Cryptography and Network Security Principles

In present day scenario security of the system is the sole priority of any organisation. The main aim of any organisation is to protect their data from attackers.
In cryptography, attacks are of two types such as Passive attacks and Active attacks. Passive attacks are those that retrieve information from the system without affecting the system resources while active attacks are those that retrieve system information and make changes to the system resources and their operations.

The Principles of Security can be classified as follows:

1. **Confidentiality:**
   The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message.
   For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

2. **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 sensible information.

3. **Integrity:**
   Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

4. **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.

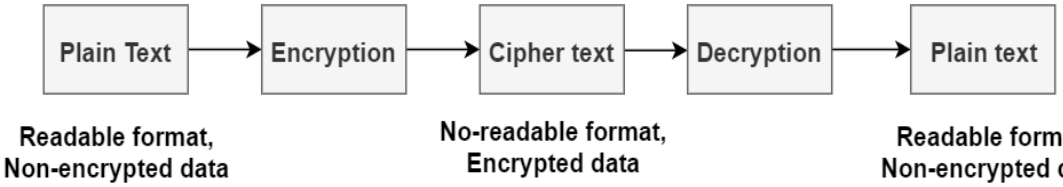
5. **Access control:**
   The principle of access control is determined by role management and rule management. Role management determines who should access the data while rule management determines up to what extent one can access the data. The information displayed is dependent on the person who is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

6. **Availability:**
   The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

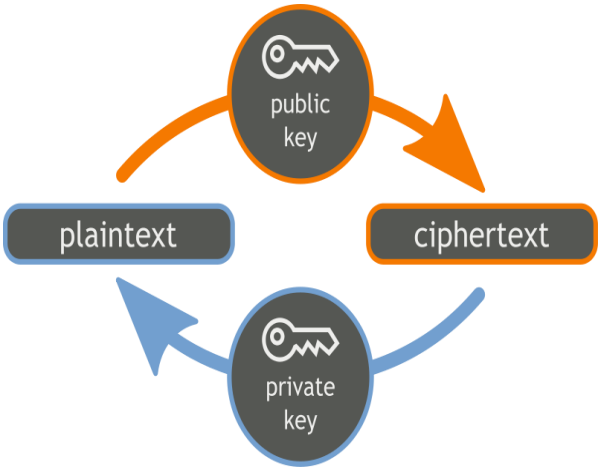
Cryptography and its Types

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.



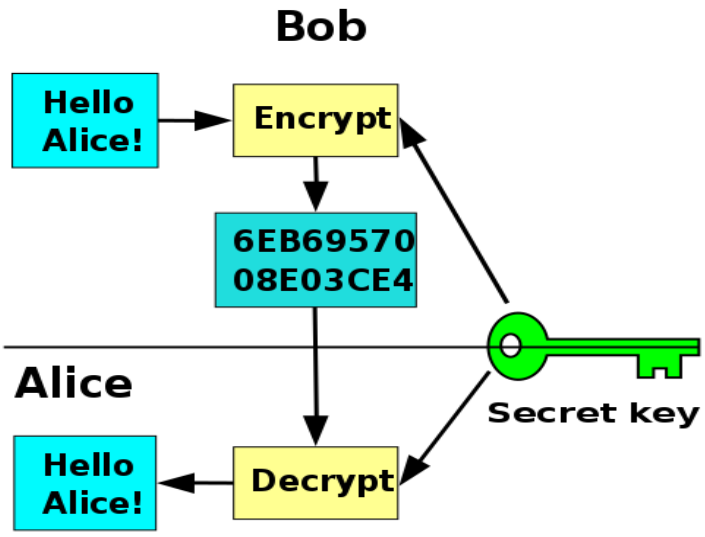
The **main difference** between public key and private key in cryptography is that the **public key is used for data encryption while the private key is used for data decryption.**
The public key and private key are two locking mechanisms used in asymmetric encryption of cryptography. Public key is a type of lock used with an encryption algorithm to convert the message to an unreadable form. Private key is a type of lock used with a decryption algorithm to convert the received message back to the original message. Both these keys help to ensure the security of the exchanged data. In brief, a message encrypted with the public key cannot be decrypted without using the corresponding private key.



TYPES OF CRYPTOGRAPHY

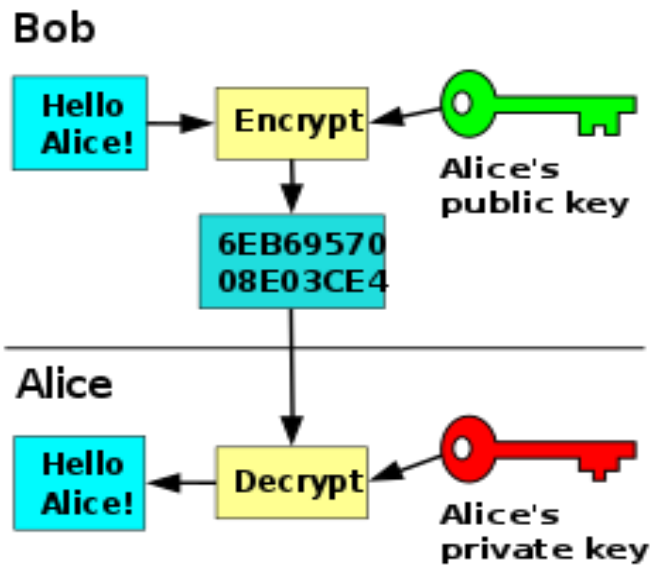
Symmetric Key cryptography:

Encryption is a process to change the form of any message in order to protect it from reading by anyone. In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.



Asymmetric Key cryptography(also called public key cryptography)

Asymmetric Key Encryption is based on public and private key encryption technique. It uses two different key to encrypt and decrypt the message. It is more secure than symmetric key encryption technique but is much slower.



DIFFERENCE BETWEEN:

SYMMETRIC KEY ENCRYPTION	ASYMMETRIC KEY ENCRYPTION
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity and non-repudiation.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

DIGITAL SIGNATURES:

A digital signature is a cryptographic mechanism used to verify the authenticity and integrity of digital data. We may consider it as a digital version of the ordinary handwritten signatures, but with higher levels of complexity and security.In simple terms, we may describe a digital signature as a code that is attached to a message or document. After generated, the code acts as proof that the message hasn't been tampered with along its way from sender to receiver.

digital signature generated in 2 steps:

1. A message digest is generated.A message is a summary of the message we are going to transmit and it has 2 properties(a)it is always smaller than the message itself (b)even the slightest change in the message produces different digest.The message digest is produced using hashing algorithm.

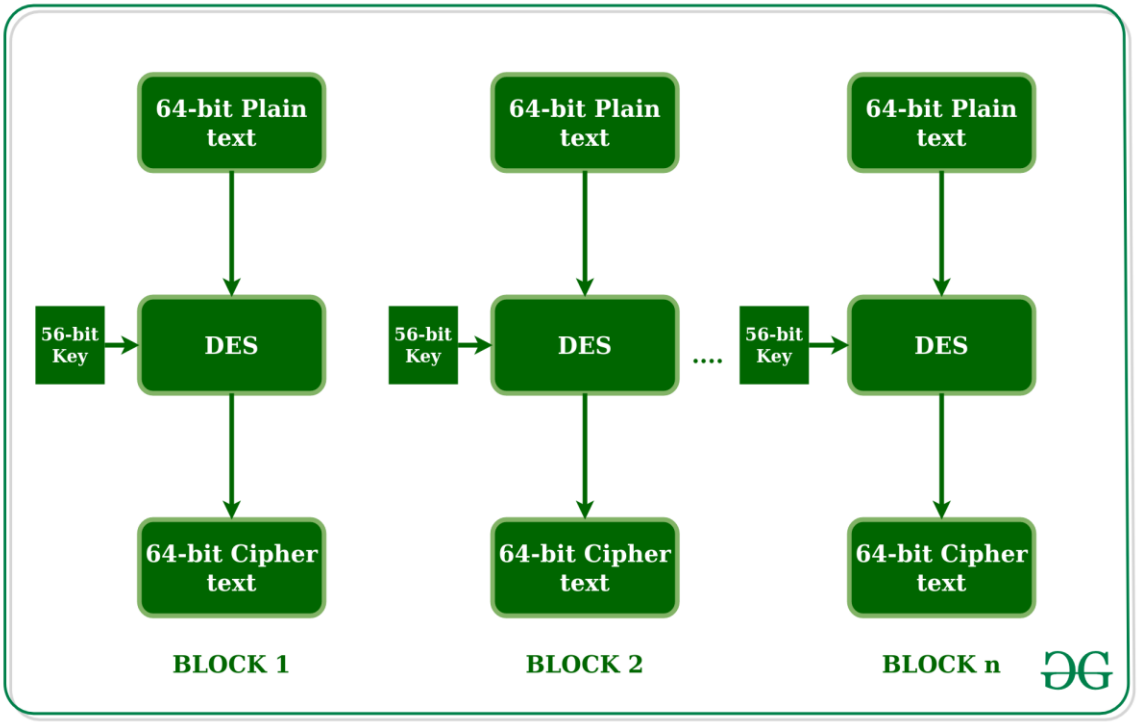
2. The message digest is encrypted using the sender's private key.

The resulting encrypted message digest is the digital signature.

CRYPTOGRAPHY ALGORITHMS:

Data encryption standard (DES)

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline.
DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The basic idea is show in figure.



DES is based on the two fundamental attributes of cryptography: substitution (also called as confusion) and transposition (also called as diffusion). DES consists of 16 steps, each of which is called as a round. Each round performs the steps of substitution and transposition.

RSA Algorithm

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown −

N=p*q

Here, let N be the specified large number.

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1

Step 3: Public key

The specified pair of numbers **n** and **e** forms the RSA public key and it is made public.

Step 4: Private Key

Private Key **d** is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows –

$ed = 1 \bmod (p-1)(q-1)$

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is **(n,e).** To encrypt the plain text message in the given scenario, use the following syntax –

$C = P^e \bmod n$

Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver **C** has the private key **d**, the result modulus will be calculated as –

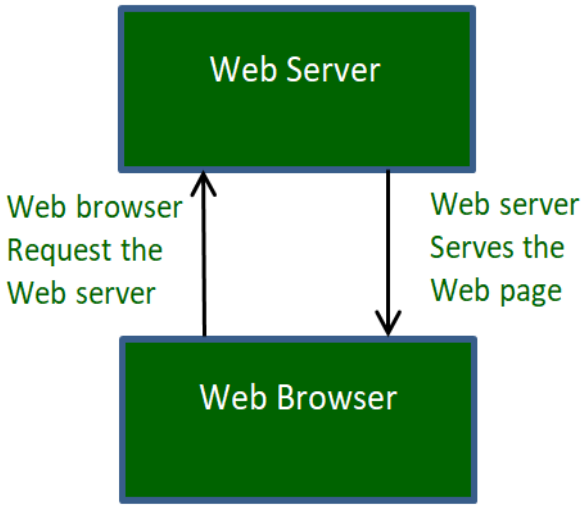
$Plaintext = C^d \bmod n$

WEB SERVER

Web servers are computers that deliver (*serves up*) Web pages. Every Web server has an IP address and possibly a domain name. For example, if you enter the URL *www.google.com* in your browser, this sends a request to the Web server whose domain name is *google.com*. The server then fetches the page named and sends it to your browser.Any computer can be turned into a Web server by installing server software and connecting the machine to the Internet.
Web Servers are basically simple computer programs that dispense the web page when they are requested using the web client. The machines on which this program run are usually called as a server, with both the names web server and server almost used interchangeably.

How Web servers work?

A page on internet can be viewed, when the browser requests it from the web server and the web server responds with that page. A simple diagrammatic representation of this is as given below in the figure:



Simple process consists of 4 steps, they are:

1. **Obtaining the IP Address from domain name:** Our web browser first obtains the IP address the domain name (for e.g., for this page the domain name is www.webbs.org) resolves to. **Note:** Any website is assigned an IP address when it is first created on web server.
2. **Browser requests the full URL** : After knowing the IP Address, the browser now demands a full URL from the web server.
3. **Web server responds to request:** The web server responds to the browser by sending the desired pages, and in case, the pages do not exist or some other error occurs, it will send the appropriate error message.
   For example:
   You may have seen **Error 404**, while trying to open a webpage, which is the message sent by the server when the page does not exist.
   Another common one is **Error 401** when access is denied to us due to incorrect credentials, like username or password, provided by us.
4. **Browser displays the web page:** The Browser finally gets the webpages and displays it, or displays the error message.

DHCP AND DHCP SERVER

DHCP is an abbreviation for Dynamic Host Configuration Protocol. It is an application layer protocol used by hosts for obtaining network setup information. The DHCP is controlled by DHCP server that **dynamically distributes** network configuration parameters such as IP addresses, subnet mask and gateway address.

What is Dynamic host configuration protocol?

- Dynamic – Automatically
- Host – Any computer that is connected to the network
- Configuration – To configure a host means to provide network information(ip address,subnet mask,Gateway address) to a host
- Protocol – Set of rules

Summing up, a DHCP server dynamically configures a host in a network.

Disadvantage of manually Configuring the host: Configuring a host when it is connected to the network can be done either manually i.e., by the network administrator or by the DHCP server. In case of home networks, manual configuration is quite easy. Whereas in the large networks, the network administrator might face many problems.
Also, the manual configuration is prone to mistakes. Say a Network administrator might assign an IP address which was already assigned. Thus, causing difficulty for both administrator as well as neighbors on network.
So, here comes the use of DHCP server. Before discussing about how DHCP server works, lets go through the DHCP entities.

Configuring a host using DHCP

To configure a host, we require the following things:

- **Leased IP address** – IP address to a host which lasts for a particular duration which goes for a few hours,few days or few weeks.
- **Subnet Mask** – The host can know on which network it is on.
- **Gateway address** – The Gateway is the Internet Service Provider that connects user to the internet.The Gateway address lets the host know where the gateway is to connect to the internet.

DHCP Entities

- **DHCP server:** It automatically provides network information(IPaddress, subnet mask, gateway address) on lease. Once the duration is expired, that network information can be assigned to other machine. It also maintains the data storage which stores the available IP addresses.
- **DHCP client:** Any node which request an IP address allocation to a network is considered as DHCP client.
- **DHCP Relay Agent:** In case, we have only one DHCP server for multiple LAN's then this Agent which presents in every network forwards the DHCP request to DHCP server. So, using DHCP Relay Agent we can configure multiple LAN's with single server.

How DHCP server assigns IP address to a host?

1. **DHCPDISCOVER:** When a new node is connected to the network, it broadcasts the DHCPDISCOVER message which contains the source address as 0.0.0.0 to every node on the network including server. DHCP server on receiving the message, returns the DHCPOFFER message to the requested host which contains the server address and new IP address to the node.
2. **DHCPOFFER:** If there are multiple servers on the network, host receives multiple DHCPOFFER messages. It is up to the host to select a particular message.
3. **DHCPREQUEST:** The requested host on receiving the offer message, it again broadcasts the DHCPREQUEST message on the network with the address of the server whose offer message is accepted by the host. The server which pertains to that server address sent by the host checks whether the address to be assigned to the node is available in the data storage.
4. **DHCPACK :** If the address is assigned , it marks the IP address in the storage as unavailable to ensure consistency. Now, the server sends DHCPACK packet to the

requested host which contains network information(IP address, subnet mask, gateway address). In case, if the address is assigned to other machine meanwhile, then the server sends the packet DHCPNAK to the requested host indicating that the IP address is assigned to some other machine.

5. **DHCPRELEASE :** And finally, If the host wants to move to other network or if it has finished its work, it sends the DHCPRELEASE packet to the server indicating that it wants to disconnect. Then the server marks the IP address as available in the storage so that it can be assigned to other machine.

TROUBLE SHOOTING IN NETWORKING TOOLS

1. Ping(Packet Internet Groper)

ping command is used to ensure that a computer can communicate to a specified device over the network. ping command sends Internet Control Message Protocol(ICMP) Echo Request messages in the form of packets to the destination computer and waits in order to get the response back. Once the packets are received by the destined computer, it starts sending the packets back. This command keeps executing until it *si* interrupted. ping command provides details such as

- number of packets transmitted
- number of packets received
- time taken by the packet to return

ping command in generally used for the following purposes:

- measuring the time taken by the packets to return to determine speed of the connection
- to make sure that the network connection between host and the destined computer can be established

2. Tracert / traceroute

Tracert: Determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the router that is closest to the sending host in the path.

This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it.

To trace the path to the host named www.google.co.in use following command

tracert www.google.co.in

3. **ipconfig**
   Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

4. **nslookup**
   nslookup command queries the DNS in order to fetch the IP address or the domain name from DNS records.
5. **Netstat:**
   Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols).

Netstat provides statistics for the following:

- Proto - The name of the protocol (TCP or UDP).
- Local Address - The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).
- Foreign Address - The IP address and port number of the remote computer to which the socket is connected. The names that corresponds to the IP address and the port are shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).

6. **pathping**

This network utility is a more advanced version of the Ping tool, which performs a ping to each hop along the route to the destination (unlike Ping, which just pings from the originating device to the destination device). It is extremely useful in diagnosing packet loss, and can help with diagnosing slow speed faults.

Nmap

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

RELATED: Best VPN routers for small business

Nmap can be used to monitor single hosts as well as vast networks that encompass hundreds of thousands of devices and multitudes of subnets.

Though Nmap has evolved over the years and is extremely flexible, at heart it's a port-scan tool, gathering information by sending raw packets to system ports. It listens for responses and determines whether ports are open, closed or filtered in some way by,

for example, a firewall. Other terms used for port scanning include port discovery or enumeration.

Tcpdump

Tcpdump is a command line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool
.A powerful and versatile tool that includes many options and filters, tcpdump can be used in a variety of cases. Since it's a command line tool, it is ideal to run in remote servers or devices for which a GUI is not available, to collect data that can be analyzed later.