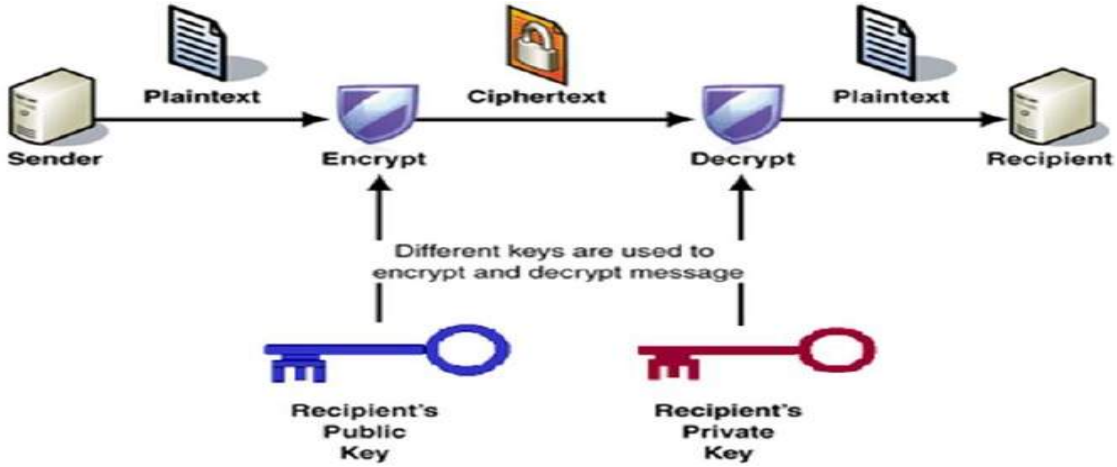
UNIT-4

Public Key Cryptography

- Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.
- Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.
- With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.
- The process of encryption and decryption is depicted in the following illustration –



- The most important properties of public key encryption scheme are −
- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- Each receiver possesses a unique decryption key, generally referred to as his private key.
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the cipher text and the encryption (public) key.

- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys**.**

RSA Cryptosystem

- This cryptosystem is one the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars Ron Rivest, Adi Shamir, and Len Adleman and hence, it is termed as RSA cryptosystem.
- We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.
- Generation of RSA Key Pair
- Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below −
- Generate the RSA modulus (n)
  - Select two large primes, p and q.
  - Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.
  - **Find Derived Number (e)**
  - Number **e** must be greater than 1 and less than (p − 1)(q − 1).
  - There must be no common factor for e and (p − 1)(q − 1) except for 1. In other words two numbers e and (p – 1)(q – 1) are coprime.
  - **Form the public key**
  - The pair of numbers (n, e) form the RSA public key and is made public.
  - Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA

    Generate the private key
  - Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
  - Number d is the inverse of e modulo (p - 1)(q – 1). This means that d is the number less than (p - 1)(q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1)(q - 1).
  - This relationship is written mathematically as follows −

– ed = 1 mod (p − 1)(q − 1)

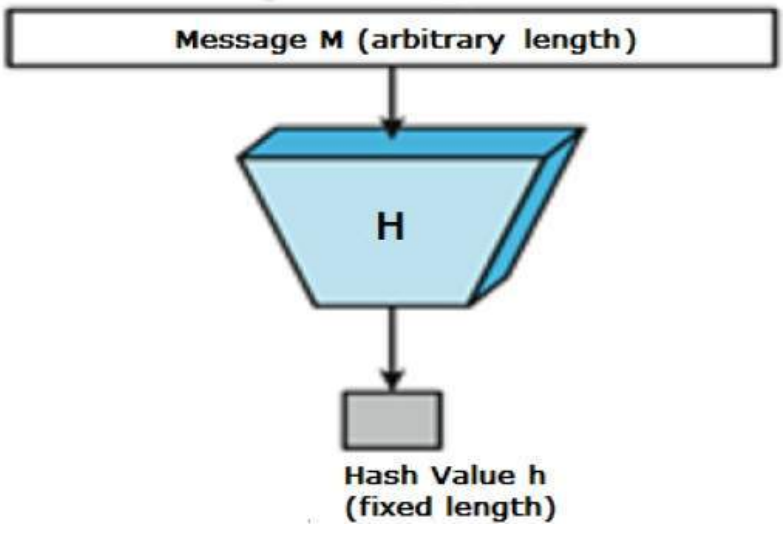
EXAMPLE:

- An example of generating RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are very high).
- Let two primes be p = 7 and q = 13. Thus, modulus n = pq = 7 x 13 = 91.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and (p − 1)(q − 1) = 6 × 12 = 72, except for 1.
- The pair of numbers (n, e) = (91, 5) forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
- Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output will be d = 29.
- Check that the d calculated is correct by computing −
- De=29x5=145=1 mod 72

Hence, public key is (91, 5) and private keys is (91, 29).

Cryptography Hash functions

- Hash functions are extremely useful and appear in almost all information security applications.
- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.
- Values returned by a hash function are called message digest or simply hash values. The following picture illustrated hash function –



Features of Hash Functions

- The typical features of hash functions are −
- **Fixed Length Output (Hash Value)**
  - Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data**.
  - In general, the hash is much smaller than the input data, hence hash functions are sometimes called **compression functions**.
  - Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.
  - Hash function with n bit output is referred to as an **n-bit hash function**. Popular hash functions generate values between 160 and 512 bits.
- **Efficiency of Operation**
  - Generally, for any hash function h with input x, computation of h(x) is a fast operation.
  - Computationally hash functions are much faster than a symmetric encryption.

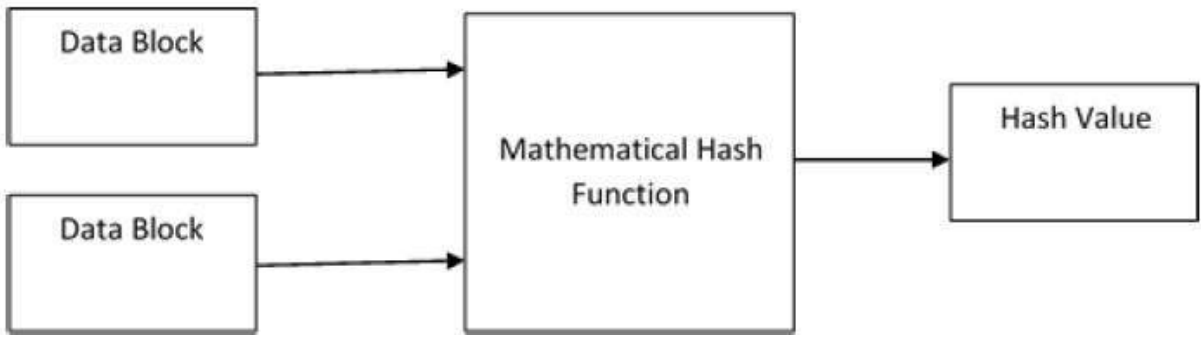
Properties of Hash Functions

- In order to be an effective cryptographic tool, the hash function is desired to possess following properties −
- **Pre-Image Resistance**
  - This property means that it should be computationally hard to reverse a hash function.
  - In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
  - This property protects against an attacker who only has a hash value and is trying to find the input.
- **Second Pre-Image Resistance**
  - This property means given an input and its hash, it should be hard to find a different input with the same hash.
  - In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).
  - This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.

- **Collision Resistance**
- This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.
- In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).
- Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find.
- This property makes it very difficult for an attacker to find two input values with the same hash.
- Also, if a hash function is collision-resistant **then it is second pre-image resistant.**

Design of Hashing Algorithms

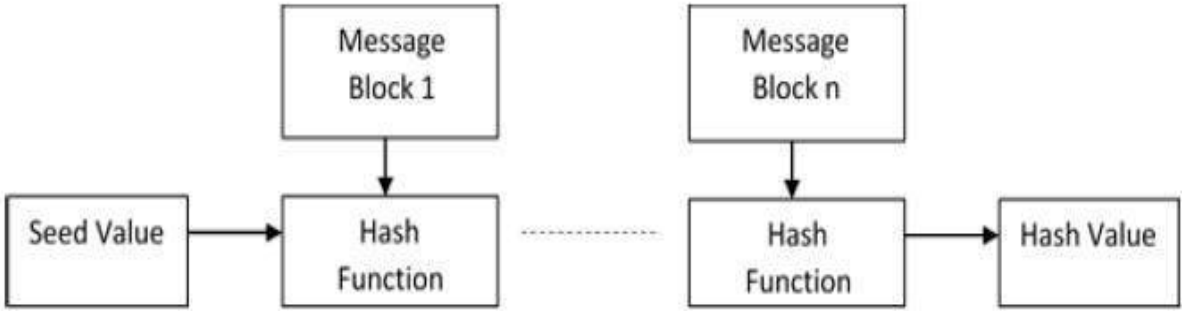
- The heart of a hashing is a mathematical function that operates on two fixed-size blocks of data to create a hash code. This hash function forms the part of the hashing algorithm.
- The size of each data block varies depending on the algorithm. Typically the block sizes are from 128 bits to 512 bits. The following illustration demonstrates hash function −
- Hashing algorithm involves rounds of above hash function like a block cipher. Each round takes an input of a fixed size, typically a combination of the most recent message block and the output of the last round.



Design of Hashing Algorithms

- This process is repeated for as many rounds as are required to hash the entire message. Schematic of hashing algorithm is depicted in the following illustration
- Since, the hash value of first message block becomes an input to the second hash operation, output of which alters the result of the third operation, and so on. This effect, known as an **avalanche** effect of hashing.

- Avalanche effect results in substantially different hash values for two messages that differ by even a single bit of data.



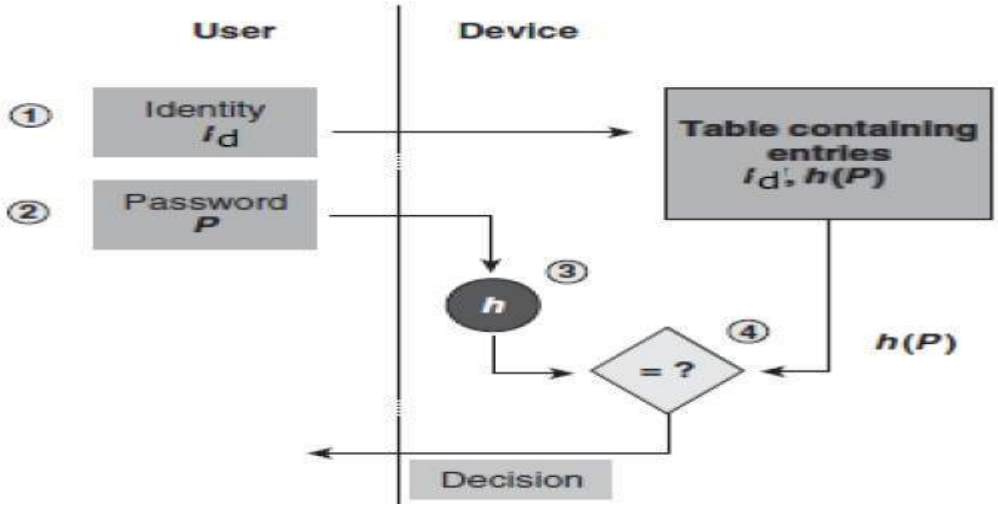
- Understand the difference between hash function and algorithm correctly. The hash function generates a hash code by operating on two blocks of fixed-length binary data.
- Hashing algorithm is a process for using the hash function, specifying how the message will be broken up and how the results from previous message blocks are chained together.

Applications of Hash Functions

There are two direct applications of hash function based on its cryptographic properties.

Password Storage

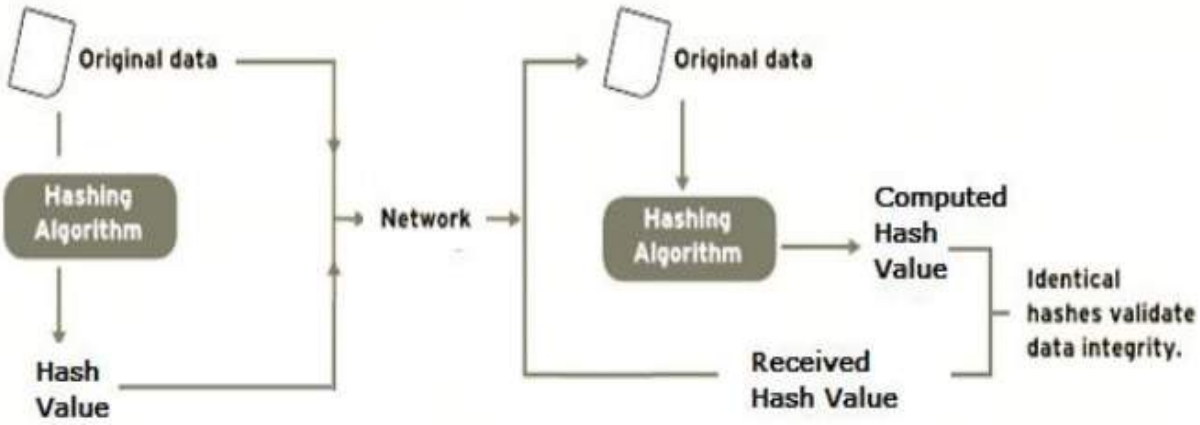
- Hash functions provide protection to password storage.
- Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.
- The Password file consists of a table of pairs which are in the form (user id, h(P)).
- The process of logon is depicted in the following illustration –



- An intruder can only see the hashes of passwords, even if he accessed the password. He can neither logon using hash nor can he derive the password from hash value since hash function possesses the property of pre-image resistance.

Data Integrity Check

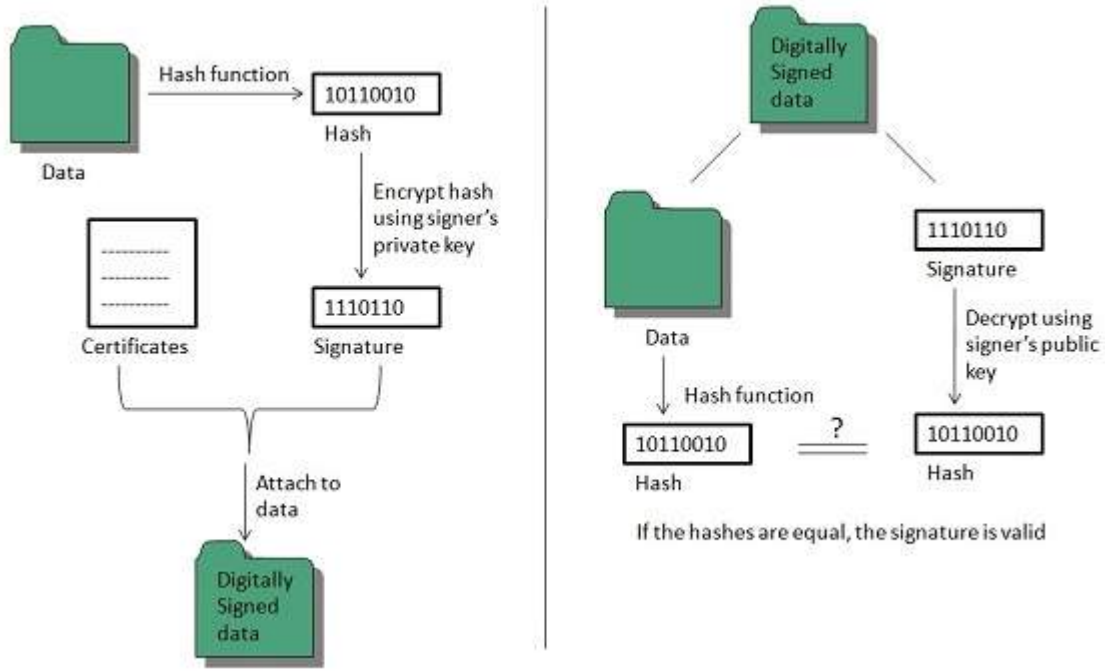
- Data integrity check is a most common application of the hash functions. It is used to generate the checksums on data files. This application provides assurance to the user about correctness of the data.
- The process is depicted in the following illustration –



- The integrity check helps the user to detect any changes made to original file. It however, does not provide any assurance about originality. The attacker, instead of modifying file data, can change the entire file and compute all together new hash and send to the receiver. This integrity check application is useful only if the user is sure about the originality of file.

Digital Signature

- Digital signatures allow us to verify the author, date and time of signatures, authenticate the message contents. It also includes authentication function for additional capabilities.



- There are several reasons to implement digital signatures to communications:

Authentication

- Digital signatures help to authenticate the sources of messages. For example, if a bank's branch office sends a message to central office, requesting for change in balance of an account. If the central office could not authenticate that message is sent from an authorized source, acting of such request could be a grave mistake.

Integrity

- Once the message is signed, any change in the message would invalidate the signature.

Non-repudiation

- By this property, any entity that has signed some information cannot at a later time deny having signed it.

Public Key Infrastructure

PKI provides assurance of public key. It provides the identification of public keys and their distribution. An anatomy of PKI comprises of the following components.

- Public Key Certificate, commonly referred to as 'digital certificate'.
- Private Key tokens.
- Certification Authority.
- Registration Authority.

- Certificate Management System.

1.Digital Certificate

- For analogy, a certificate can be considered as the ID card issued to the person. People use ID cards such as a driver's license, passport to prove their identity. A digital certificate does the same basic thing in the electronic world, but with one difference.
- Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world.
- Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.
- Public key pertaining to the user client is stored in digital certificates by The Certification Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.
- CA digitally signs this entire information and includes digital signature in the certificate.
- Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA's public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.

2.Certifying Authority (CA)

- Key Functions of CA
- The key functions of a CA are as follows −
- **Generating key pairs** − The CA may generate a key pair independently or jointly with the client.
- **Issuing digital certificates** − The CA could be thought of as the PKI equivalent of a passport agency − the CA issues a certificate after client provides the credentials to confirm his identity. The CA then signs the certificate to prevent modification of the details contained in the certificate.
- **Publishing Certificates** − The CA need to publish certificates so that users can find them. There are two ways of achieving this. One is to publish certificates in the equivalent of an electronic telephone directory. The other is to send your certificate out to those people you think might need it by one means or another.
- **Verifying Certificates** − The CA makes its public key available in environment to assist verification of his signature on clients' digital certificate.

- **Revocation of Certificates** − At times, CA revokes the certificate issued due to some reason such as compromise of private key by user or loss of trust in the client. After revocation, CA maintains the list of all revoked certificate that is available to the environment.

3.Classes of Certificates

- There are four typical classes of certificate −
- **Class 1** − These certificates can be easily acquired by supplying an email address.
- **Class 2** − These certificates require additional personal information to be supplied.
- **Class 3** − These certificates can only be purchased after checks have been made about the requestor's identity.
- **Class 4** − They may be used by governments and financial organizations needing very high levels of trust.

4.Registration Authority (RA)

- CA may use a third-party Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to confirm their identity. The RA may appear to the client as a CA, but they do not actually sign the certificate that is issued.

5.Certificate Management System (CMS)

- It is the management system through which certificates are published, temporarily or permanently suspended, renewed, or revoked. Certificate management systems do not normally delete certificates because it may be necessary to prove their status at a point in time, perhaps for legal reasons. A CA along with associated RA runs certificate management systems to be able to track their responsibilities and liabilities.

6.Private Key Tokens

- While the public key of a client is stored on the certificate, the associated secret private key can be stored on the key owner's computer. This method is generally not adopted. If an attacker gains access to the computer, he can easily gain access to private key. For this reason, a private key is stored on secure removable storage token access to which is protected through a password.

E-mail Security

- Email hacking can be done in any of the following ways:
- Spam
- Virus
- Phishing

1.Spam

- E-mail spamming is an act of sending **Unsolicited Bulk E-mails (UBI)** which one has not asked for. Email spams are the junk mails sent by commercial companies as an advertisement of their products and services.

2.Virus

- Some emails may incorporate with files containing malicious script which when run on your computer may lead to destroy your important data.

3.Phishing

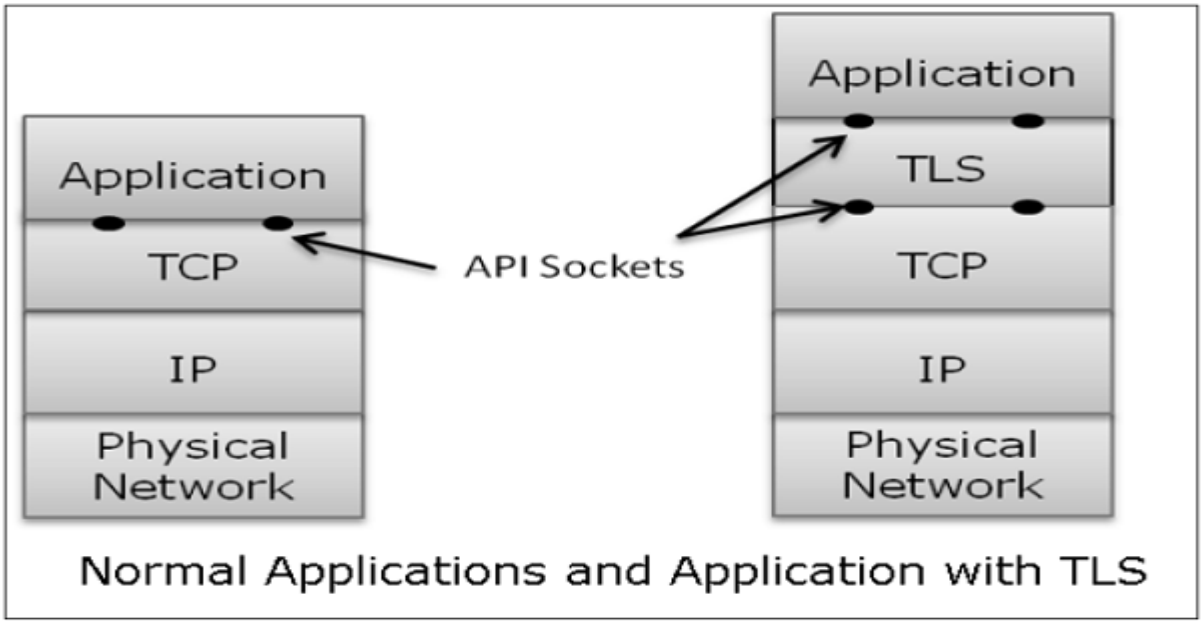
- Email phishing is an activity of sending emails to a user claiming to be a legitimate enterprise. Its main purpose is to steal sensitive information such as usernames, passwords, and credit card details.
- Such emails contain link to websites that are infected with malware and direct the user to enter details at a fake website whose look and feels are same to legitimate one.
- E-mail Spamming and Junk Mails
- Email spamming is an act of sending Unsolicited Bulk E-mails (UBI) which one has not asked for. Email spams are the junk mails sent by commercial companies as an advertisement of their products and services.
- Spams may cause the following problems:
- It floods your e-mail account with unwanted e-mails, which may result in loss of important e-mails if inbox is full.
- Time and energy is wasted in reviewing and deleting junk emails or spams.
- It consumes the bandwidth that slows the speed with which mails are delivered.
- Some unsolicited email may contain virus that can cause harm to your computer

Transport Layer security (TLS)

Let's discuss a typical Internet-based business transaction.

- Bob visits Alice’s website for selling goods. In a form on the website, Bob enters the type of good and quantity desired, his address and payment card details. Bob clicks on Submit and waits for delivery of goods with debit of price amount from his account. All this sounds good, but in absence of network security, Bob could be in for a few surprises.
- If transactions did not use confidentiality (encryption), an attacker could obtain his payment card information. The attacker can then make purchases at Bob's expense.
- If no data integrity measure is used, an attacker could modify Bob's order in terms of type or quantity of goods.

- Lastly, if no server authentication is used, a server could display Alice's famous logo but the site could be a malicious site maintained by an attacker, who is masquerading as Alice. After receiving Bob's order, he could take Bob's money and flee. Or he could carry out an identity theft by collecting Bob's name and credit card details.
- Transport layer security schemes can address these problems by enhancing TCP/IP based network communication with confidentiality, data integrity, server authentication, and client authentication.
- The security at this layer is mostly used to secure HTTP based web transactions on a network. However, it can be employed by any application running over TCP.
- Philosophy of TLS Design
- Transport Layer Security (TLS) protocols operate above the TCP layer. Design of these protocols use popular Application Program Interfaces (API) to TCP, called “sockets" for interfacing with TCP layer.
- Applications are now interfaced to Transport Security Layer instead of TCP directly. Transport Security Layer provides a simple API with sockets, which is similar and analogous to TCP's API.
- In the above diagram, although TLS technically resides between application and transport layer, from the common perspective it is a transport protocol that acts as TCP layer enhanced with security services.
- TLS is designed to operate over TCP, the reliable layer 4 protocol (not on UDP protocol), to make design of TLS much simpler, because it doesn't have to worry about ‘timing out’ and ‘retransmitting lost data’. The TCP layer continues doing that as usual which serves the need of TLS.



IP security (IPSec)

- The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.
- **Uses of IP Security –**
  IPsec can be used to do the following things:
- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security –
It has the following components:

- **Encapsulating Security Payload (ESP) –**
  It provides data integrity, encryption, authentication and anti-replay. It also provides authentication for payload.
- **Authentication Header (AH) –**
  It also provides data integrity, authentication and anti-replay and it does not provide encryption. The anti-replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.
  Internet Key Exchange (IKE) –
  It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

DNS security

- **Domain Name System** helps to resolve the host name to an address. It uses a hierarchical naming scheme and distributed database of IP addresses and associated names

  IP Address

- IP address is a unique logical address assigned to a machine over the network. An IP address exhibits the following properties:
- IP address is the unique address assigned to each host present on Internet.
- IP address is 32 bits (4 bytes) long.
- IP address consists of two components: **network component** and **host component**.
- Each of the 4 bytes is represented by a number from 0 to 255, separated with dots. For example, 137.170.4.124
- The Domain name system comprises of **Domain Names, Domain Name Space, Name Server** that have been described below:
- Domain Names
- Domain Name is a symbolic string associated with an IP address. There are several domain names available; some of them are generic such as **com, edu, gov, net** etc, while some country level domain names such as **au, in, za, us** etc.

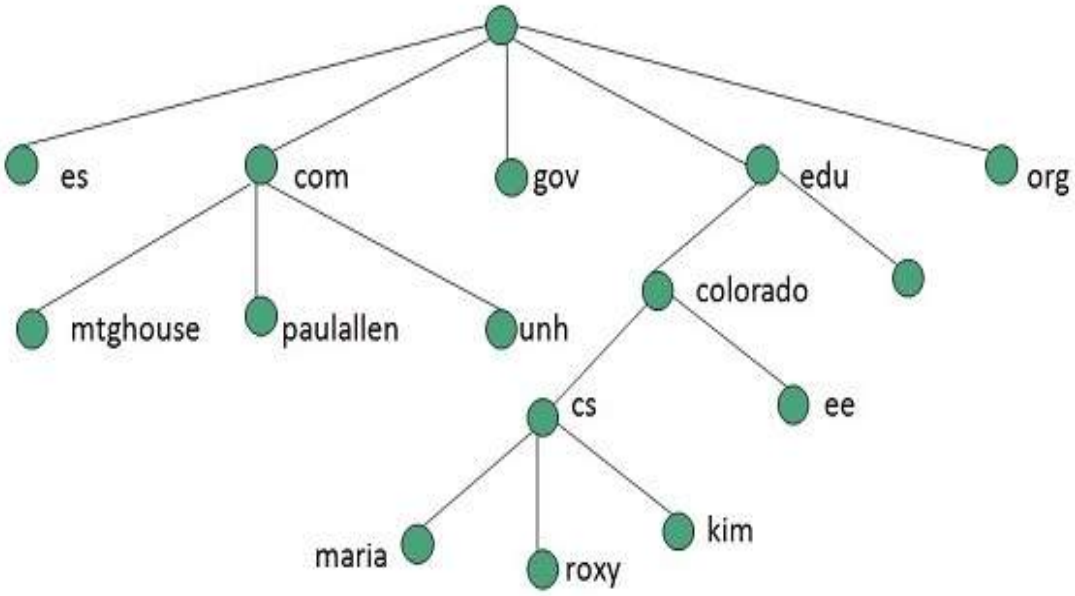
Domain Name	Meaning
Com	Commercial business
Edu	Education
Gov	U.S. government agency
Int	International entity
Mil	U.S. military
Net	Networking organization
Org	Non profit organization

Domain Name	Meaning
Au	Australia

In	India
Cl	Chile
Fr	France
Us	United States
Za	South Africa
Uk	United Kingdom
Jp	Japan
Es	Spain
De	Germany
Ca	Canada
Ee	Estonia
Hk	Hong Kong

Domain Name Space

- The domain name space refers a hierarchy in the internet naming structure. This hierarchy has multiple levels (from 0 to 127), with a root at the top. The following diagram shows the domain name space hierarchy:



DNS Working

- DNS translates the domain name into IP address automatically. Following steps will take you through the steps included in domain resolution process:
- When we type **www.abcd.com** into the browser, it asks the local DNS Server for its IP address.
- When the local DNS does not find the IP address of requested domain name, it forwards the request to the root DNS server and again enquires about IP address of it.
- The root DNS server replies with delegation that **I do not know the IP address of www.abcd.com but know the IP address of DNS Server.**
- The local DNS server then asks the com DNS Server the same question.
- The **com** DNS Server replies the same that it does not know the IP address of www.abcd.com but knows the address of abcd.com.
- Then the local DNS asks the abcd.com DNS server the same question.
- Then abcd.com DNS server replies with IP address of www.abcd.com.
- Now, the local DNS sends the IP address of www.abcd.com to the computer that sends the request.

Real world protocol

1. Secure Socket Layer (SSL)

- **Secure Socket Layer (SSL)** provide security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser

which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

Silent Features of Secure Socket Layer:

- Advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is two-layered protocol.

2.Internet key exchange:

- Internet Key Exchange (IKE) is the protocol used to set up a secure, authenticated communications channel between two parties. IKE typically uses X.509 PKI certificates for authentication and the Diffie–Hellman key exchange protocol to set up a shared session secret.
- IKE is part of the Internet Security Protocol (IPSec) which is responsible for negotiating security associations (SAs), which are a set of mutually agreed-upon keys and algorithms to be used by both parties trying to establish a VPN connection/tunnel.

  IKE is a hybrid protocol based on:

- ISAKMP (RFC2408): Internet Security Association and Key Management Protocols are used for negotiation and establishment of security associations. This protocol establishes a secure connection between two IPSec peers.
- Oakley (RFC2412): This protocol is used for key agreement or key exchange. Oakley defines the mechanism that is used for key exchange over an IKE session. The default algorithm for key exchange used by this protocol is the Diffie-Hellman algorithm.
- SKEME: This protocol is another version for key exchange.

3.Kerberos authentication protocol:

- **Kerberos** provides a centralize authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos run as a third-party trusted

server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.

The main components of Kerberos are:

- **Authentication Server (AS):**
  The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.
- **Database:**
  The Authentication Server verifies access rightd of users in database.
- **Ticket Granting Server (TGS):**
  The Ticket Granting Server issues the ticket for the Server

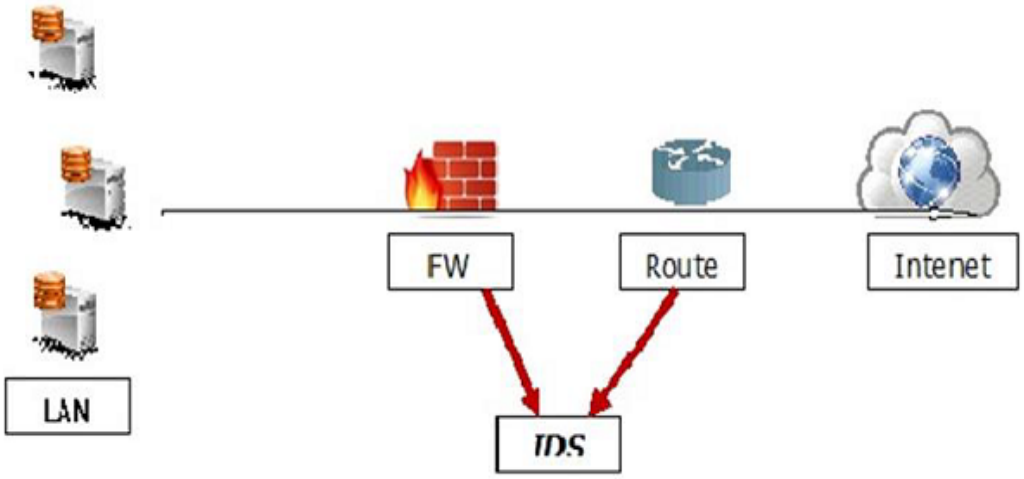
4.Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Service Layer (SSL). TLS ensures that no third party may eavdrops or tamper with any message.

There are several benefits of TLS:

- **Encryption:**
  TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:**
  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:**
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:**
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:**
  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

Intrusion Detection Systems

- Intrusion Detection Systems are also as important as the firewall because they help us to detect the type of attack that is being done to our system and then to make a solution to block them. The monitoring part like tracing logs, looking for doubtful signatures and keeping history of the events triggered. They help also the network administrators to check the connection integrity and authenticity that occur.
- Let us see the schema of their positions −



Intrusion Detection Tools

Intrusion Detection Tools

- One of the best intrusion detection tool is **Snort**.
- It is software based, but is an open source so it is free and easy to configure. It has a real time signature based network – IDS, which notifies the system administrators or attacks like port scanners, DDOS attacks, CGI attacks, backdoors, OS finger printing.

The other IDS are −

- BlackICE Defender
- CyberCop Monitor
- Check point RealSecure
- Cisco Secure IDS
- Vanguard Enforcer
- Lucent RealSecure.

Firewall Security

- **Firewall** is a barrier between Local Area Network (LAN) and the Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions.
- The following diagram depicts a sample firewall between LAN and the internet. The connection between the two is the point of vulnerability. Both hardware and the software can be used at this point to filter network traffic.

Types of Firewall

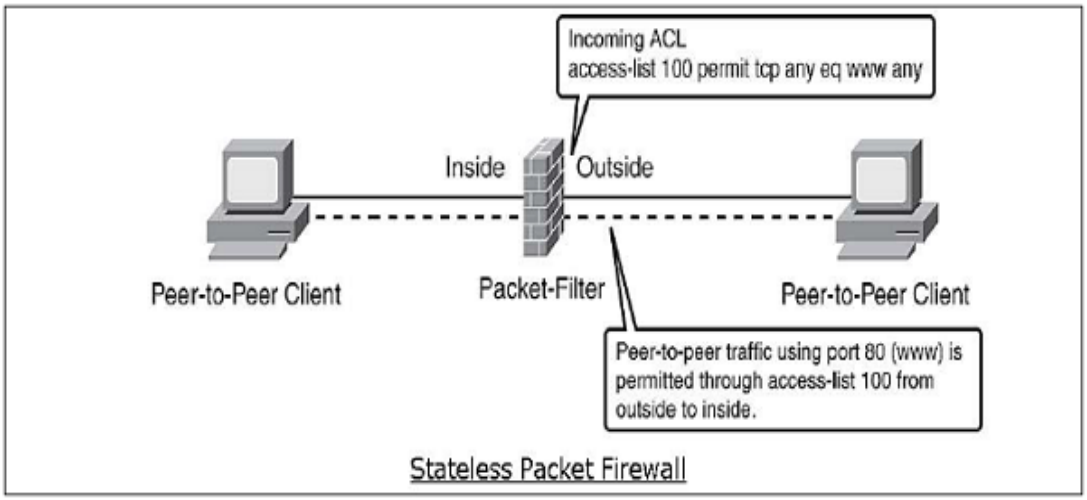
- Firewall is a network device that isolates organization's internal network from larger outside network/Internet. It can be a hardware, software, or combined system that prevents unauthorized access to or from internal network.
- All data packets entering or leaving the internal network pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.

Stateless & Stateful Packet Filtering Firewall

- In this type of firewall deployment, the internal network is connected to the external network/Internet via a router firewall. The firewall inspects and filters data packet-by-packet.
- Packet-filtering firewalls allow or block the packets mostly based on criteria such as source and/or destination IP addresses, protocol, source and/or destination port numbers, and various other parameters within the IP header.
- The decision can be based on factors other than IP header fields such as ICMP message type, TCP SYN and ACK bits, etc.

Packet filter rule has two parts –

- Selection criteria − It is a used as a condition and pattern matching for decision making.
- Action field − This part specifies action to be taken if an IP packet meets the selection criteria. The action could be either block (deny) or permit (allow) the packet across the firewall.
- Packet filtering is generally accomplished by configuring Access Control Lists (ACL) on routers or switches. ACL is a table of packet filter rules.
- As traffic enters or exits an interface, firewall applies ACLs from top to bottom to each incoming packet, finds matching criteria and either permits or denies the individual packets.
- **Stateless firewall** is a kind of a rigid tool. It looks at packet and allows it if its meets the criteria even if it is not part of any established ongoing communication.
- Hence, such firewalls are replaced by **stateful firewalls** in modern networks. This type of firewalls offer a more in-depth inspection method over the only ACL based packet inspection methods of stateless firewalls.
- Stateful firewall monitors the connection setup and teardown process to keep a check on connections at the TCP/IP level. This allows them to keep track of connections state and determine which hosts have open, authorized connections at any given point in time.



Stateless Packet Firewall