WORLD WIDE WEB (WWW)

Web was first proposed by Tim Beoness-Lee in 1989 at CERN, the European Organization for Nuclear Research,

Repository of information in which the documents called web pages, are distributed all over the world and related documents are linked together.

The linking of web pages was achieved using a concept called hypertext.

The term hypertext, coined to mean linked text documents, has been changed to hypermedia, to show that a web page can be text document an image, an audio file or a video file

Web Client (Browsers)

A variety of vendors offer commercial browsers that interpret and display a web page and all of them use nearly the same architecture

Each Browser consists of three parts a controller, client protocols and interpreters

Web Server

The web page is stored at the server. Each time a request arrives, the corresponding document is sent to the client

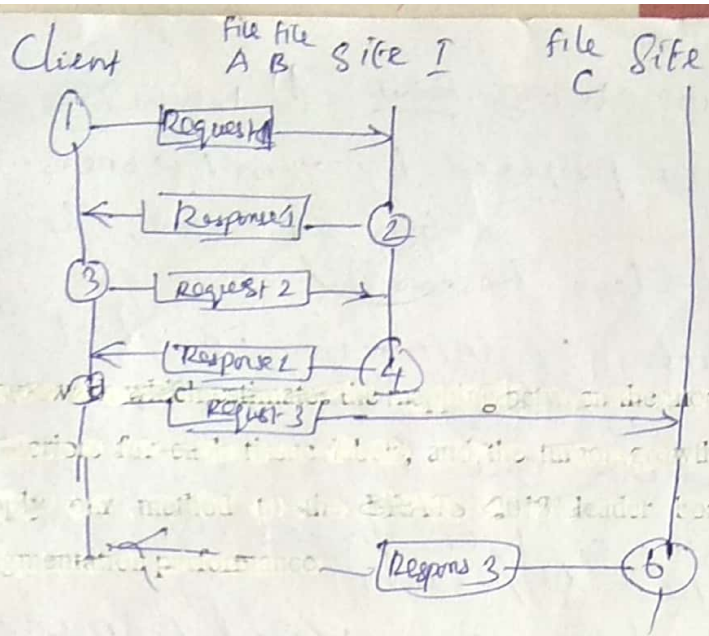
To improve efficiency; servers normally store requested files in a cache in memory, memory is faster to access than a disk.

URL (Uniform Resource Locator)

A web page, as a file needs to have a unique identifier to distinguish it from other web pages

to define a web page, three identifiers, host, port and path. before defining web page, need to browser what client server application want to use, called protocol

Means need four identifiers to define the web page.



Protocol: The first identifier is the abbreviation for the client-server program that to access the web page.

Host: The Host identifier can be IP address of the server or unique name given to server.

IP address can be defined in dotted decimal Notation (64.23.56.17). DNS (Domain Name S/m)

Port: The port, a 16 bit integer is normally predefined for the client-server application.

The well known port number 80

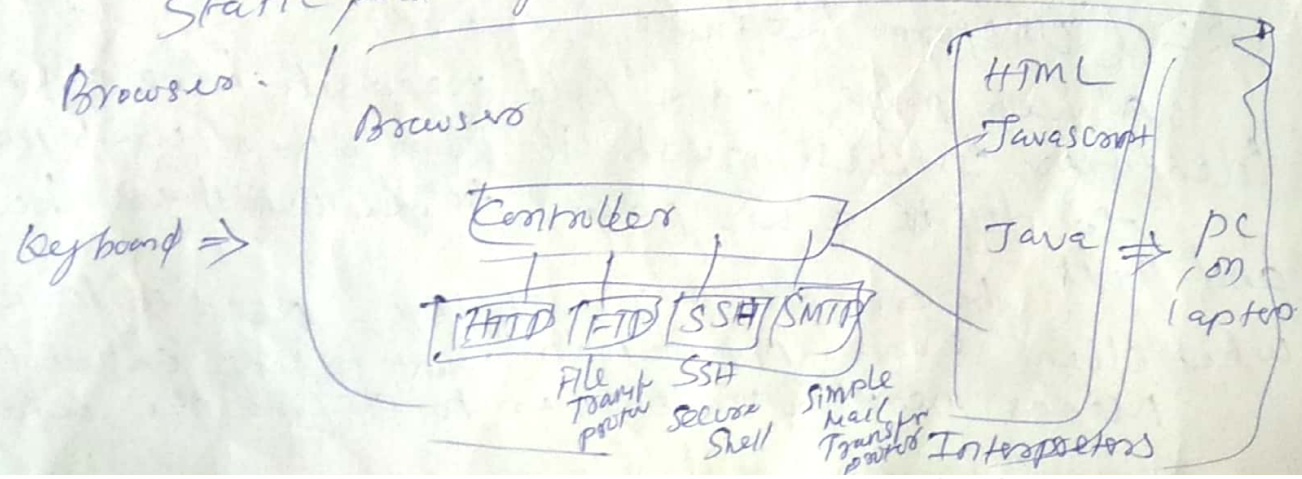
Path: The path Identifies the location and the name of the file in the underlying operating system.

UNIX.

Web documents:

Static, dynamic and Active.

Browsers.



HTTP (HYPER TEXT TRANSFER PROTOCOL):

DEFINITION:

It is a protocol used mainly to access data on the world wide web.

HTTP functions as a combination of FTP and SMTP.

HTTP uses the services of TCP on well-known port 80.

BLOCK DIAGRAM / CONCEPTS:

DIAGRAM OF HTTP TRANSACTION:

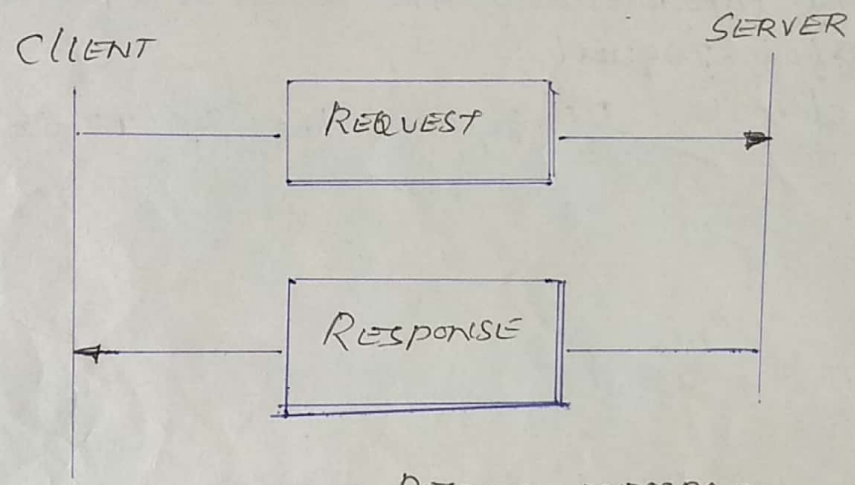
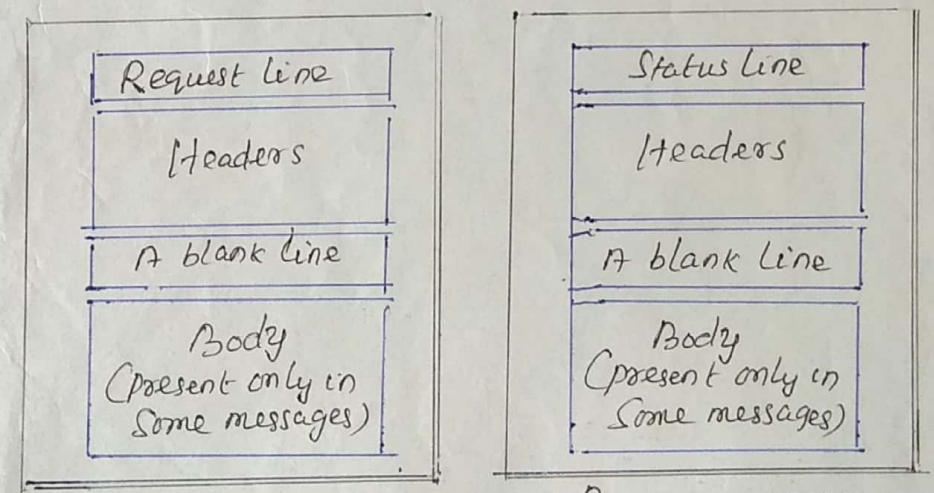


DIAGRAM OF REQUEST AND RESPONSE MESSAGES:



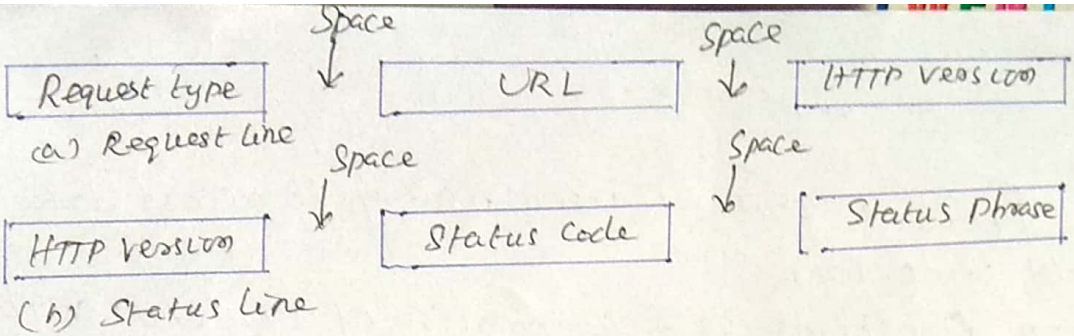
EXPLANATION:

REQUEST AND STATUS LINES:

The first line in a request message is called a request line,

The first line in the response message is called status line.

Request type: The field is used in request message. Version 1.1 of HTTP, several request types are defined.



(a) Request line

(b) Status line

Status code: The field is used in response message. Status code field is similar to FTP and SMTP protocols.

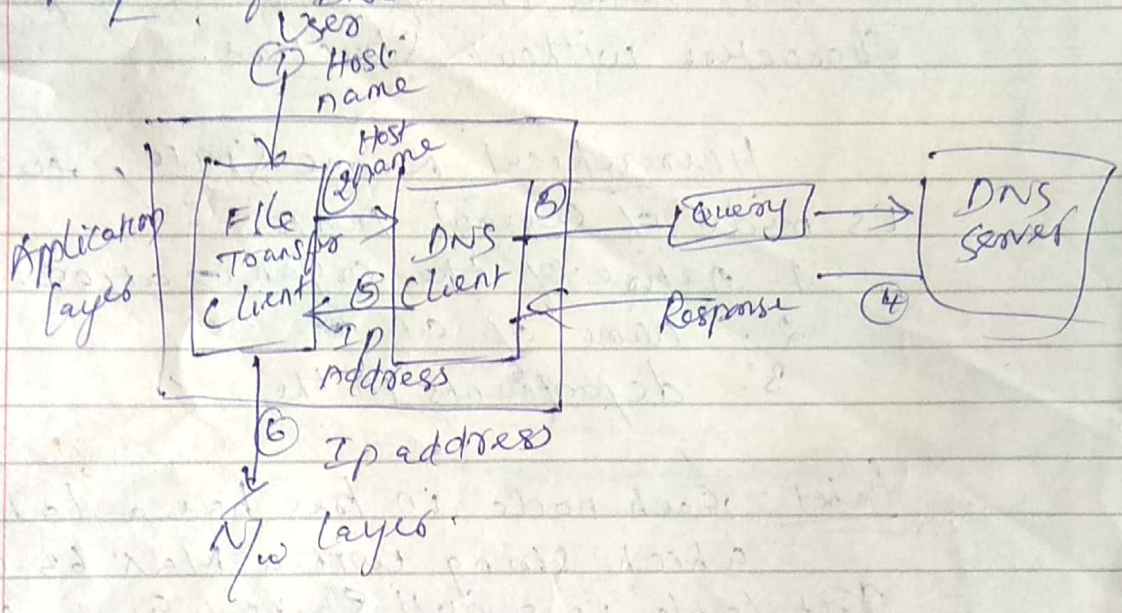
Consists of Three digits. whereas the codes in 100 range only informational, the codes in 200 range indicate a successful request.

Status Phrase. It explains the status code in text form.

DNS: (Domain Name S/m)

The host needs mapping can contact the closest computer holding the needed information. This method is used by Domain Name System.

Purpose of DNS:



Six Steps map the host name to IP address:

1. User passes the host name to the file Transfer Client
2. File Transfer Client passes the host name to the DNS Client
3. Each computer, after being booted, knows the address of one DNS server.
4. DNS server responds with the IP address of desired File Transfer server
5. DNS server passes the IP address to file transfer client
6. File transfer client now uses the Received IP address to access the file transfer server

Name Space:

A Name Space that maps each address to a unique name can be organized in two ways, flat or hierarchical.

Flat name space, name is assigned to an address. name in space is a sequence of characters without structure.

Hierarchical Name Space, each name is made of several parts.

1. nature of the organization.
2. name of an "
3. departments in the "

Label: Each node in tree has a label, which string with a Max 63 characters. Root table is a null String (Empty String)

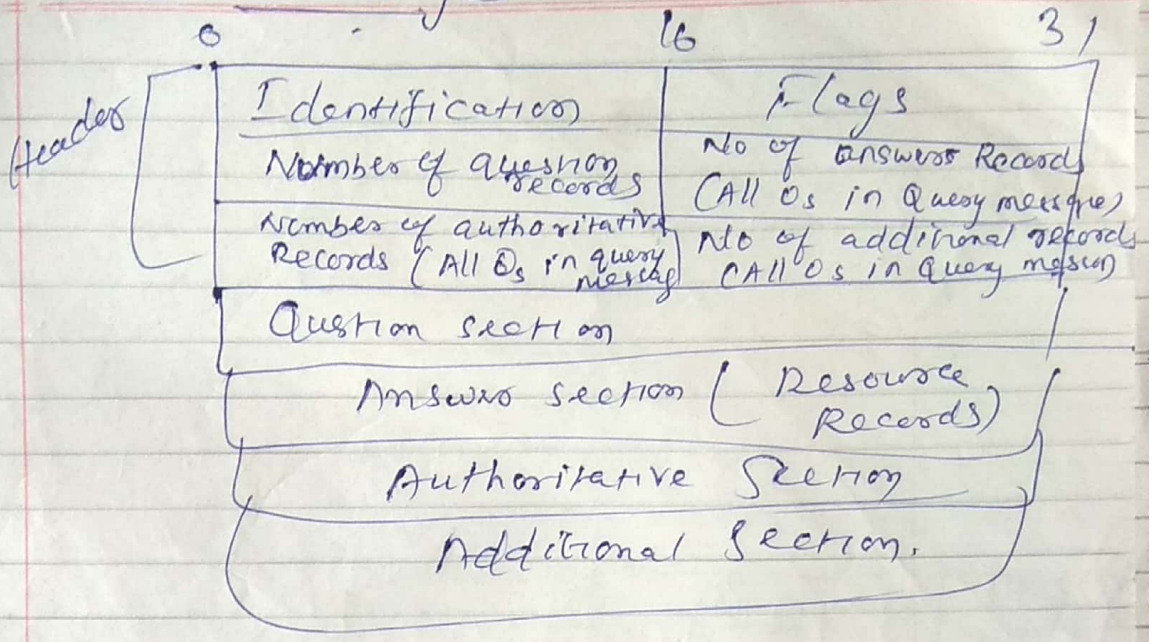
Domain Name: Each node in tree has a domain name. A full domain name is a sequence of tables separated by dots.

If a table is terminated by a null String is called Fully Qualified Domain Name (FQDN).

If a table is not terminated by a null string, is called partially Qualified Domain Name (PQDN).

Domain: A domain is a subtree of domain name space. The name of the domain is the name of node at the top of the subtree.

DNS Messages



Query Message Contains only the Question Section.

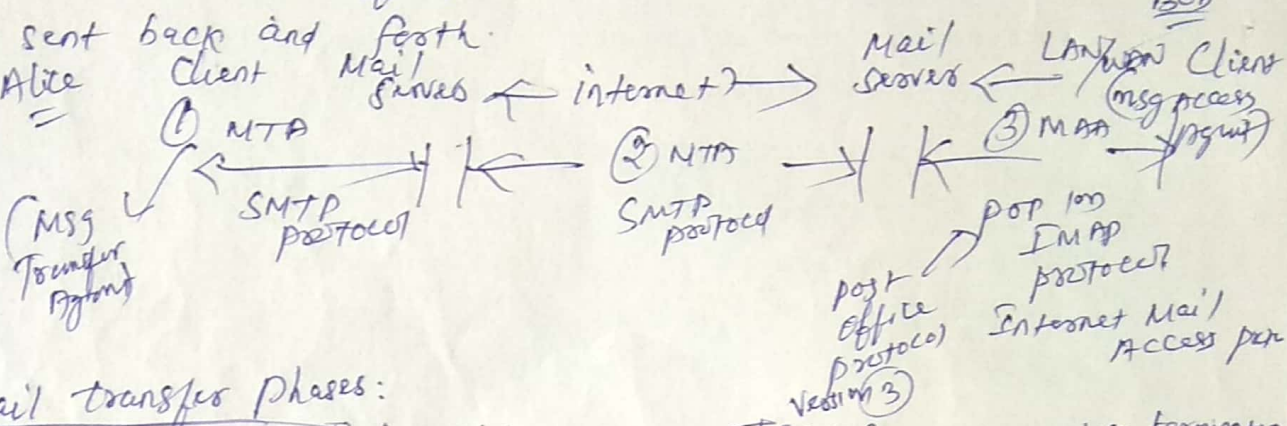
Response Message includes the Question Section, the answer Section, and possibly two other sections.

To retrieve information about hosts, DNS uses two types of messages, query and response.

SMTP (Simple Mail Transfer Protocol)

MTA client and server in internet is called SMTP. It is used two times, b/w send and sender's mail server and b/w two Mail Server.

SMTP defines how commands and responses must be sent back and forth.

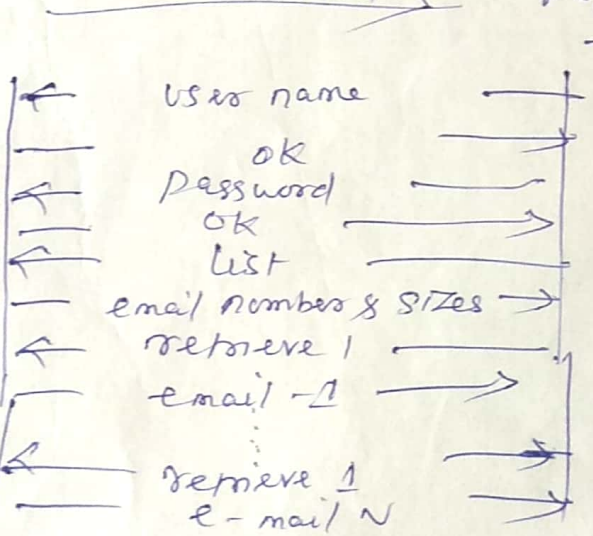


Mail transfer phases:

Connection establishment; Message Transfer, connection termination

POP3 Simple but limited in functionality. The client POP3 s/w is installed on recipient computers, the server pop3 s/w is installed on the mail server.

Mail access starts with client when the users needs to download its e-mail from the mailbox on the mail server.

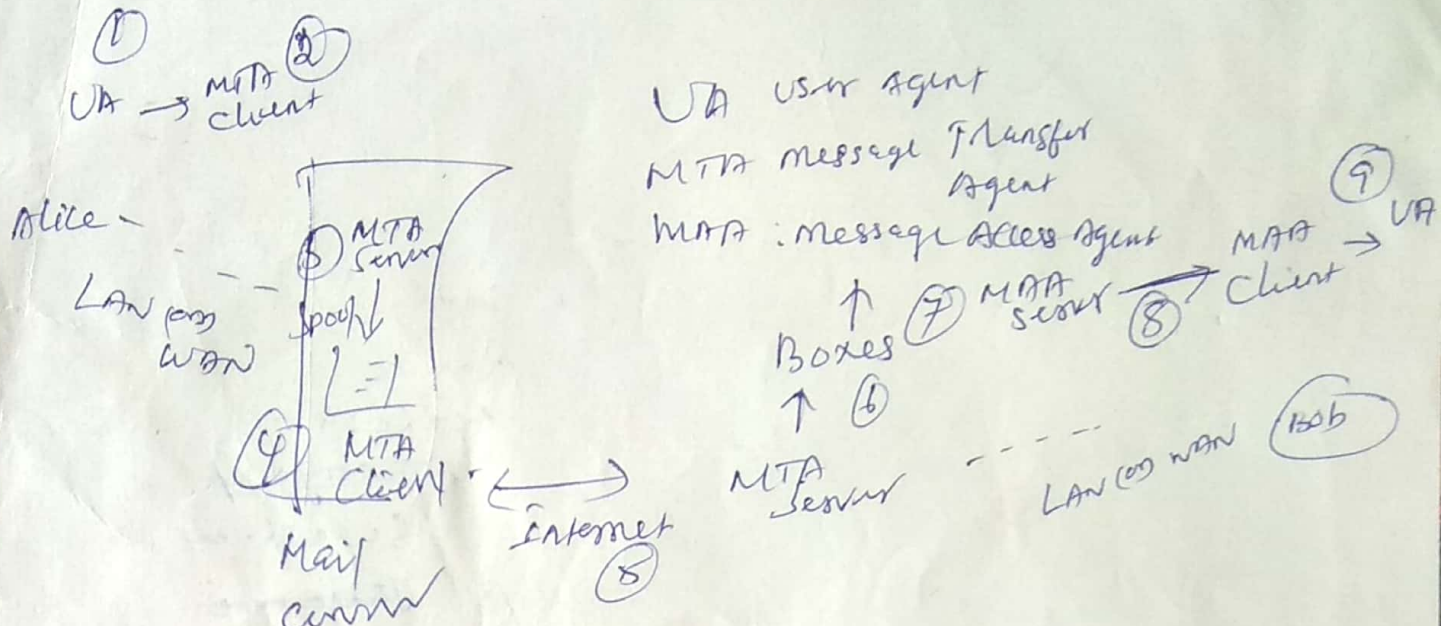


POP3 two modes:

1. delete mode
2. keep mode.

→ The mail is deleted from the mailbox after each retrieval.

→ The mail remains in the mailbox after retrieval.



The e-mail S/m needs two UAs, two pairs of MTAs (client & server), & a pair of MAAs (client & server)

e-mail allows user to exchange message.

HTTP (or) FTP, server program is running & waiting request from a client all the time

We have planned to conduct Symposium on 20/9/19, in our dept. for the we Request you to provide Lunch and tea for ~~the~~ our students participant are approximately 300 members, Chief guest and faculties. Kindly do the needful.

Email Address

Local part @ Domain name

(Mailbox address of recipient) (The domain name of the Mail server)

Format of e-mail

To

From

Sub

Yours Truly,

Mail From
RCpt To:
Envelope

Header: From: To Date Sub..

Body: Dear: .. Content .. Yours Truly

message

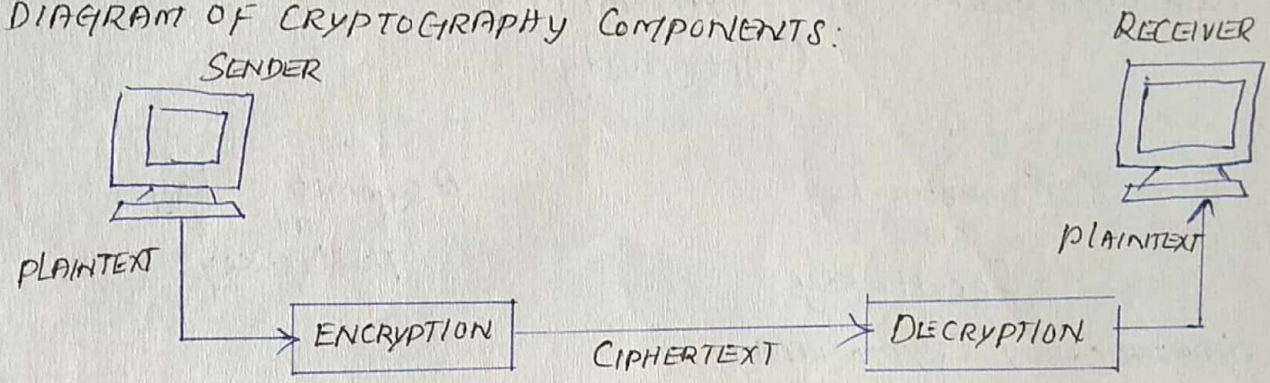
CRYPTOGRAPHY:

DEFINITION:

Cryptography, a word with Greek origins, means "SECRET WRITING".

It refer to the Science and art of transforming messages to secure and immune to attacks.

DIAGRAM OF CRYPTOGRAPHY COMPONENTS:



EXPLANATION:

PLAINTEXT AND CIPHERTEXT:

The original message, before being transformed, is called PLAINTEXT.

After the message is transformed, is called CIPHERTEXT.

ENCRYPTION AND DECRYPTION:

Encryption Algorithm transforms the plaintext into ciphertext.

A DECRYPTION ALGORITHM transforms the ciphertext back into plain-text.

The sender uses an Encryption Algorithm, and the receiver uses a decryption algorithm.

CIPHER:

To refer encryption and decryption algorithms as ciphers.

Cipher is used to different categories of algorithms in cryptography.

This is not to every sender-receiver pair needs their very own unique cipher for a secure communication one cipher can serve millions of communicating pairs.

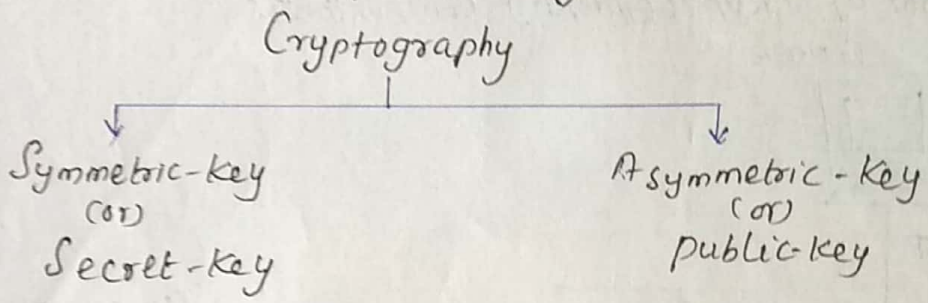
KEY: A key is a number (or) set of numbers that cipher

as, an algorithm, operates on.

To encrypt a message, need an encryption algorithm, an encryption key and the plaintext, create the Ciphertext.

To decrypt a message, need a decryption algorithm, a decryption key and Ciphertext, Reveal the original plaintext.

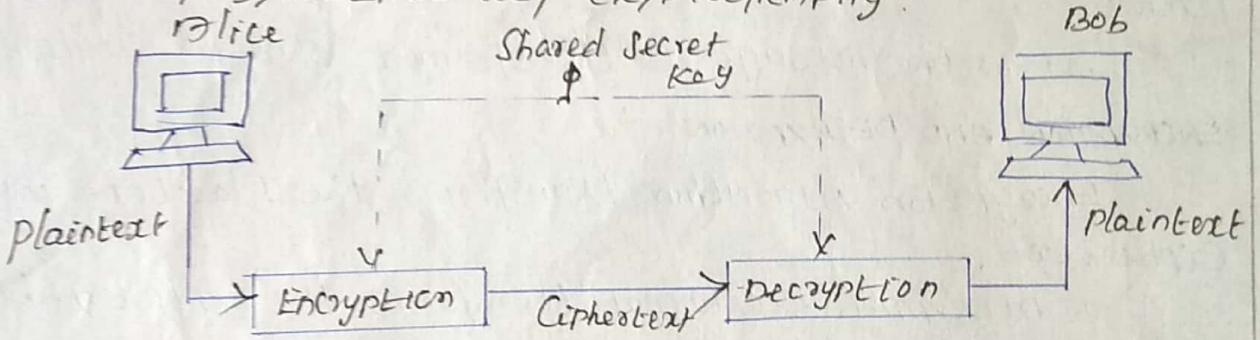
TWO CATEGORIES OF CRYPTOGRAPHY:



SYMMETRIC-KEY CRYPTOGRAPHY:

In symmetric-key Cryptography, the same key is used by sender (Encryption) and the receiver (decryption).
The key is shared.

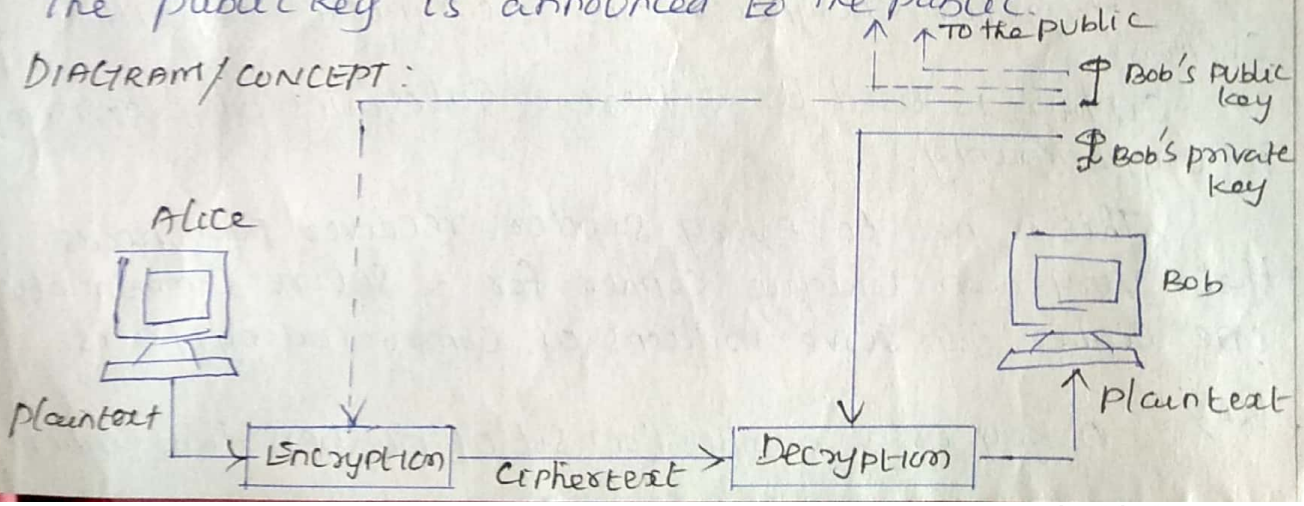
DIAGRAM OF SYMMETRIC-KEY CRYPTOGRAPHY:



ASYMMETRIC-KEY CRYPTOGRAPHY:

There are two keys, (i) private key (ii) public key
The private key is kept by Receiver.
The public key is announced to the public.

DIAGRAM/CONCEPT:



CRYPTOGRAPHY & NETWORK SECURITY:

DESCRIPTION :

Network Security can provide of the various Services are (i) Message Confidentiality (ii) Integrity (iii) Authentication (iv) Non-repudiation (v) Entity. Authentication (or) Identification

EXPLANATION OF SECURITY SERVICES:

(i) MESSAGE CONFIDENTIALITY:

(or) PRIVACY. It means that the sender and Receiver expect Confidentiality.

Transmitted message must Sense to only the intended receiver. To all others, the message must be garbage.

(ii) MESSAGE INTEGRITY:

The data must arrive at the receiver exactly as they were sent.

Must be no changes during the transmission, neither accidentally nor Maliciously.

(iii) MESSAGE AUTHENTICATION:

Service beyond message integrity. Message Authentication the receiver needs to be sure of the senders identity and imposter has not sent the message.

(iv) MESSAGE NON-REPUDIATION:

A sender must not be able to deny sending a message that he (or) she, in fact, did send.

The burden of proof falls on the Receiver.

(v) ENTITY AUTHENTICATION.

(or) User Identification. The Entity (or) user is verified prior to access to the System resources (files)

Ex: to protect the interests of university and the studen

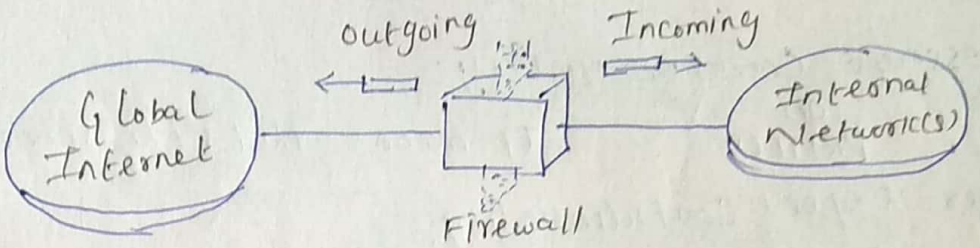
FIREWALLS:

DEFINITION:

A Firewall is a device (router (or) Computer) installed between the internal network of an organization and rest of the internet.

It designed to forward some packets and filter (not forward) others.

CONCEPT/DIAGRAM OF FIREWALL:



EXPLANATION:

Ex: A firewall may filter all incoming packets destined for a specific host (or) a specific server such as HTTP.

A firewall can be used to deny access to a specific host (or) a specific service in the organization.

CLASSIFICATION:

Classified as a (i) packet-filter firewall (or) a proxy-based firewall.

PACKET-FILTER FIREWALL:

A firewall can be used as a packet filter

It can forward (or) block packets based on information in N/w layer and transport layer headers. (TCP (or) UDP)

DEFINITION: It is a router that uses a filtering table to decide which packets must be discarded (not forwarded)