

CRYPTOGRAPHY NETWORK SECURITY

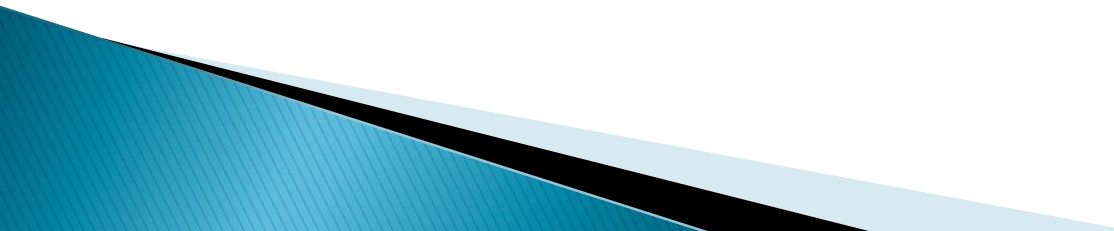
Security Services

1.Authentication:

Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identity is preregistered can prove his/her identity and can access the sensitive information.

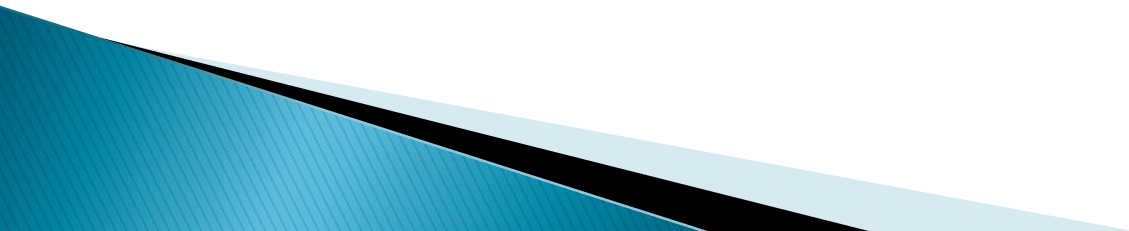
2.Authorization(Access control):

The principle of access control is determined by role management and rule management. Role management determines who should access the data while rule management determines up to what extent one can access the data. The information displayed is dependent on the person who is accessing it.



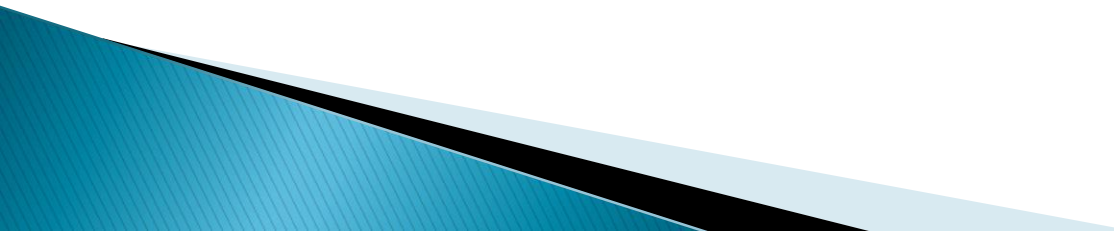
3.Non-Repudiation:

Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.



4.Auditing

It will analyze the data. It is having entire information of data. So, whenever hacking or any unauthorized transaction happens this data will be in auditing. This data will be trace by hacker. It will have sender and receiver data. How the data being sent through SMS or Internet all this data will be in auditing.



Security Mechanisms

- Network Security is field in computer technology that deals with ensuring security of computer network infrastructure. Therefore security mechanism can also be termed as is set of processes that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.

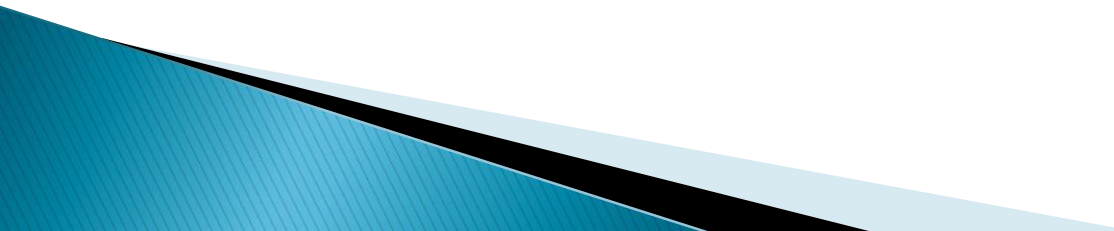
- ▶ There are five types of security mechanisms. They are:

1. **Encipherement :**

This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherement. Level of data encryption is dependent on the algorithm used for encipherement.

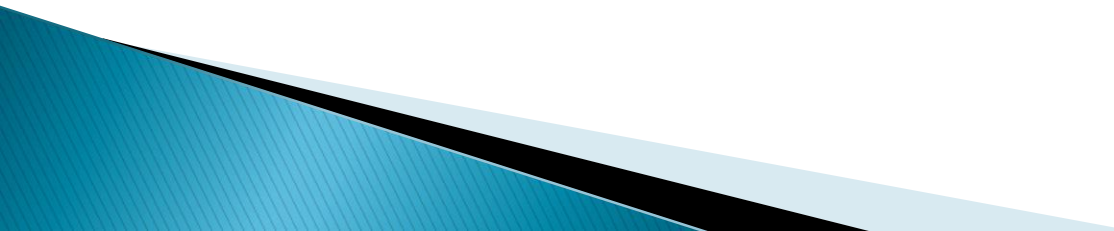
2.Digital Signature :

This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.



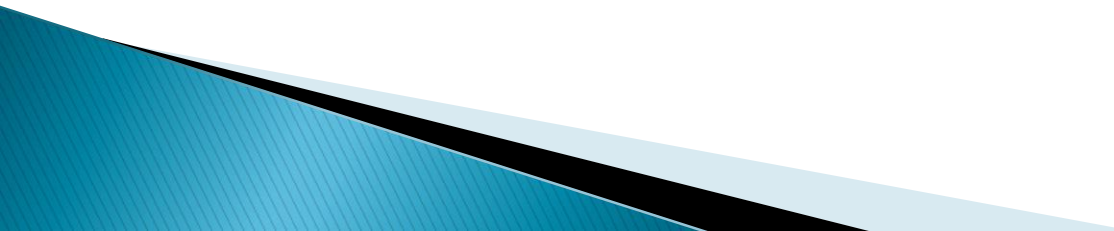
3.Access Control :

This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.



4.Authentication exchange :

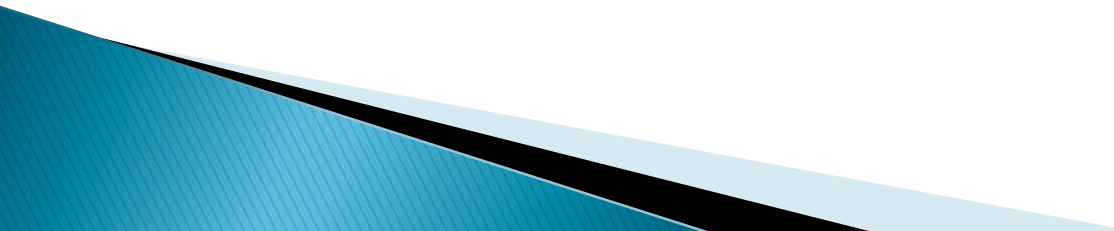
This security mechanism deals with identity to be known in communication. In this we will Authenticate user that means we will allow him to do modifications in our data. By declaring a person as authenticate user.



5.Traffic Padding

In this we add extra bits or extra packets. The main purpose to add extra bits is to in order to confuse the Attacker means third party person.

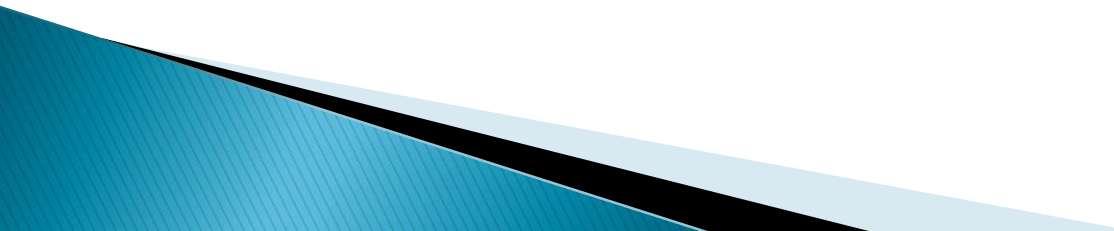
Traffic padding is done in order to prevent the process of Traffic analysis. We can add extra bits in between or starting or at end.



6. Routing Control

When we are sending a message from sender to receiver, we are having different paths we can choose any path or mixture of paths also.

In order to confuse third party we choose mixture path. If we change directions multiple time the third party will get confused.



▶ Cryptographic systems in which the system we use Cryptography all those things divided based on three main Categories:

1. Based on type of Operation: which type of operation is used to convert plain text to cipher text. Based on that it is divided in to two parts:

1. Substitution Technique

2. Transposition Technique



Substitution technique

- ▶ The *substitution technique* involves replacing letters with other letters and symbols. In simple terms, the plaintext characters are substituted, and additional substitute letters, numerals, and symbols are implemented in their place.

Example: Good
 Hood

Transposition Technique

- ▶ In the *transposition technique*, the characters' identities are kept the same, but their positions are altered to produce the cipher text. Transposition technique elements in plain text are arranged. We cannot add new element in it.

Example: Good

dooG