized access or granting only limited access to data or network resources.

4- **Data Integrity :** It ensures that the data received on receiver side is same as sent by the original data transfer.

5- **Routing Control :** Routing control is a computer network technique that uses various mechanisms to avoid the traffic congestion in the network. It helps in denial of service attack.

★ **Cryptography** :- Cryptography is a science which is used in encryption and decryption of data. Cryptography enables us to store sensitive information or transmit it across insecure networks (like internet) so that it cannot be read by anyone except the intended receipent.

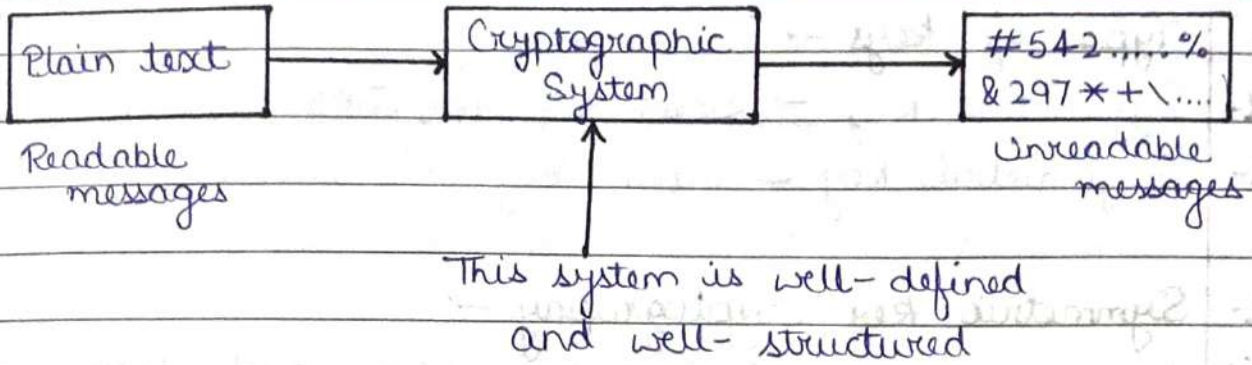
Cryptography is a Greek word which means secret writing.

The sender encrypts a message using a secret key and the receiver decrypts it before reading. Someone who intercepts the message sees only a apparently random symbols. Without the key he cannot read it. Cryptography is a practice and study of hiding information.

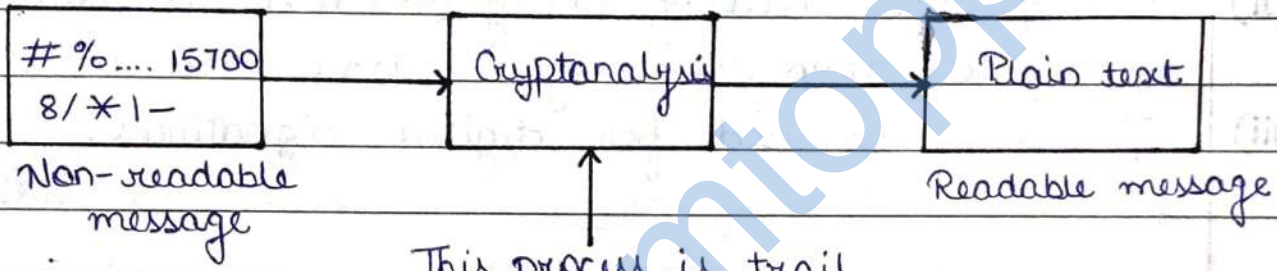
Example —

It is the art and science of achieving security by encoding messages to make them non-readable. Cryptography has been defined as the 'UMBRELLA' word used to describe the entire field of secret communication.

The purpose of cryptography was to hide something that had been written. It can also be applied to software, graphics, voice i.e. it can be applied to anything. That can be digitally coded.



* **Cryptanalysis :-** It is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.



Cryptology – It is the combination of cryptography and cryptanalysis.

Cryptography + Cryptanalysis = Cryptology

* **Key :-** In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text or to decrypt encrypted text.

In database content, a key is a unique field that is used for sorting or selecting record.

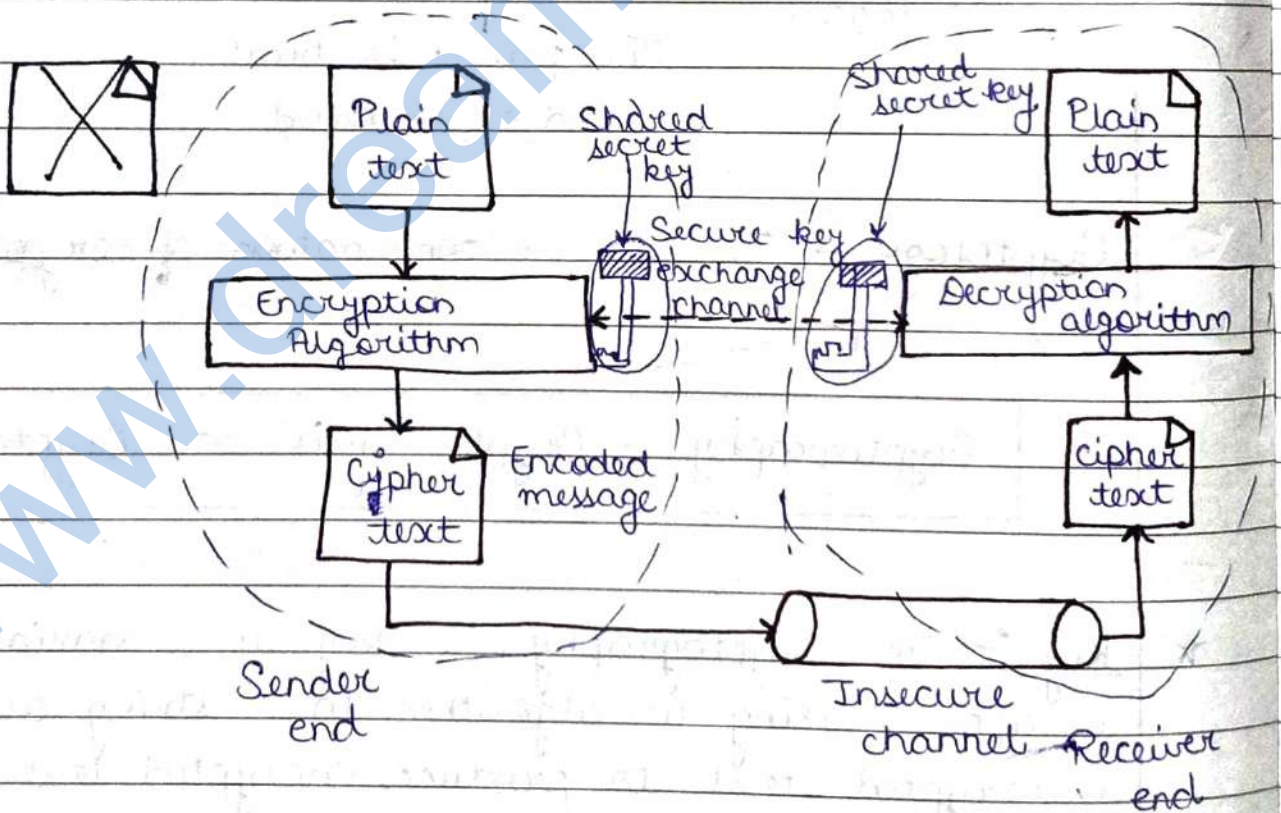
1. Symmetric key
2. Asymmetric key

• Types of keys –

1- Symmetric key – Secret key encryption
2- Asymmetric key – Public key encryption

1- Symmetric key cryptography –

(i) Same key is used for encryption and decryption.
(ii) It is very fast.
(iii) Key exchange is a big problem.
(iv) It is also called secret key encryption.
(v) The sender and receive must share the algorithm and the key.
(vi) Size of the resulting encrypted text is usually same as or less than the original clear text size.
(vii) It cannot be used for digital signatures.



2- Asymmetric key cryptography –

(i) One key for encryption and other key for decryption are used.

(ii) It is slower than symmetric key encryption.
(iii) Key exchange is not a problem.
(iv) One of the two keys must be kept secret.
(v) The sender and the receiver must each have one of the matched pair of keys.
(vi) Size of the resulting encrypted text is more than original clear text size.
(vii) It can be used for digital signature.

★ **Public Key Encryption / Public key Cryptography :-**

→ It is also called assymmetric key encryption. It uses two keys - public key and private key.

→ Public key of a user is used to encrypt message. Public key is also known as encryption key.

→ Private key of the receiver is used to decrypt the message. Private key is also called decryption key.

→ It is asymmetric because those who encrypt the message or verify signatures cannot decrypt messages or create signatures.

→ A message can be encrypted with the public key and decrypted by the private key, to provide security.

→ Each system generates a pair of keys. Each system publishes its public key and keeps its private key as secret. The keys are generated in such a way that it is impossible to derive the private key from the public key.

→ The private key is kept secret and it not sent over the message to the receiver, although the public key is.

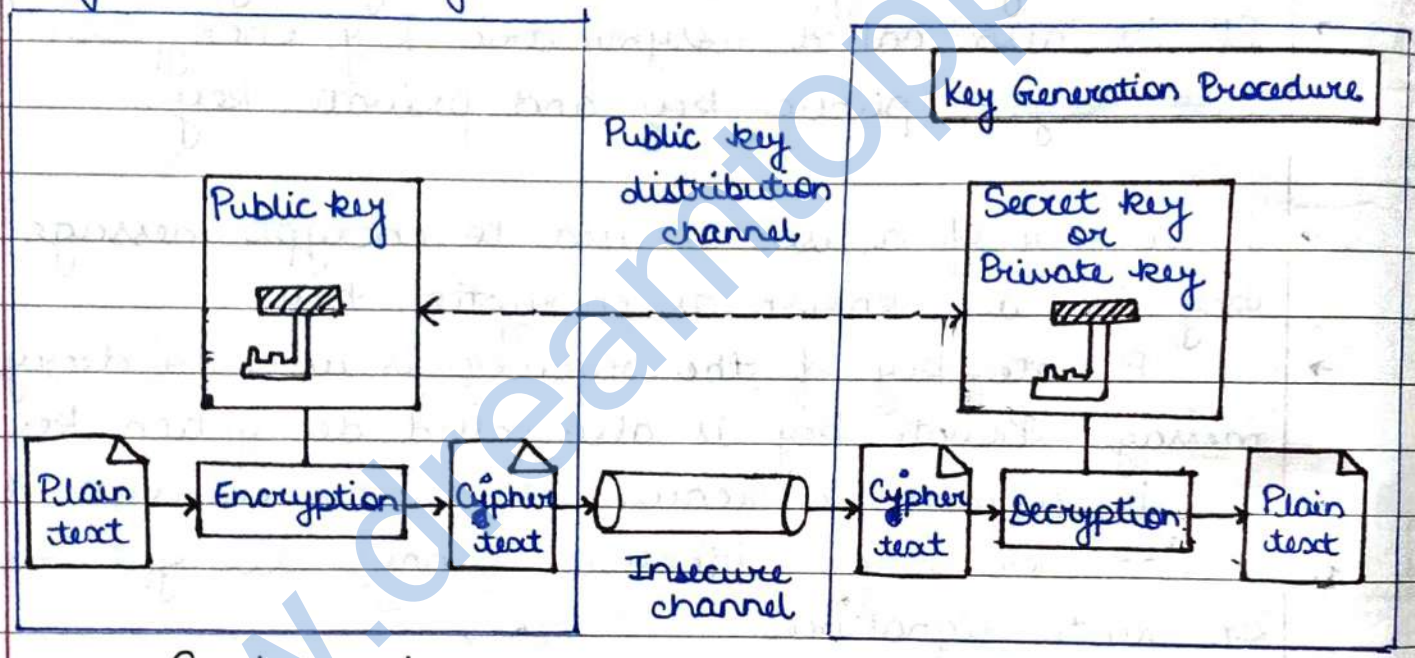
8 → Public key encryption is also used for authentication.

Advantages –

1- It provides strong security, because of two keys are used.
2- They can provide a method for digital signature.
3- There is no need for exchange keys, so it reduces key distribution problem.

Disadvantages –

1- Encryption and decryption takes long time.
2- Not suitable for long messages.
3- Key size is larger.



2- Discuss the role of digital signature in modern communication. Also discuss the differences between digital certificates and digital signatures in authentication.

★ Digital signature and authentication :-

- Digital signature is same as a person's signature on a document. A digital signature on a message is required for the authentication and identification of right sender.
- Digital signature supposed to be unique to an individual and serves as a means of identification of the sender.
- Any public key cipher can be used for digital

signature. Digital signature standard (DSS) is a digital signature format that has been standardized by NIST (National Institute of Standards and Technology) a unit of US commerce department.

- Hash value of a message when encrypted with the private key of a person is his digital signature on that e-document.
- Digital signature of a person therefore varies from document to document, thus ensuring authenticity of each word of that document.
- As the public key of the signer is known, anybody can verify the message and the digital signature.
- Each individual generates his own key-pair. Public key is known to everyone and private key only to the owner.
- The originator of a message uses a signing key (private key) to sign the message and that it has not been tempered with while in transmit.
- Digital signatures uses three algorithm -

1. Key generation
2. Signing algorithm
3. Signature verifying algorithm

1- Key Generation — This algorithms selects a private key uniformly at random from a set of possible private keys. Output of this algorithm is private key and its corresponding public key.

2- Signing Algorithm — It produce signature by using message and private key.

3- Signature Verifying Algorithm — For a given message,