7. Network Security

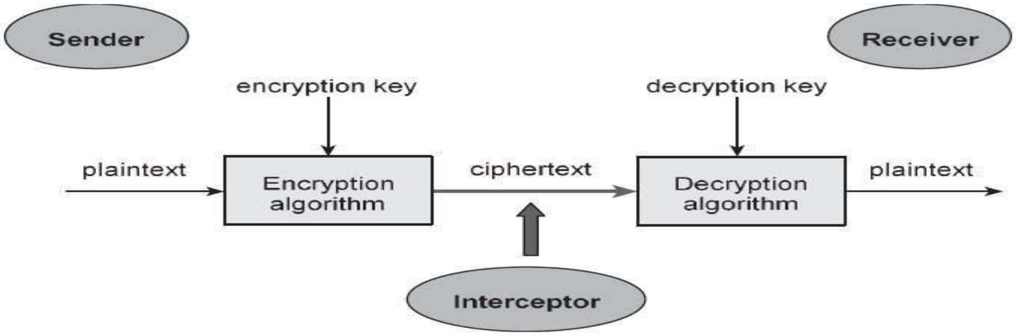
A) Cryptography, Digital Signature

1. Cryptography

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.

Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in nonrepudiation. This means that the sender and the delivery of a message can be verified.

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a **cipher system**.



The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.
The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

Components of a Cryptosystem
The various components of a basic cryptosystem are as follows −

- **Plaintext.** It is the data to be protected during transmission.
- **Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key.
- **Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
- **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext.
- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext. For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

Classification –

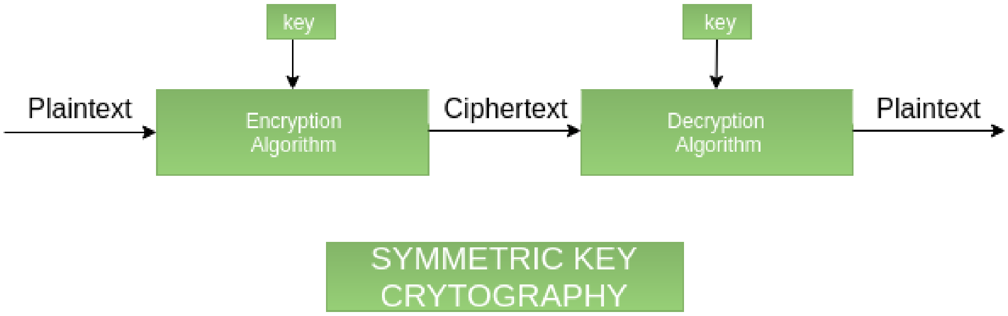
The flowchart depicts that cryptology is only one of the factors involved in securing networks. Cryptology refers to study of codes, which involves both writing (cryptography) and solving (cryptanalysis) them. Below is a classification of the crypto-terminologies and their various types:

a) Cryptography –

Cryptography is classified into symmetric cryptography, asymmetric cryptography and hashing. Below are the description of these types.

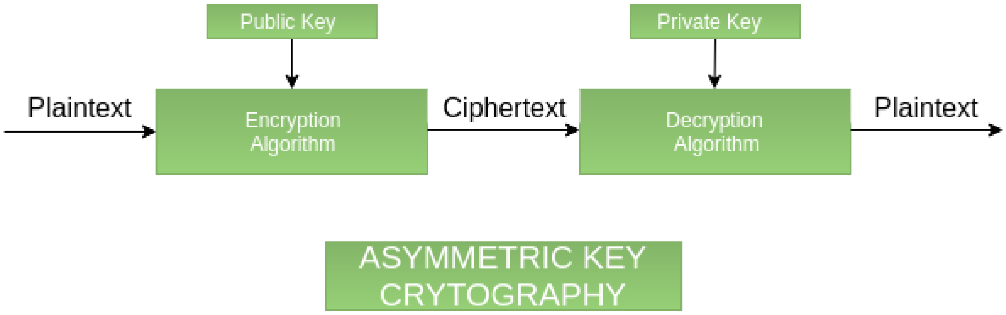
i. **Symmetric key cryptography –**

It involves usage of one secret key along with encryption and decryption algorithms which help in securing the contents of the message. The strength of symmetric key cryptography depends upon the number of key bits. It is relatively faster than asymmetric key cryptography. There arises a key distribution problem as the key has to be transferred from the sender to receiver through a secure channel.



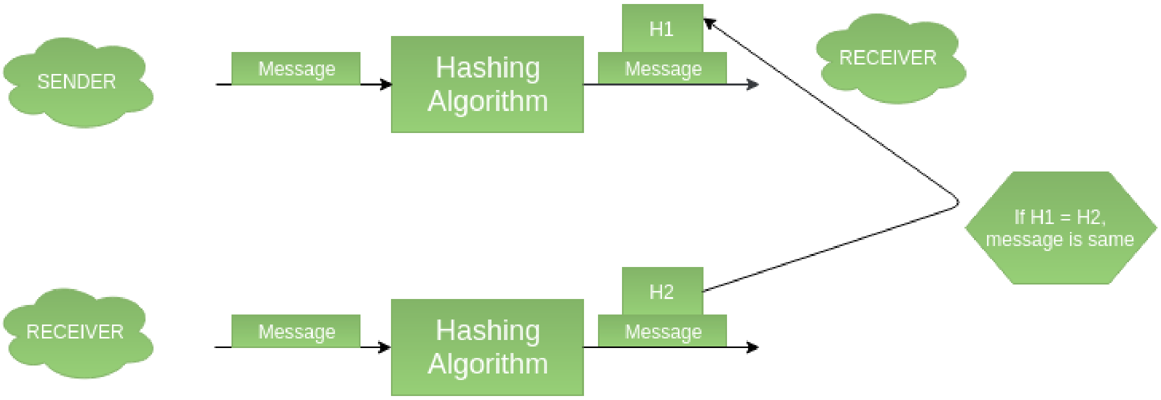
ii. **Assymetric key cryptography –**

It is also known as public key cryptography because it involves usage of a public key along with secret key. It solves the problem of key distribution as both parties uses different keys for encryption/decryption. It is not feasible to use for decrypting bulk messages as it is very slow compared to symmetric key cryptography.



iii. **Hashing –**

It involves taking the plain-text and converting it to a hash value of fixed size by a hash function. This process ensures integrity of the message as the hash value on both, sender\'s and receiver\'s side should match if the message is unaltered.



b) Cryptanalysis –

1. **Classical attacks –**
   It can be divided into a)Mathematical analysis and b) Brute-force attacks. Brute-force attacks runs the encryption algorithm for all possible cases of the keys until a match is found. Encryption algorithm is treated as a black box. Analytical attacks are those attacks which focuses on breaking the cryptosystem by analysing the internal structure of the encryption algorithm.
2. **Social Engineering attack –**
   It is something which is dependent on the human factor. Tricking someone to reveal their passwords to the attacker or allowing access to the restricted area comes under this attack. People should be cautious when revealing their passwords to any third party which is not trusted.
3. **Implementation attacks –**
   Implementation attacks such as side-channel analysis can be used to obtain a secret key. They are relevant in cases where the attacker can obtain physical access to the cryptosystem.

2. Digital Signature:

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer. A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature:

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

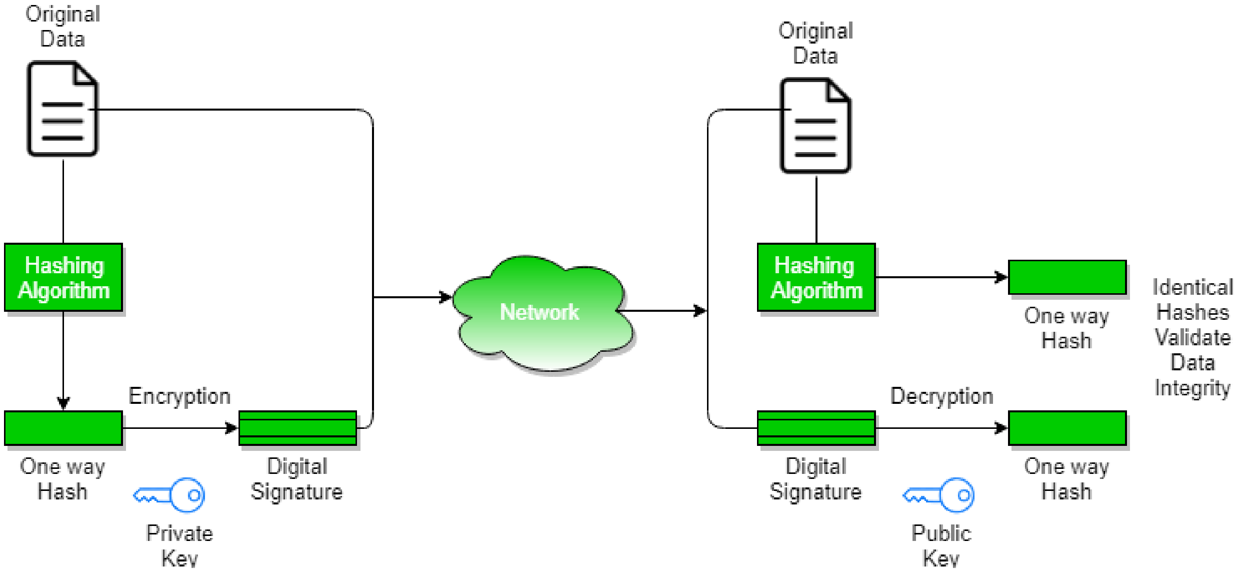
Components in Digital Signature:

1. **Key Generation Algorithms** : Digital signature are electronic signatures, which assures that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise the data can be altered or someone can also act as if he was the sender and expect a reply.
2. **Signing Algorithms**: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier.
3. **Signature Verification Algorithms** : Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.

The steps followed in creating digital signature are :

1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
2. Digital signature is then transmitted with the message.(message + digital signature is transmitted)
3. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).
4. The receiver now has the message digest.
5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).
6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a is easy but computation of a from hash value of a is very difficult.



Digital Certificate

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.

A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital signature is used to attach public key with a particular individual or an entity.

Digital certificate contains:-

1. Name of certificate holder.
2. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
3. Expiration dates.
4. Copy of certificate holder's public key.(used for encrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

Digital ceritifcate is also sent with the digital signature and the message.

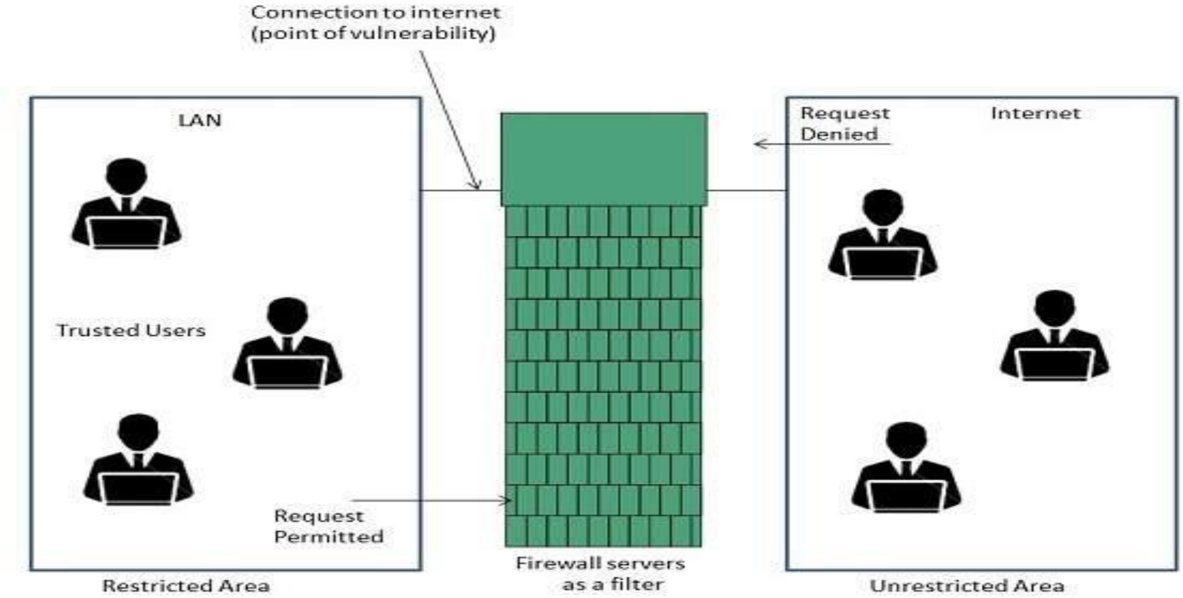
B) Firewalls

Firewall establishes a barrier between secured internal networks and outside untrusted network, such as Internet. Firewall is a network security device, either hardware or software based, which monitors all incoming and outgoing traffic and based on defined set of security rules it accept, reject or drop that specific traffic.

Accept : allow the traffic

Reject : block the traffic but reply with an “unreachable error”

Drop : block the traffic with no reply



Types of Firewall

Firewalls are generally of two types:

1. **Host- based Firewalls :** Host-based firewall are installed on each network node which controls each incoming and outgoing packet. It is a software application or suit of applications, comes as a part of operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filters all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on firewall. A Network firewall might have two or more network interface cards (NICs). Network-based firewall is usually a dedicated system with proprietary software installed.

Firewall Methodologies –

There are certain methods through which firewall can be implemented. These are as follows:

1. **Static packet filtering –** Packet filtering is a firewall technique used to control access on the basis of source IP address, destination IP address, source Port number and destination port number. It works on layer 3 and 4 of OSI model. Also, an ACL doesn’t maintain the state of session. A router with ACL applied on it is an example of static packet filtering.
2. **Stateful packet filtering –**
   In stateful packet filtering, the state of the sessions are maintained i.e when a session is initiated within a trusted network, it’s source and destination IP address, source and destination ports and other layer information are recorded. By default, all the traffic from untrusted network is denied.
   The replies of this session will be allowed only when the IP addresses (source and destination IP address) and port numbers (source and destination)are swapped.

3. **Proxy firewalls –**
   These are also known as application layer firewalls. Proxy firewall acts as an intermediary between the original client and the server. No direct connection takes place between the original client and the server. The client, who has to establish a connection directly to the server to communicate with it, now have to establish a connection with proxy server. The proxy server then establishes a connection with the server on the behalf of client. Now, the client sends the data to the proxy server and proxy server forwards it to the server. Proxy server can operate upto layer 7 (application layer).

4. **Application inspection –**
   These can analyze the packet upto layer 7 (deep inspection) but can't act as a proxy server. These can deeply analyze conversation between a client and server even when the server is assigning a dynamic port to the client therfore it doesn't fail in these cases (which can occur in stateful firewall).

5. **Transparent firewall –**
   By default, the firewall operates at layer 3 but the benefit of using transparent firewall is that it can operate at layer 2. It has 2 interfaces which will act like a bridge so can be configured through a single management IP address. Also, users accessing the network will not even know about that a firewall exists.

6. **Network Address Translation (NAT) –**
   NAT is implemented on a router or firewall. NAT is used to translate private IP address into a public IP address through which we can hide our source IP address.
   And if we are using dynamic NAT or PAT, an attacker will not be able to know that what devices are dynamically assigned which IP address from the pool. This makes difficult to make a connection from outside world to our private network.

7. **Next-Generation Firewalls –**
   NGFWs are third generation security firewall that is implemented in either in software or device. It combines basic firewall properties like static packet filtering, application inspection with advanced security features like integrated intrusion prevention system. Cisco ASA with firePOWER services is an example of Next-Generation firewall.

C) VPN or Virtual Private Network

VPN stands for virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. Virtual Private network is a way to extend a private network using a public network such as internet. The name only suggests that it is Virtual "private network" i.e. user can be the part of local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

Why do I need a VPN?

- **Hide your IP address**
  Connecting to a Virtual Private Network often conceals your real IP address.
- **Change your IP address**
  Using a VPN will almost certainly result in getting a different IP address.
- **Encrypt data transfers**
  A Virtual Private Network will protect the data you transfer over public WiFi.
- **Mask your location**
  With a Virtual Private Network, users can choose the country of origin for their Internet connection.
- **Access blocked websites**
  Get around website blocked by governments with a VPN.

Types of VPN

VPN is a Virtual Private Network that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection, known as VPN tunnel, and all Internet traffic and communication is passed through this secure tunnel. Thus, keeping the user data secure and private.

There are two basic VPN types which are explained below.

1. Remote Access VPN

Remote access VPN allows a user to connect to a private network and access its services and resources remotely. The connection between the user and the private network happens through the Internet and the connection is secure and private. Remote Access VPN is useful for business users as well as home users.
A corporate employee, while traveling, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network.
Home users, or private users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users conscious of Internet security also use VPN services to enhance their Internet security and privacy.

2. Site – to – Site VPN

A Site-to-Site VPN is also called as Router-to-Router VPN and is mostly used in the corporates. Companies, with offices in different geographical locations, use Site-to-site VPN to connect the network of one office location to the network at another office location. When multiple offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN. When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN. Basically, Site-to-site VPN create a virtual bridge between the networks at geographically distant offices and connect them through the Internet and maintain a secure and private communication between the networks.

Since Site-to-site VPN is based on Router-to-Router communication, in this VPN type one router acts as a VPN Client and another router as a VPN Server. The communication between the two routers starts only after an authentication is validated between the two.

Types of VPN protocols

The above two VPN types are based on different VPN security protocols. Each of these VPN protocols offer different features and levels of security, and are explained below:

1. Internet Protocol Security or IPSec:

Internet Protocol Security or IPSec is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by authenticating the session and encrypts each data packet during the connection.

IPSec operates in two modes, Transport mode and Tunneling mode, to protect data transfer between two different networks. The transport mode encrypts the message in the data packet and the tunneling mode encrypts the entire data packet. IPSec can also be used with other security protocols to enhance the security system.

2. Layer 2 Tunneling Protocol (L2TP):

L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is usually combined with another VPN security protocol like IPSec to create a highly secure VPN connection. L2TP creates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and handles secure communication between the tunnel.

3. Point – to – Point Tunneling Protocol (PPTP):

PPTP or Point-to-Point Tunneling Protocol creates a tunnel and encapsulates the data packet. It uses a Point-to-Point Protocol (PPP) to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the time of Windows 95. Apart from Windows, PPTP is also supported on Mac and Linux.

4. Secure Sockets Layer (SSL) and Transport Layer Security (TLS):

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) create a VPN connection where the web browser acts as the client and user access is restricted to specific applications instead of entire network. SSL and TLS protocol is most commonly used by online shopping websites and service providers. Web browsers switch to SSL with ease and with almost no action required from the user, since web browsers come integrated with SSL and TLS. SSL connections have https in the beginning of the URL instead of http.

5. OpenVPN:

OpenVPN is an open source VPN that is useful for creating Point-to-Point and Site-to-Site connections. It uses a custom security protocol based on SSL and TLS protocol.

6. Secure Shell (SSH):

Secure Shell or SSH creates the VPN tunnel through which the data transfer happens and also ensures that the tunnel is encrypted. SSH connections are created by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.