**UNIT -06**

**Network Security**

6.1Active and Passive attacks

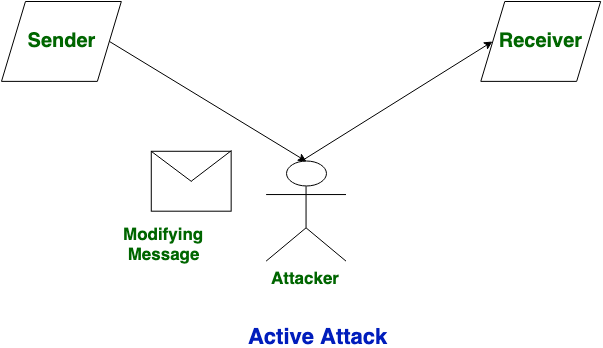
6.2Cryptography (Symmetric and Asymmetric)

6.3Firewall

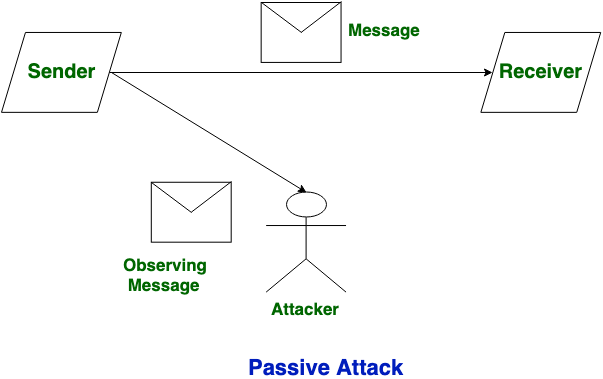
Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

**ActiveAttacks:**  
Active attacks are the type of attacks in which, The attacker efforts to change or modify the content of messages. Active Attack is danger for Integrity as well as availability. Due to active attack system is always damaged and System resources can be changed. The most important thing is that, In active attack, Victim gets informed about the attack.



**Passive Attacks:**  
Passive Attacks are the type of attacks in which, The attacker observes the content of messages or copy the content of messages. Passive Attack is danger for Confidentiality. Due to passive attack, there is no any harm to the system. The most important thing is that In passive attack, Victim does not get informed about the attack.



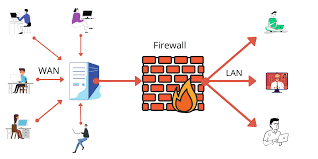
**Difference between Active Attack and Passive Attack:**

|  |  |  |
| --- | --- | --- |
| S.NO | Active Attack | Passive Attack |
| 1. | In active attack, Modification in information take place. | While in passive attack, Modification in the information does not take place. |
| 2. | Active Attack is danger for **Integrity** as well as **availability**. | Passive Attack is danger for **Confidentiality**. |
| 3. | In active attack attention is on detection. | While in passive attack attention is on prevention. |
| 4. | Due to active attack system is always damaged. | While due to passive attack, there is no any harm to the system. |
| 5. | In active attack, Victim gets informed about the attack. | While in passive attack, Victim does not get informed about the attack. |
| 6. | In active attack, System resources can be changed. | While in passive attack, System resources are not change. |
| 7. | Active attack influence the services of the system. | While in passive attack, information and messages in the system or network are acquired. |
| 8. | In active attack, information collected through passive attacks are used during executing. | While passive attack are performed by collecting the information such as passwords, messages by itself. |
| 9. | Active attack is tough to restrict from entering systems or networks. | Passive Attack is easy to prohibited in comparison to active attack. |

## Firewalls

Firewalls function much like gates that can be used to secure the borders between your network and the internet. Firewalls are used to manage network traffic, allowing authorized traffic through while blocking access to non-authorized traffic.

A firewall is a [network security](https://www.forcepoint.com/cyber-edu/network-security)device that monitors incoming and outgoing network traffic and permits or blocks data [packets](https://www.forcepoint.com/cyber-edu/packet-loss) based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.



A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

**Firewalls are commonly used in private networks** or *intranets* to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

### Hardware and Software Firewalls

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

## **Types of Firewalls**

## **Packet filtering**

A small amount of data is analyzed and distributed according to the filter’s standards.

* **Proxy service**

Network security system that protects while filtering messages at the application layer.

* **Stateful inspection**

Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.

### **Next Generation Firewall (NGFW)**

Deep packet inspection Firewall with application-level inspection.

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

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

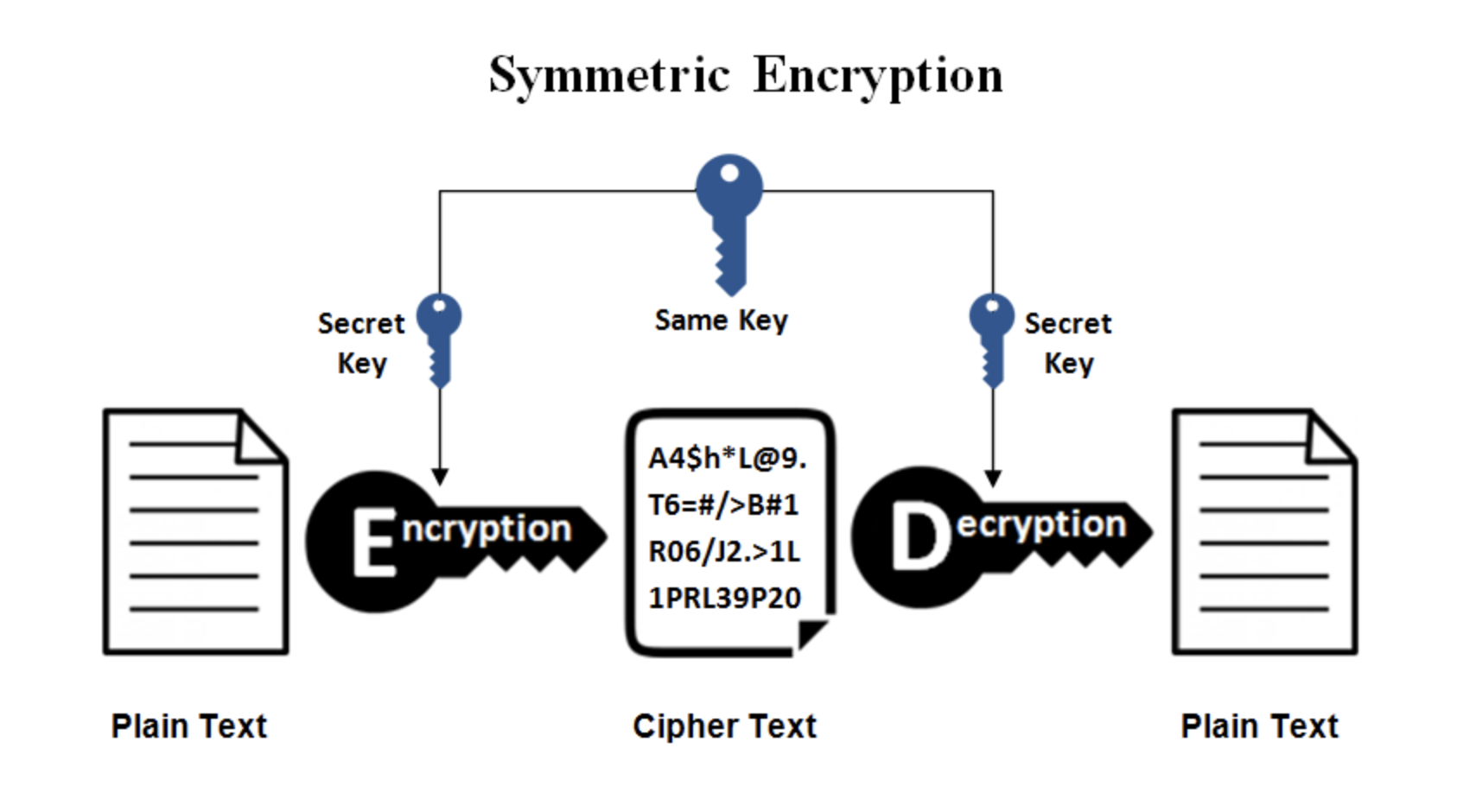
**Techniques used For Cryptography:**  
In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

**Features Of Cryptography are as follows:**

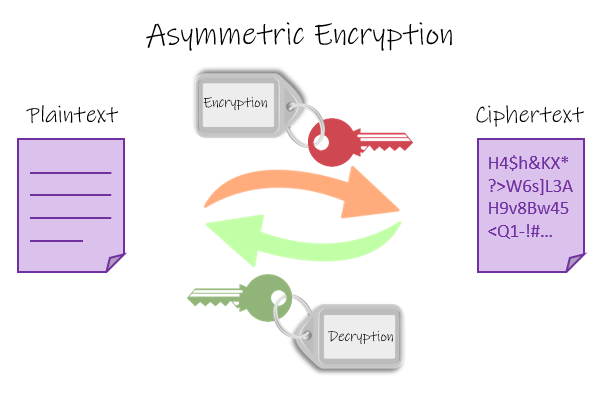
1. **Confidentiality:**  
   Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:**  
   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:**  
   The creator/sender of information cannot deny his or her intention to send information at later stage.
4. **Authentication:**  
   The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

**Types Of Cryptography:**  
In general there are three types Of cryptography:

1. **Symmetric Key Cryptography:**  
   It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).



1. **Hash Functions:**  
   There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
2. **Asymmetric Key Cryptography:**  
   Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.



Symmetric key encryption algorithms use a single symmetric key for both encryption and decryption, whereas asymmetric key encryption algorithms (aka public key algorithms) use two different but related keys for encryption and decryption.

Symmetric algorithms have the advantage in that they are much faster than asymmetric algorithms, and can handle thousands of keys with very little computing overhead. However, the disadvantage is that a symmetric key must be kept secret, and yet has to be transmitted to the receiving end, which means there is a possibility of it being intercepted and used by an eavesdropper to illicitly decrypt the message.

In Assymetric key sender can encrypt the message with the intended recipient’s public key and the recipient can use their corresponding private key to decrypt it.

