THIRD YEAR B. Sc.
COMPUTER SCIENCE

SEMESTER-V

NEW SYLLABUS
CBCS PATTERN

COMPUTER NETWORKS–II

Dr. Ms. MANISHA BHARAMBE
Dr. Mrs. HARSHITA VACHHANI

NIRALI PRAKASHAN
ADVANCEMENT OF KNOWLEDGE

SPPU New Syllabus

A Book Of

COMPUTER NETWORKS - II

For T.Y.B.Sc. Computer Science : Semester – V

[Course Code CS 352 : Credits - 2]

CBCS Pattern

As Per New Syllabus, Effective from June 2021

Dr. Ms. Manisha Bharambe

M.Sc. (Comp. Sci.), M.Phil. Ph.D. (Comp. Sci.)

Vice Principal, Associate Professor, Department of Computer Science

MES's Abasaheb Garware College

Karve Road, Pune

Dr. Mrs. Harshita Vachhani

M.Sc. (Comp. Sci.), M.B.A. (H.R.) Ph.D. (Comp. Sci.)

Head, Department of Computer Science

Pratibha College of Commerce and Computer Studies

Chinchwad, Pune

Price ₹ 200.00

NIRALI PRAKASHAN

ADVANCEMENT OF KNOWLEDGE

N5862

COMPUTER NETWORKS - II **ISBN 978-93-5451-177-6**

First Edition : August 2021

Published By :
NIRALI PRAKASHAN
Abhyudaya Pragati, 1312, Shivaji Nagar,
Off J.M. Road, Pune – 411005
Tel - (020) 25512336/37/39
Email : niralipune@pragationline.com

Polyplate

Printed By :
YOGIRAJ PRINTERS AND BINDERS
Survey No. 10/1A, Ghule Industrial Estate
Nanded Gaon Road
Nanded, Pune - 411041

DISTRIBUTION CENTRES

PUNE

Nirali Prakashan
(For orders outside Pune)
S. No. 28/27, Dhayari Narhe Road, Near Asian College
Pune 411041, Maharashtra
Tel : (020) 24690204; Mobile : 9657703143
Email : bookorder@pragationline.com

Nirali Prakashan
(For orders within Pune)
119, Budhwar Peth, Jogeshwari Mandir Lane
Pune 411002, Maharashtra
Tel : (020) 2445 2044; Mobile : 9657703145
Email : niralilocal@pragationline.com

MUMBAI

Nirali Prakashan
Rasdhara Co-op. Hsg. Society Ltd., 'D' Wing Ground Floor, 385 S.V.P. Road
Girgaum, Mumbai 400004, Maharashtra
Mobile : 7045821020, Tel : (022) 2385 6339 / 2386 9976
Email : niralimumbai@pragationline.com

DISTRIBUTION BRANCHES

DELHI

Nirali Prakashan
Room No. 2 Ground Floor
4575/15 Omkar Tower, Agarwal Road
Darya Ganj, New Delhi 110002
Mobile : 9555778814/9818561840
Email : delhi@niralibooks.com

BENGALURU

Nirali Prakashan
Maitri Ground Floor, Jaya Apartments,
No. 99, 6th Cross, 6th Main,
Malleswaram, Bengaluru 560003
Karnataka; Mob : 9686821074
Email : bengaluru@niralibooks.com

NAGPUR

Nirali Prakashan
Above Maratha Mandir, Shop No. 3,
First Floor, Rani Jhanshi Square,
Sitabuldi Nagpur 440012 (MAH)
Tel : (0712) 254 7129
Email : nagpur@niralibooks.com

KOLHAPUR

Nirali Prakashan
New Mahadvar Road, Kedar Plaza,
1st Floor Opp. IDBI Bank
Kolhapur 416 012 Maharashtra
Mob : 9850046155
Email : kolhapur@niralibooks.com

JALGAON

Nirali Prakashan
34, V. V. Golani Market, Navi Peth,
Jalgaon 425001, Maharashtra
Tel : (0257) 222 0395
Mob : 94234 91860
Email : jalgaon@niralibooks.com

SOLAPUR

Nirali Prakashan
R-158/2, Avanti Nagar, Near Golden
Gate, Pune Naka Chowk
Solapur 413001, Maharashtra
Mobile 9890918687
Email : solapur@niralibooks.com

marketing@pragationline.com | www.pragationline.com

Also find us on www.facebook.com/niralibooks

Preface ...

We take an opportunity to present this Text Book on **"Computer Networks - II"** to the students of Third Year B.Sc. (Computer Science) Semester-V as per the New Syllabus, June 2021.

The book has its own unique features. It brings out the subject in a very simple and lucid manner for easy and comprehensive understanding of the basic concepts. The book covers theory of Application Layer, Multimedia, Cryptography and Network Security and Security in the Internet.

A special word of thank to Shri. Dineshbhai Furia and Mr. Jignesh Furia for showing full faith in us to write this text book. We also thank to Mr. Amar Salunkhe and Mrs. Prachi Sawant of M/s Nirali Prakashan for their excellent co-operation.

We also thank Mr. Ravindra Walodare, Mr. Sachin Shinde, Mr. Ashok Bodke, Mr. Moshin Sayyed and Mr. Nitin Thorat.

Although every care has been taken to check mistakes and misprints, any errors, omission and suggestions from teachers and students for the improvement of this text book shall be most welcome.

Authors

❖❖❖

Syllabus ...

1. Application Layer (10 Lectures)

- Domain Name System:
  - Name Space: Flat Name Space, Hierarchical Name Space
  - Domain Name Space: Label, Domain Name, FQDN, PQDN
  - Distribution of Domain Name Space: Hierarchy of Name Servers, Zone, Root Server, Primary and Secondary Servers
  - DNS in the Internet: Generic Domains, Country Domains, Inverse Domain
  - Resolution: Resolver, Mapping Names to Address, Mapping Addresses to Names, Recursive Resolution, Iterative Resolution, Caching
- Electronic Mail:
  - Architecture: First Scenario, Second Scenario, Third Scenario, Fourth Scenario
  - User Agent: Services of User Agent, Types of UA, Format of E-mail
  - MIME: MIME Header
  - Message Transfer Agent: SMTP
  - Message Access Agent: POP and IMAP
- File Transfer:
  - FTP: Communication over Data and Control Connection, File Type, Data Structure, Transmission Mode, Anonymous FTP

2. Multimedia (8 Lectures)

- Digitizing Audio and Video, Audio and Video Compression
- Streaming Stored Audio/Video:
  - First Approach
  - Second Approach
  - Third Approach
  - Fourth Approach
- Streaming Live Audio/Video
- Real Time Interactive Audio/Video:
  - Characteristics, Time Relationship, Timestamp, Playback Buffer, Ordering, Multicasting, Translation
- RTP: Packet Format
- RTCP: Message Types
- Voice over IP:
  - SIP: SIP Session
  - H.323: Architecture, Protocols

3. Cryptography and Network Security (9 Lectures)

- Terminology:
  - Cryptography, Plain text and Cipher text, Cipher key, Categories of Cryptography: Symmetric Key, Asymmetric Key
- Encryption Model

- Symmetric Key Cryptography:
  - Traditional Ciphers: Substitution Cipher, Shift Cipher, Transposition Cipher
  - Simple Modern Ciphers: XOR, Rotation Cipher, s-box, p-box
  - Modern Round Ciphers: DES
  - Mode of Operation: ECB, CBC, CFB, OFB
- Asymmetric Key Cryptography: RSA
- Security Services
  - Message Confidentiality: With Symmetric Key Cryptography, With Asymmetric Key Cryptography
  - Message Integrity: Document and Fingerprint, Message and Message Digest
  - Message Authentication: MAC, HMAC
  - Digital Signature
  - Entity Authentication: Passwords, Fixed Passwords, Challenge-response

4. Security in the Internet (9 Lectures)

- IP Security (IPSec):
  - Two Modes
  - Two Security Protocols
  - Services provided by IPSec
  - Security Association
  - Internet Key Exchange
  - Virtual Private Network
- SSL/TLS:
  - SSL Services
  - Security Parameters
  - Sessions and Connections
  - Four Protocols
  - Transport Layer Security
- PGP:
  - Security Parameters
  - Services
  - PGP Algorithms
  - Key Rings
  - PGP Certificates
- Firewalls:
  - Packet Filter Firewall
  - Proxy Firewall

❖❖❖

Contents ...

❖❖❖

CHAPTER 1

Application Layer

Objectives...

- To understand Application Layer
- To learn Concepts of E-mail
- To study File Transfer using FTP
- To learn Basic Concepts of DNS

1.0 INTRODUCTION

- The application layer is the top most layer in OSI and TCP/IP reference models. The application layer provides a means for the user to access information on the network through an application.
- The application layer is responsible for providing services to the user and user applications. The application layer enables the user, whether human or software to access the network.
- The application layer is the main interface for the user to interact with the application and therefore the network.
- The application layer provide user interfaces and support for services such as DNS, e-mail, remote file access and transfer, access to system resources, shared database management, surfing the World Wide Web (WWW) and other types of distributed information services.

1.1 DOMAIN NAME SYSTEM (DNS) (April 16, 18)

- Application layer supports several applications that follow the client/server environment.
- In client/server environment the client sends requests a resource on the network (Internet) then the server provides services in response to requests from the client.
- DNS is a client/server application program used to help other application programs and to map a host name in the application layer to an IP address in the network layer.
- The client/server programs can be divided into two categories i.e., programs which are directly used by user like e-mail and those that support other application program. DNS is a supporting program used by other applications like e-mail.

- We knew that network layer provides unique identification and source to destination delivery for a host on the Internet. For this, network layer uses its own IP protocol (for source to destination delivery) and IP addressing (for unique identification).
- However, people prefer to use names instead of numeric addresses. Therefore, we need a system that can map a name to an address or an address to a name.
- When the Internet was small, mapping was done by using a host file. Every host stores these hosts file on its disk and update it periodically from a master file. This file had two columns i.e., name and address.
- When a program or a user wanted to map a name to an address, the host consulted the host file and found the mapping.
- Today, since the size of Internet is so large and growing day-by-day, the host file becomes too large to store on every host. It would also be impossible to update all host files every time there was a change.
- One solution to this problem is, instead of storing the host file on every computer, the host file is stored on single computer and allows access to this centralized information to every computer who needs mapping.
- But it will create large traffic on the Internet and number of users will not get the mapping. So this solution also not works.
- Another solution is, instead of storing this huge information on single computer, divide this huge information into smaller parts and store each part on a different computer.
- The host that needs mapping can contact the closest computer holding the needed information. This method is Doman Name System (DNS).
- Domain Name Systems (DNS) is mechanisms that assign easy to remember names to IP address. Domain is a large group of computers on the Internet. Under this scheme each computer has an IP address and a domain name.
- Domains have been made on the base of organization type or geographical locations, e.g., the domain name google.com (where, .com indicates that Google is a commercial organization).
- In Fig. 1.1, a user wants to use a file transfer client to access the corresponding file transfer server running on a remote host. The user knows only the file transfer server name, such as Nashik.com.
- However, the TCP/IP suite needs the IP address of the file transfer server to make the connection. The following six steps map the host name to an IP address:

  Step 1: The user passes the host name to the file transfer client.

  Step 2: The file transfer client passes the host name to the DNS client.

  Step 3: Each computer, after being booted, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server.

  Step 4: The DNS server responds with the IP address of the desired file transfer server.

Step 5: The DNS client passes the IP address to the file transfer server.

Step 6: The file transfer client now uses the received IP address to access the file transfer server.

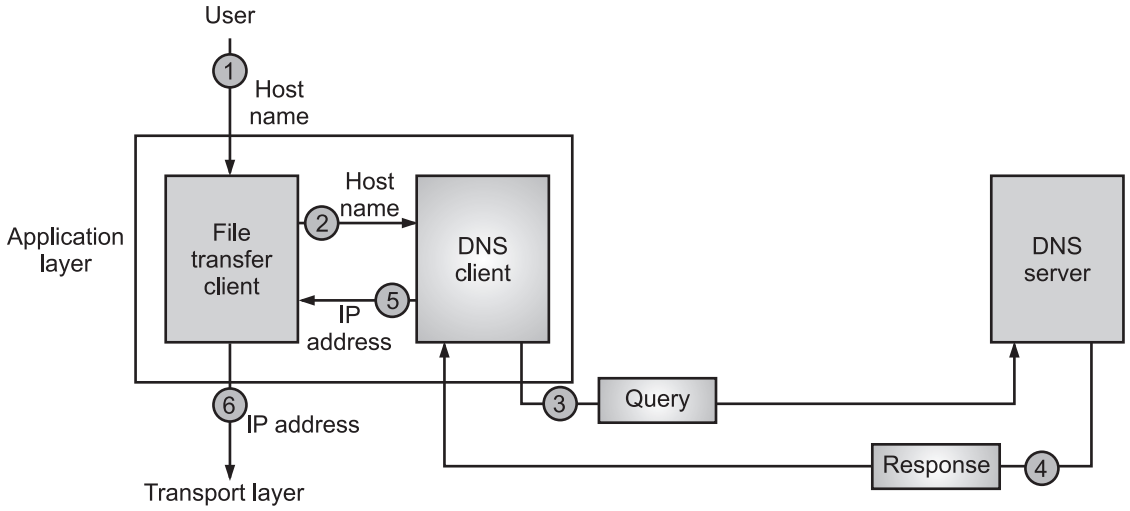


Fig. 1.1: How TCP/IP uses a DNS Client and a DNS Server to Map a Name to an Address

- Fig. 1.2 shows an example of how a DNS client/server program supports a user to find IP address.

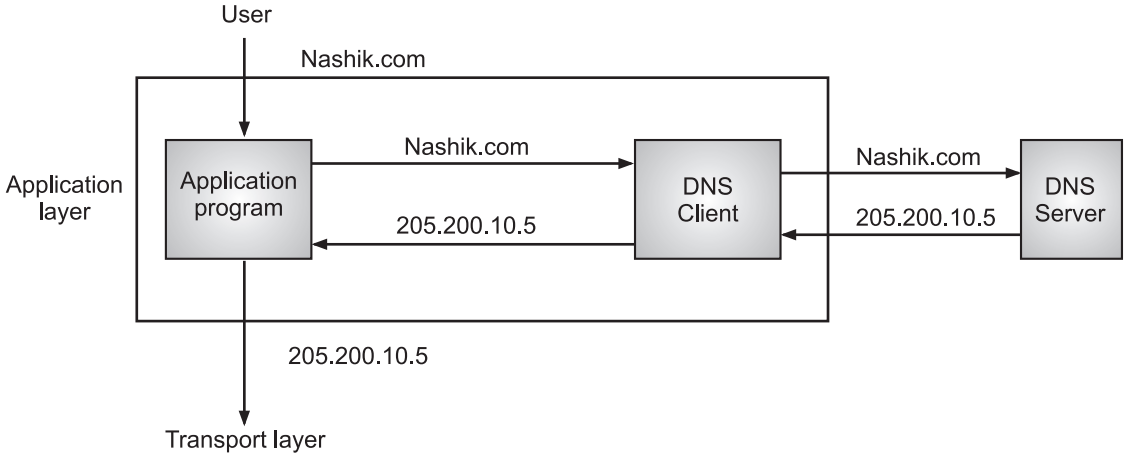


Fig. 1.2: Example of DNS Service

1.1.1 Name Space

- The names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses.
- The names must be unique because the addresses are unique. A name space that maps each address to a unique name can be organized in two ways i.e., flat or hierarchical.

1. Flat Name Space:

- In flat name space, a name is assigned to an address. A name in this space is a sequence of characters without structure.
- The names may or may not have common section. But this name space cannot be used in Internet because ambiguity and duplication is not avoided.
- For example, a Uniform Resource Locator (URL) which uniquely identifies a resource over the network likes nashik or rediff or google.

2. Hierarchical Name Space: **(April 19)**

- In hierarchical name space, every name is made up of several parts. The first part can define the nature or organization, the second part defines name of organization and third part defines departments in the organization, if any and so on.
- A central authority can assign the part of the name that defines nature of the organization and name of organization. The organization can add suffixes or prefixes to the name.
- These names are unique and cannot be duplicated. For examples, nashik.com, rediff.com, kthmcollege.edu, pune.com, nirali.com etc.

1.1.2 Domain Name Space **(April 16)**

- The domain name space refers a hierarchy in the internet naming structure. In this space, the names are defined in an inverted tree structure with the root at the top.
- The Fig. 1.3 shows the domain name space hierarchy.

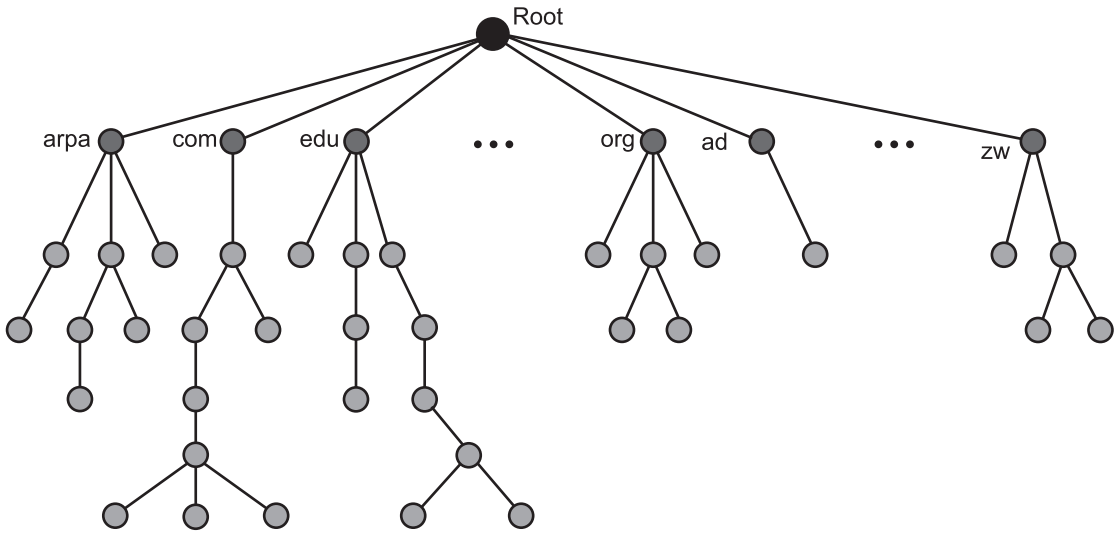


Fig. 1.3: Domain Name Space

- To have a hierarchical name space, a domain name space was designed. The names are defined in an inverted-tree structure (Refer Fig. 1.3) with root at the top.

Label:

- Each node in the tree has a label, which is a string with a maximum of 63 characters. The root label is null string.

Domain Name:

- Every node in the tree has a domain name. A full domain name is a sequence of labels separated by dots (.).
- Domain names are always read from the node up to the root. Fig. 1.4 shows some domain names.

1. Fully Qualified Domain Name:

- If a label is terminated by a null string, it is called a Fully Qualified Domain Name (FQDN).
- A FQDN is the complete domain name for a specific computer, or host, on the Internet. FQDN contains full name and all labels of a host.
- For example: unipune.ernet.in, unipune.ac.in, kthmcollege.com etc.

2. Partially Qualified Domain Name:

- If a label is not terminated by a null string, it is called a Partially Qualified Domain Name (PQDN).
- A PQDN starts from a node, but it does not reach the root.
- For example: unipune.

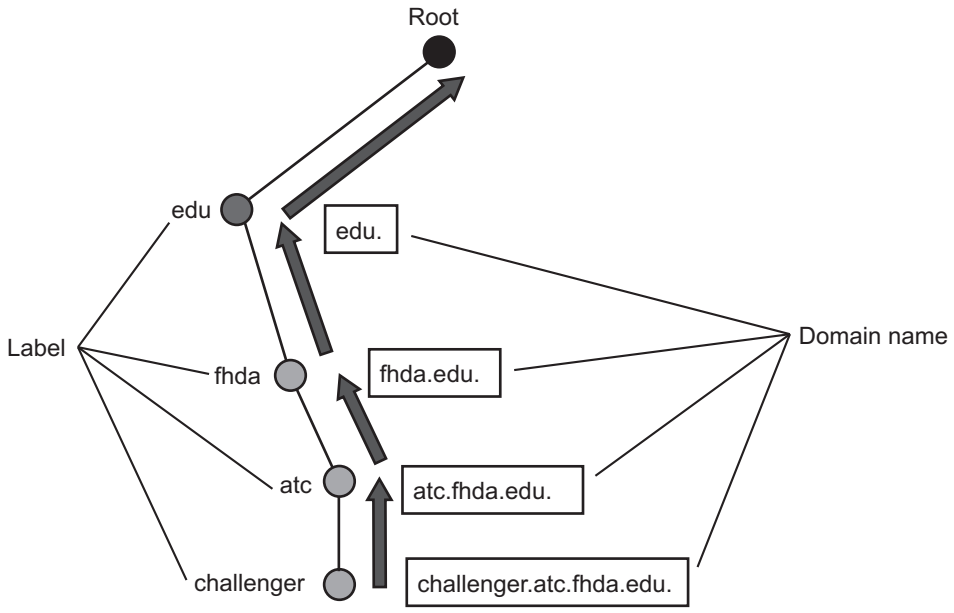


Fig. 1.4: Domain Names and Labels

3. Domain:

- A domain is a subtree of the domain name space.
- The name of the domain is the domain name of the node at the top of the subtree. A domain may be divided into sub-domains.

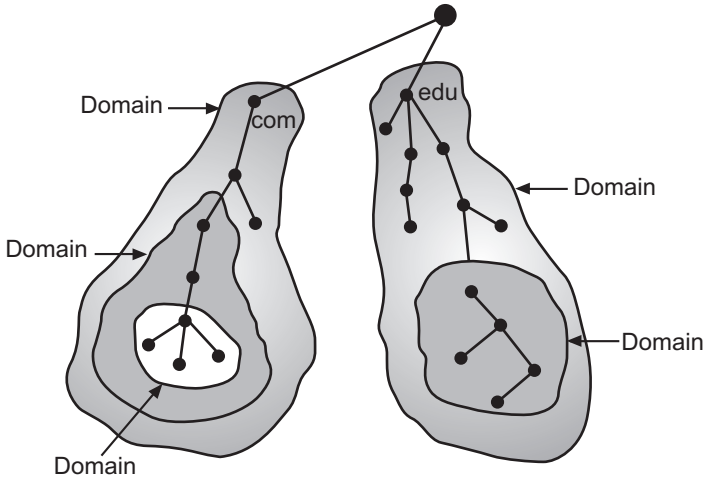


Fig. 1.5: Domains in Internet Naming Structure

- 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.

1.1.3 Distribution of Name Space

- The information contained in the domain name space must be stored. Storing this huge information on single computer is inefficient and unreliable.
- It is inefficient because all users from the world send their requests to this computer, which places a heavy load. If this computer fails then data becomes inaccessible, so it is unreliable.
- The solution of above problem is to distribute the information among many computers called DNS Servers.

Hierarchy of Name Servers:

- Name server contains the DNS database. DNS database comprises of various names and their corresponding IP addresses.
- Since it is not possible for a single server to maintain entire DNS database, therefore, the information is distributed among many DNS servers.
- Hierarchy of server is same as hierarchy of names. The entire name space is divided into the zones.

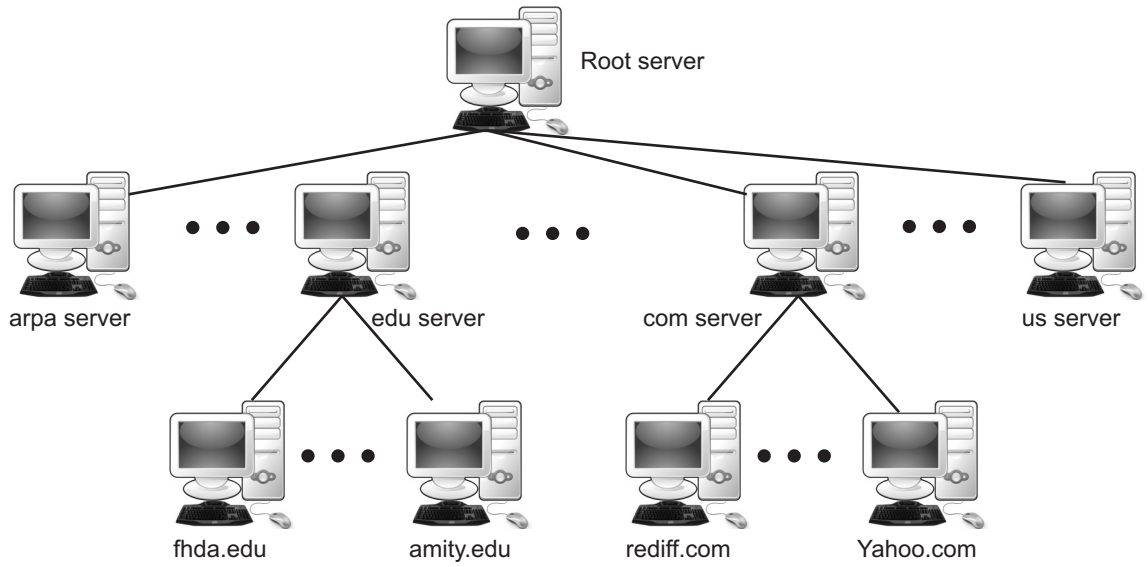


Fig. 1.6: Hierarchy of Name Servers

- DNS allows domains to be divided further into sub-domains. Each server can be responsible for either a large or small domain. We have hierarchy of servers in the same way as hierarchy of names.
- If the server divides the domain into sub-domains and assigns responsibility to different servers, zone and domain are different. Each server has authority over a zone.
- A DNS zone is a portion of the global Domain Name System (DNS) net-nuance for which administrative responsibility has been delegated.
- The authority over each DNS zone is delegated to a legal entity or organization (i.e. a country-code lop-level domain registry) or a company/individual.
- A zone is created mainly for administrative purposes. If a server stores the entire domain, the zone and domain are the same.

Zone:

- Since, the complete domain name hierarchy cannot be stored on a single server, it is divided among many servers. What a server is responsible for or has authority over is called a zone.
- If a server accepts responsibility for a domain and does not divide the domain into smaller domains (sub-domains), the "domain" and the 'zone" refers to the same thing.
- The server makes a database called a zone file and keeps all the information for every node under that domain.

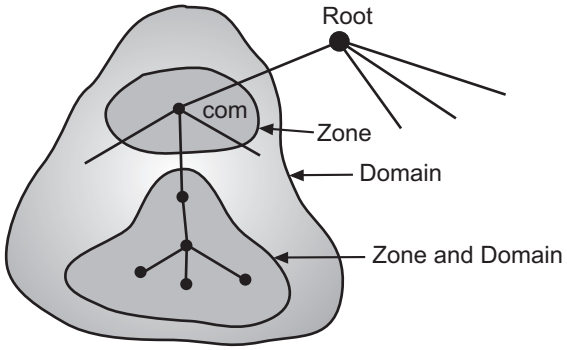


Fig. 1.7: Zones and domains

Root Server:

- Root servers are DNS name servers that operate in the root zone. Root Server is the top level server which consists of the entire DNS tree.
- It does not contain the information about domains but delegates the authority to the other server.
- Root servers are an essential part of the infrastructure of the Internet; web browsers and many other internet tools would not work without them.

Primary and Secondary Servers:

- DNS defines two types of servers i.e., Primary and Secondary.

1. **Primary Servers:**

- A primary server is a server that stores a file about the zone for which it is an authority.
- It is responsible for creating, maintaining and updating the zone file. It stores the zone file on a local disk.

2. **Secondary Server:**

- A secondary server is a server that transfers all information from the primary server.
- When the secondary downloads information from the primary, it is called zone transfer.

Zone Transfer:

- A primary server loads all information from the disk file; the secondary DNS Server loads all information from the primary server.
- When the primary DNS server downloads information from the secondary, it is called zone transfer.

1.1.4 DNS in the Internet

- In the Internet, the domain name space is divided into three different sections i.e., generic domains, country domains and the inverse domain.

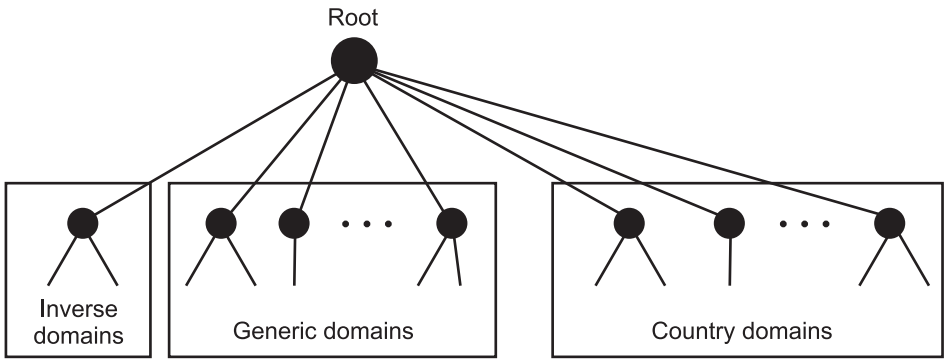


Fig. 1.8: DNS used in the Internet

- The domain names in Fig. 1.8 are explained below:

1. Generic Domains: **(April 17)**

- The generic domains define registered host according to their generic behavior.
- In generic domains each node in the tree defines a domain, which is an index to the domain name space database as shown Fig. 1.9.

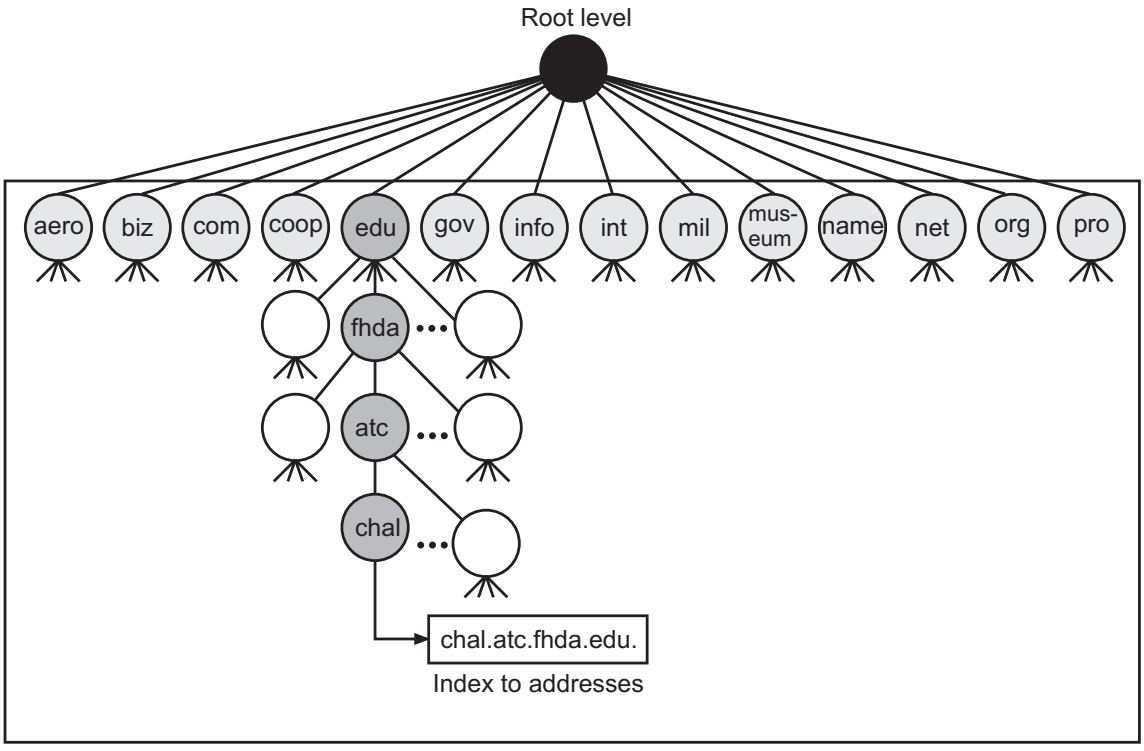


Fig. 1.9: Generic Domains

- Table 1.1 gives list of labels used in generic domain.

Table 1.1: Generic Domain Labels

Label	Description
aero	Airlines and aerospace companies.
biz	Business or firms.
com	Commercial organizations.
coop	Co-operative business organizations.
edu	Educational institutions.
gov	Government institutions.
info	Information service providers.
int	International organizations.
mil	Military groups.
museum	Museums and other non-profit organizations.
name	Personal names.
net	Network support centers.
org	Non-profit organizations.

2. Country Domains:

- Country domains uses two characters country abbreviations (e.g. in for India). Second labels can be organizational or national designations.
- Fig. 1.10 shows the country domains.

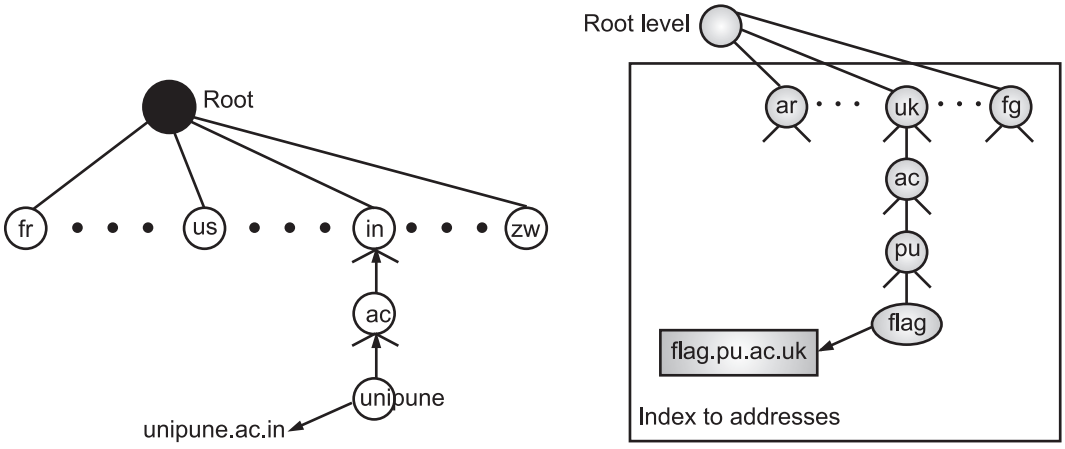


Fig. 1.10: Country Domains

3. Inverse Domain:

- The inverse domain is used to map an address to a name. This can be happen, for example, server want to check his authorized client.
- Fig. 1.11 shows example of inverse domain.

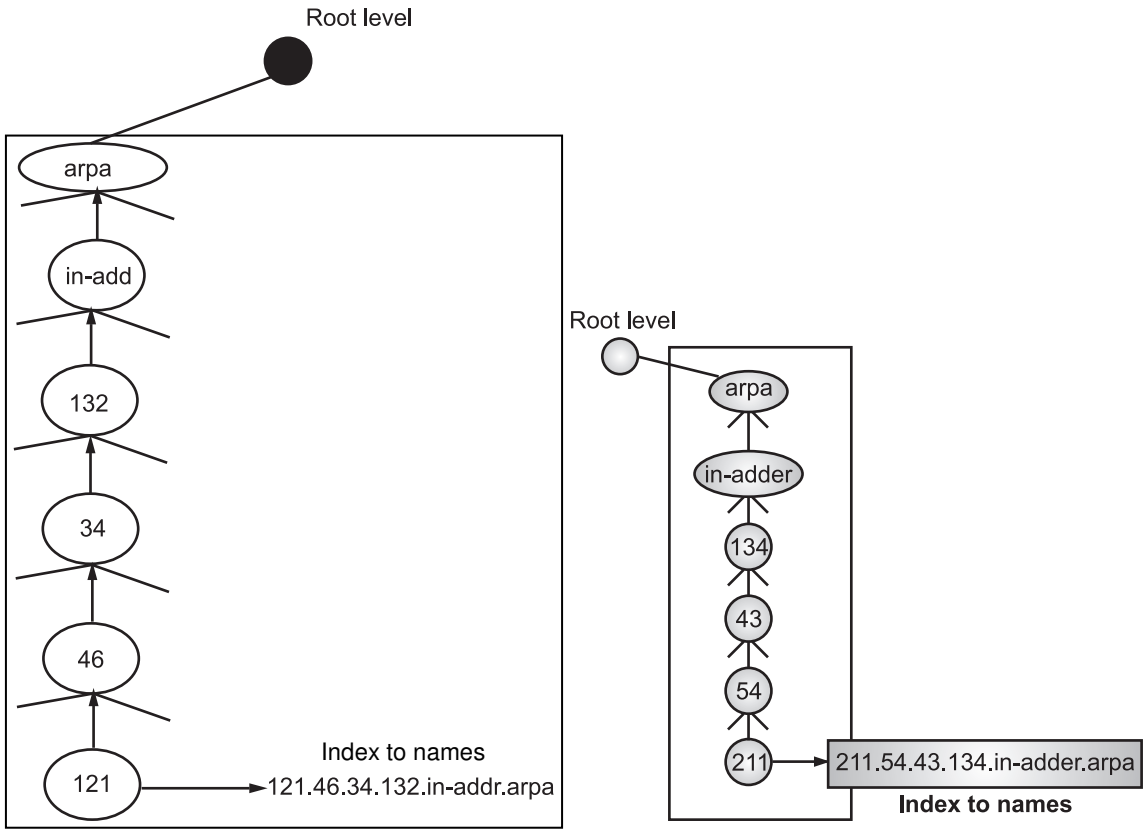


Fig. 1.11: Inverse Domain

1.1.5 Resolution

(Oct. 18, April 19)

- Mapping a name to an address or an address to a name is called as address resolution.

Resolver:

- DNS is a client/server application. When a host requires mapping of name to an address or an address to a name, it calls DNS client called a resolver.
- The resolver accesses the closest DNS sever with mapping request. If the server knows the mapping, it gives it to resolver or it redirects the resolver to other server.

Mapping Names to Addresses:

- The resolver gives a domain name to the server and asks for the correct address. The server either checks the generic domains or the country domains for the mapping.
- Query is sent by the resolver to the local DNS server for resolution. If the local server cannot resolve the query, it either refers the resolver to other servers or asks other servers directly.

Mapping Addresses to Names:

- A client can send an IP address to a server to be mapped to a domain name.
- To answer such type of query, DNS server uses inverse domain.

Recursive Resolution:

- If the client (resolver) sends recursive query to the DNS server and expects the server to supply the final answer, if that server is the authority for the domain name, it checks the database and responds.
- If the server is not authority, it sends the request to another server and waits for response. If this server is authority, it responds, otherwise it sends the query to yet another server.
- When the query is finally resolved, the response travels back up to the requesting client. This is called recursive resolution and it is shown in Fig. 1.12.

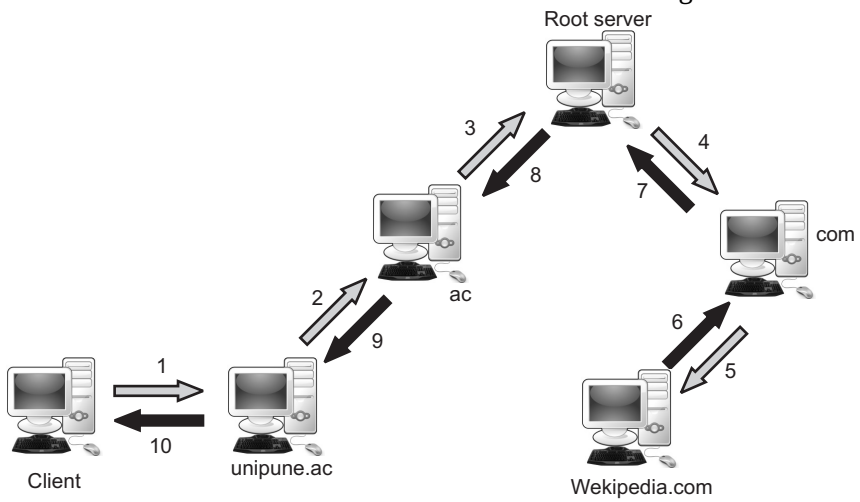


Fig. 1.12: Recursive Resolution

Iterative Resolution:

- If the client does not ask for a recursive query, the mapping can be iterative. If the server is authority for the name it gives reply to the client. Otherwise it returns the IP address of a server that it thinks can resolve the query.
- Now client again ask to that new server about mapping, if it knows, it gives reply, otherwise it gives the IP address of server which he thinks solve the query.
- Now, the client must repeat the query to the third server and so on. This process is called iterative resolution because the client repeats the same query to multiple servers.
- Fig. 1.13 shows iterative resolution.

Caching:

- Every time when DNS server receives a request from client, it has to search in its database and then gives reply. If this search time reduces, efficiency increases.
- DNS use caching to do this. When a server asks for a mapping from another server and receives the response, it stores the information in its cache memory before sending it to the client.

- If the same or another client asks for the same mapping, it can check its cache memory and gives reply. The server marks such type of response as un-authoritative.
- Caching speeds up the resolution but sometimes it can also be problematic.

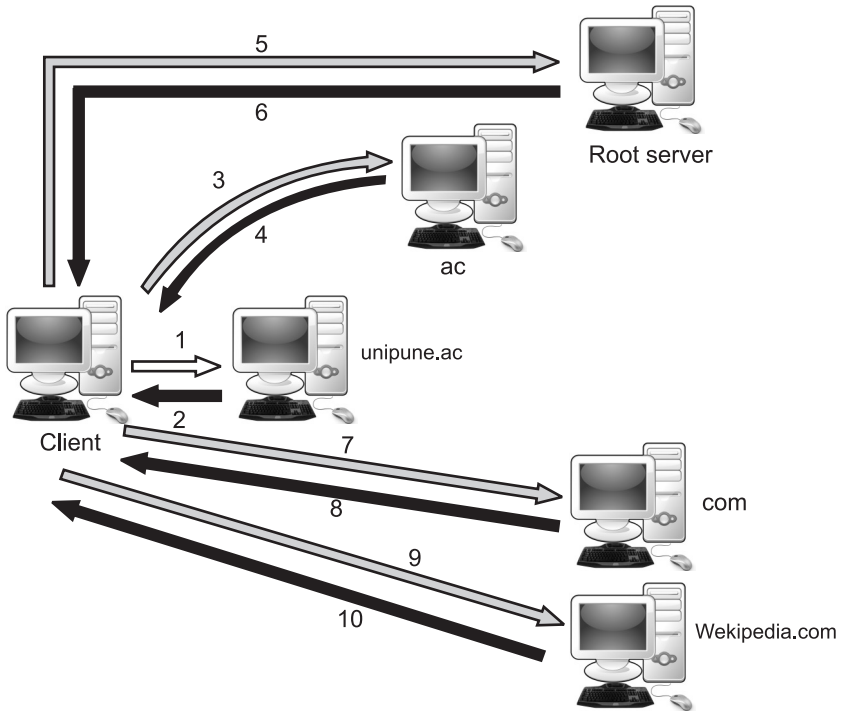
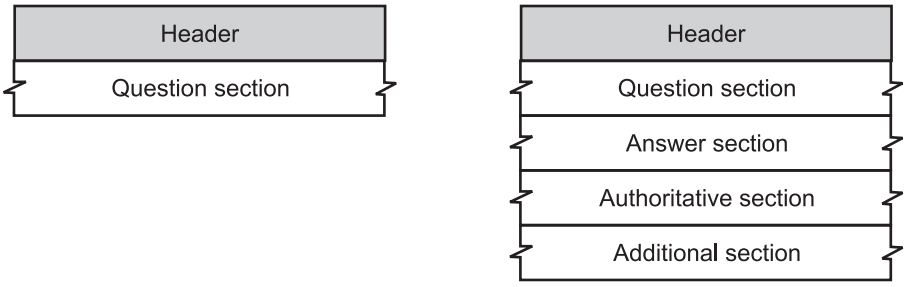


Fig. 1.13: Iterative Resolution

1.1.6 DNS Messages

- DNS has two types of messages namely, query and response. Both types of messages have the same format.
- The query message consists of a header and question records as shown in Fig. 1.14 (a).
- The response message consists of a header, question records, answer records, authoritative records, and additional records as shown in Fig. 1.14 (b).



(a) DNS Query Message **(b) DNS Response Message**

Fig. 1.14: DNS Messages

Header:

- Both query and response messages have the same header format with some fields set to zero for the query messages.
- The header is 12 bytes and its format is shown in Fig. 1.15.

Identification	Flags
Number of question records	Number of answer records (all 0s in query message)
Number of authoritative records (all 0s in query message)	Number of additional records (all 0s in query message)

Fig. 1.15: Header Format

- The header fields are as follows:
  - **Identification** is a 16-bit field used by the client to match the response with the query. The client uses a different identification number each time it sends a query. The server duplicates this number in the corresponding response.
  - **Flags,** is a 16-bit field consisting of the subfields shown in Fig. 1.16.

Fig. 1.16: Flag Fields

A brief description of each flag subfield follows:

- **QR (Query/Response)** is a 1-bit subfield that defines the type of message. If it is 0, the message is a query. If it is 1, the message is a response.
- **OpCode** is a 4-bit subfield that defines the type of query or response (0 if standard, 1 if inverse, and 2 if a server status request).
- **AA (Authoritative Answer)** is a 1-bit subfield. When it is set (value of 1) it means that the name server is an authoritative server. It is used only in a response message.
- **TC (TrunCated)** is a 1-bit subfield. When it is set (value of 1), it means that the response was more than 512 bytes and truncated to 512. It is used when DNS uses the services of UDP.
- **RD (Recursion Desired)** is a 1-bit subfield. When it is set (value of 1) it means the client desires a recursive answer. It is set in the query message and repeated in the response message.
- **RA (Recursion Available)** is a 1-bit subfield. When it is set in the response, it means that a recursive response is available. It is set only in the response message.

- **Reserved** is a 3-bit subfield set to 000.
- **rCode** is a 4-bit field that shows the status of the error in the response.

- **Question Section** consisting of one or more question records. It is present on both query and response messages.
- **Answer Section** consisting of one or more resource records. It is present only on response messages. This section includes the answer from the server to the client (resolver).
- **Authoritative Section** consisting of one or more resource records. It is present only on response messages. This section gives information (domain name) about one or more authoritative servers for the query.
- **Additional Information Section** consisting of one or more resource records. It is present only on response messages. This section provides additional information that may help the resolver.

1.2 E-MAIL

- The main task of the Internet is to provide services to users. E-mail is most popular application of Internet. E-mail is short form of electronic mail.
- At the beginning of the Internet, the messages sent by electronic mail were short and contains text only. Today, e-mails are much more complex and contains text, audio and video and one message can be sent to multiple recipients.
- We will study architecture of e-mail and the components of e-mail system in this section.

1.2.1 Architecture (April 19)

- To understand the architecture of e-mail, we will discuss four scenarios associated with e-mail system.

First Scenario:

- In this scenario, the sender and the receiver of the e-mail are users on the same system. Every user is having one mail box created by administrator.
- A mail box is a part of local hard disk. When user Amar (A) wants to send a message to another user Bhushan (B), Amar runs a User Agent (UA) program to create mail and store it in Bhushan's mail box.
- Every mail has sender's and recipient mail addresses. Bhushan can read the contents of his mail box at his convenience, using a user agent.
- When the sender and the receiver of an e-mail are on the same system, we need only two user agents. This is shown in Fig. 1.17.

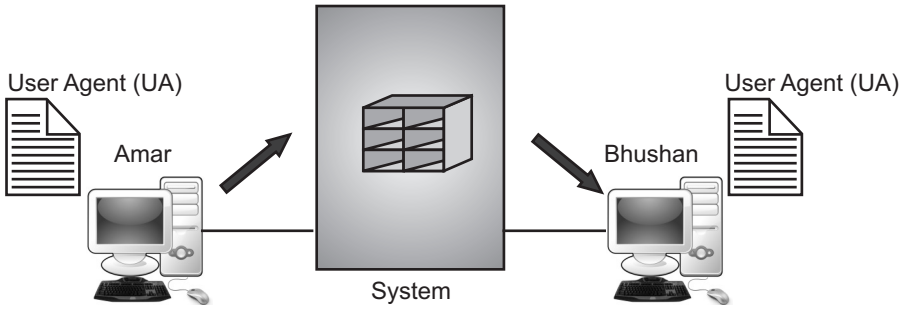


Fig. 1.17: First scenario in Electronic Mail

Second Scenario:

- In the second scenario, the sender and receiver of the e-mail are users from different systems. The message is sent over the Internet. Thus, we need two user agents and pair of MTAs (client and server).
- Amar, the sender uses user agent program to send her message at her own site. Bhushan, the receiver needs user agent program to retrieve messages stored in the mail box of the system at his site.
- To send the messages from Amar's site to Bhushan's site, two Message Transfer Agents (MTAs) are needed, one client and one server. This is shown in Fig. 1.18.

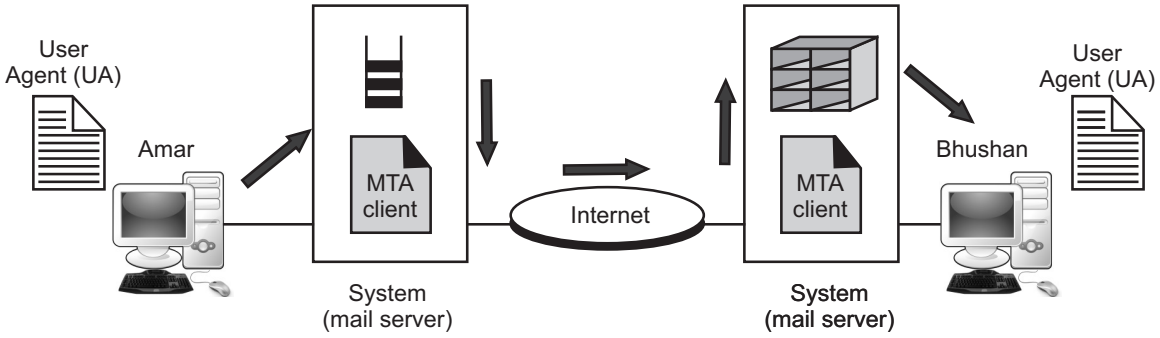


Fig. 1.18: Second scenario in Electronic Mail

Third Scenario:

- In this scenario, Bhushan, the receiver is directly connected to his system. Amar, the sender is separated from him system. He is connected to the system via dial up modem or DSL etc.
- Amar uses user agent to prepare his message.
- The message is now send through the LAN or WAN. This is done by using pair of message transfer agent (client and server).

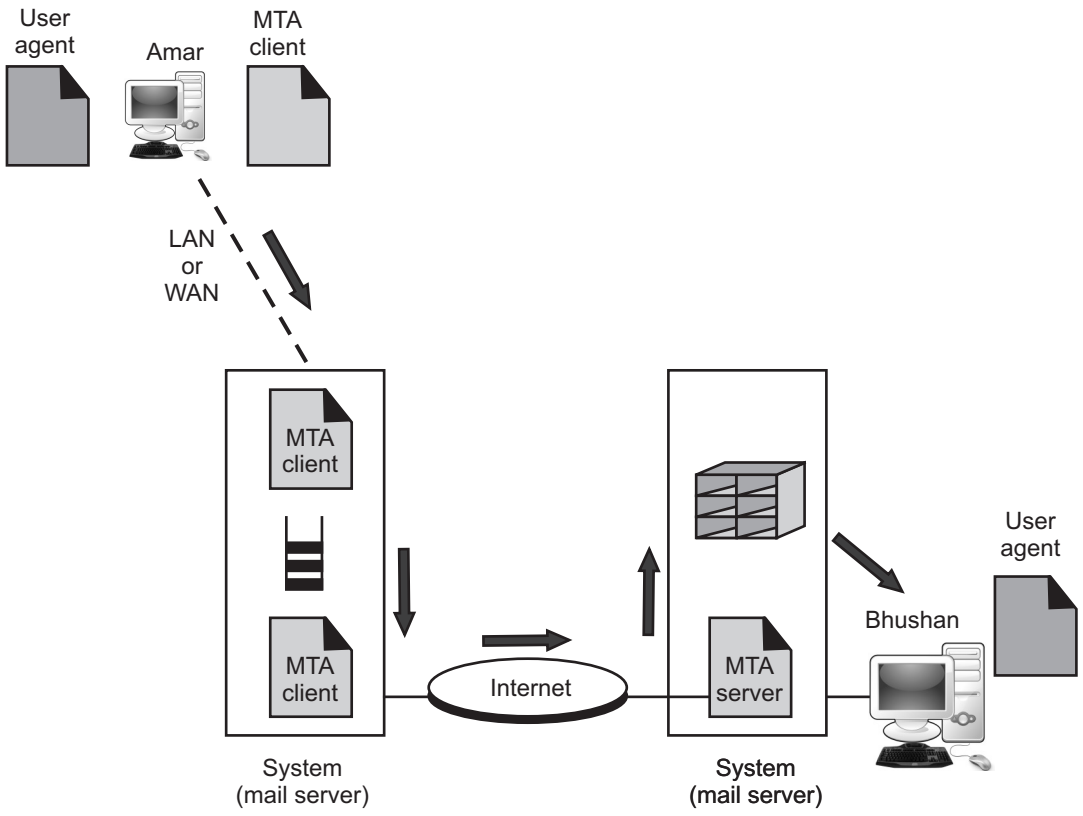


Fig. 1.19: Third scenario in Electronic Mail

- MTA client establishes a connection with MTA server. MTA client then send the message to the system at Bhushan's site.
- System receives it and stores it in Bhushan's mail box. As per his convenience, Bhushan uses his user agent to retrieve his message.
- Note that, when the sender is connected to the mail server via a LAN or a WAN, we need two UAs and two pairs of MTAs (client and server).

Fourth Scenario:

- In the fourth and most common scenario, Bhushan, the receiver is also connected to his mail server by a WAN or LAN. When the message is arrived at Bhushan's server, he retrieves it by using another set of client/server agents also called as Message Access Agents (MAAs).
- Bhushan uses MAA client to retrieve the message. The MAA client pulls the messages from the mail server and pushes them into a special MAA server.
- Bhushan uses MAA client to retrieve messages from the MAA server.

- In short, we can say, when both sender and receiver are connected to the mail server via a LAN or WAN, we need two UAs, two pairs of MTAs, and a pair of MAAs. This is most common situation today, shown in Fig. 1.20.

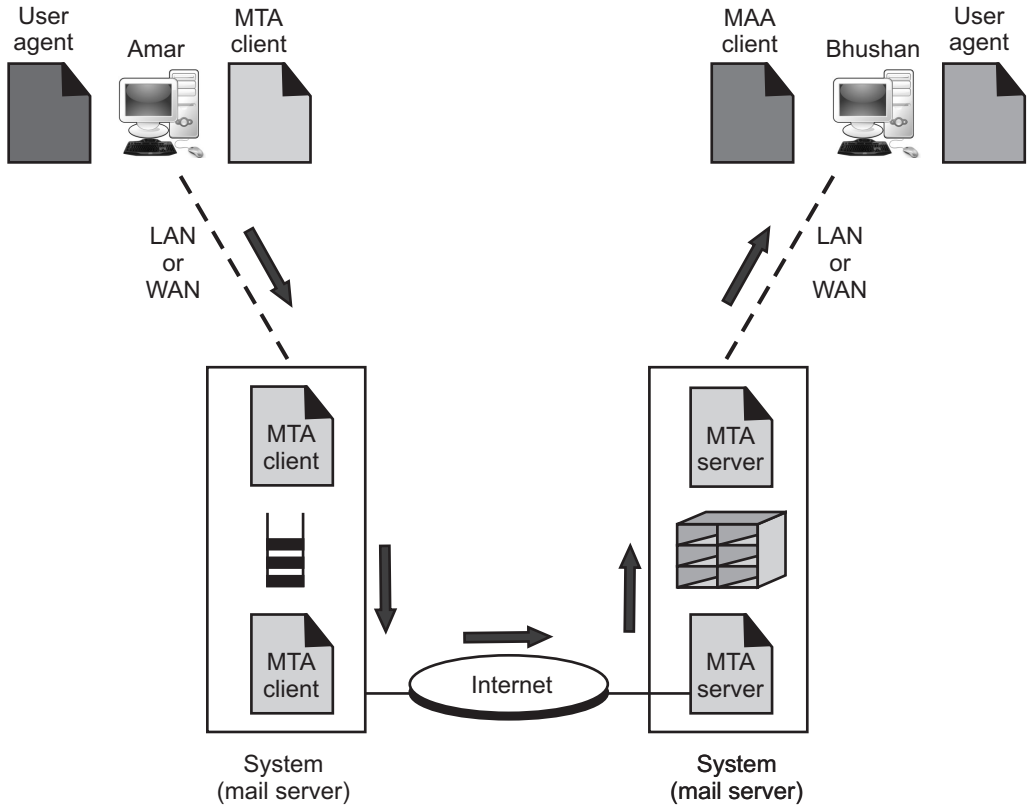


Fig. 1.20: Fourth scenario in Electronic Mail

1.2.2 User Agent

- The first component of e-mail system is User Agent (UA). It provides services to user. The user agent provides service to the user to make the process of sending and receiving a message easier.

Services Provided by User Agent:

- A user agent is a software that provides following services shown in Fig. 1.21.

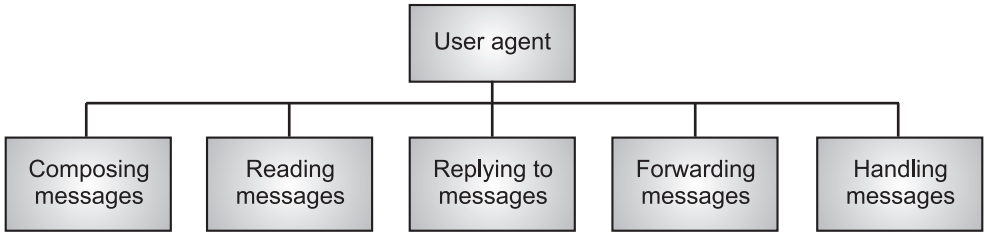


Fig. 1.21: Services of User Agent

- Let us see messages in Fig. 1.21 in detail:

1. Composing Messages:

- A user agent helps the user to compose (create) an e-mail. User agent provides a template on the screen, which helps the user.
- Some even have built in editor that can do spell checking, grammar checking, cut, copy, paste etc. text formatting functions.

2. Reading Messages:

- Next function of user agent is to read incoming messages. User agent first checks the mail in the incoming mail box. User agent shows a one line summary of every received mail.
- Every e-mail contains number field, flag showing status of e-mail like new, read, replied etc., size of message, the sender and the optional subject field.

3. Replying to Messages:

- After reading a message, user sent reply by using user agent.
- The user agent allows the user to reply to the original sender or to reply all recipients of the messages.

4. Forwarding Messages:

- User agent allows the receiver to forward the message, with or without extra comments, to a third party.

5. Handling Mail Boxes:

- A user agent creates two mail boxes i.e., inbox and outbox.
- Inbox keeps all the received e-mails until they are deleted by the user. The outbox keeps all the sent e-mails until the user deletes them.

Types of User Agent:

- User agent can be of two types:

1. Command Driven:

- Command driven user agents belong to the early days of e-mail.
- A command driven user agent normally accepts one character from the keyboard to perform its task, e.g. mail, pine and elm.

2. GUI Based:

- Modern user agents are GUI-based, which contains graphical user interface that allow the user to use keyboard and mouse, e.g. Outlook, Netscape, Eudor(a)

Sending Mail:

- To send mail, user creates a mail. E-mail has an envelope and a message as shown in Fig. 1.22.

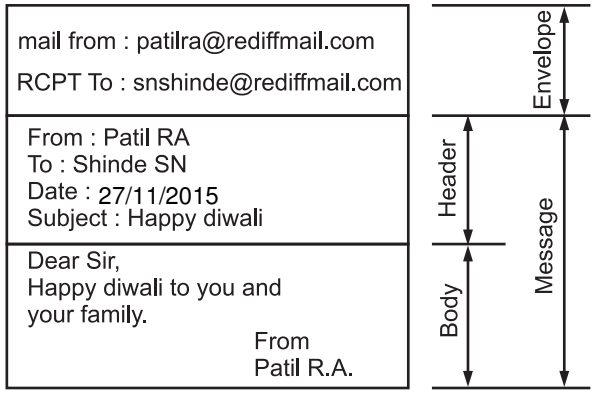


Fig. 1.22: Format of E-mail

- The fields in email message are explained below:

Envelope:

- The envelope contains sender and receiver addresses.

Message:

- Message contains header and body. In header, sender, receiver, date, subject of e-mail are defined. Body part contains actual information to be read by the recipient.

Receiving Mail:

- If user has a mail, UA informs the user. A list is displayed to the user in which summary of e-mail is mentioned.
- The user can selects any of the messages and display its contents on the screen.

Addresses:

- To deliver a mail, a mail handling system must use an addressing system with unique addresses.
- E-mail address contains two parts, local port and a domain name, separated by @ sign (Refer Fig. 1.23).
- Local port defines the name of user mail box. And domain name defines the name of mail server (Refer Fig. 1.24).

Fig. 1.23: E-mail Address

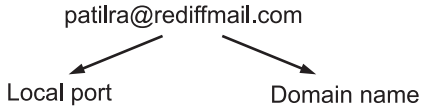


Fig. 1.24

1.2.3 MIME

- E-mail system has one limitation, it can send messages only in NVT 7-bit ASCII. It cannot be used for languages like German, Russian, Chinese, Japanese and Hebrew. Also it cannot be used to send binary files or video or audio data.
- The Multipurpose Internet Mail Extensions (MIME) is a protocol that allows non-ASCII data to be sent through e-mail.

- MIME transforms non-ASCII data at sender site to NVT (Network Virtual Terminal) ASCII and delivers them to the client MTA to be sent through the Internet. The message at the receiving site is transformed back to the original data
- Suppose a user (Amar) wants to send an email through user agent and it is in a non-ASCII format so there is a MIME protocol which converts it into 7-bit NVT ASCII format.
- Message is transferred through e-mail system to the other side in 7-bit format now MIME protocol again converts it back into non-ASCII code and now the user agent of receiver side reads it and then information is finally read by the receiver (Bhushan).

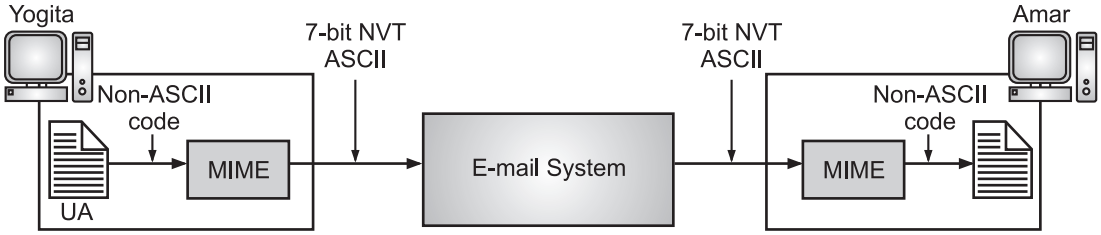


Fig. 1.25: MIME

MIME Headers:

- MIME header is basically inserted at the beginning of any e-mail transfer. MIME defines five headers namely, MIME-Version, Content-Type, Content-Type-Encoding, Content-Id and Content-Description (Refer Fig. 1.40) that can be added to the original e-mail header section to define the transformation parameters.

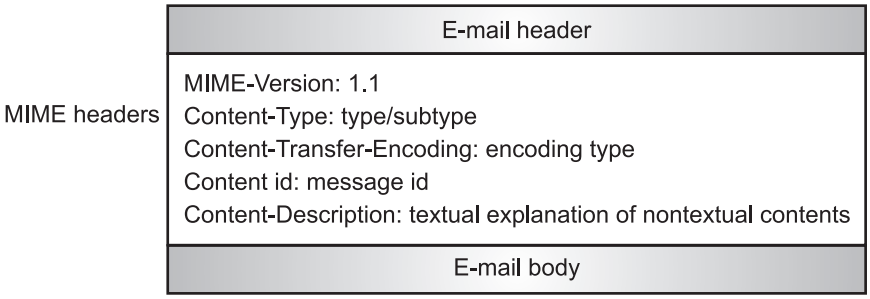


Fig. 1.26: MIME Headers

- MIME headers in Fig. 1.26 are explained below:
  1. **MIME-Version** header defines version of MIME protocol. It must have the parameter value 1.1, which indicates that message is formatted using MIME.
  2. **Content-Type** header defines type of data used in the body of message. They are of different types like text data (plain, HTML), image, audio content or video content.
  3. **Content-Type-Encoding** header defines the method used for encoding the message into 0s and 1s for transport like 7-bit encoding, 8-bit encoding, Base64 etc.

4. **Content-Id** header is used for uniquely identifying the whole message in a multiple message environment.
5. **Content-Description** header defines whether the body is actually image, video or audio.

1.2.4 Message Transfer Agent: SMTP (April 16, 17, Oct. 17)

- The mail transfer is done by Message Transfer Agents (MTA). To send mail, a system must have client MTA and to receive mail, a system must have server MTA.
- The protocol that defines the communication between MTA client and MTA server is called Simple Mail Transfer Protocol (SMTP).
- SMTP is a TCP/IP protocol that specifies how computers exchange electronic mail. SMTP is used twice, between the sender and the sender's mail server and between the two mail servers.
- Another protocol i.e. POP3 or IMAP4 is needed between the mail server and the receiver.

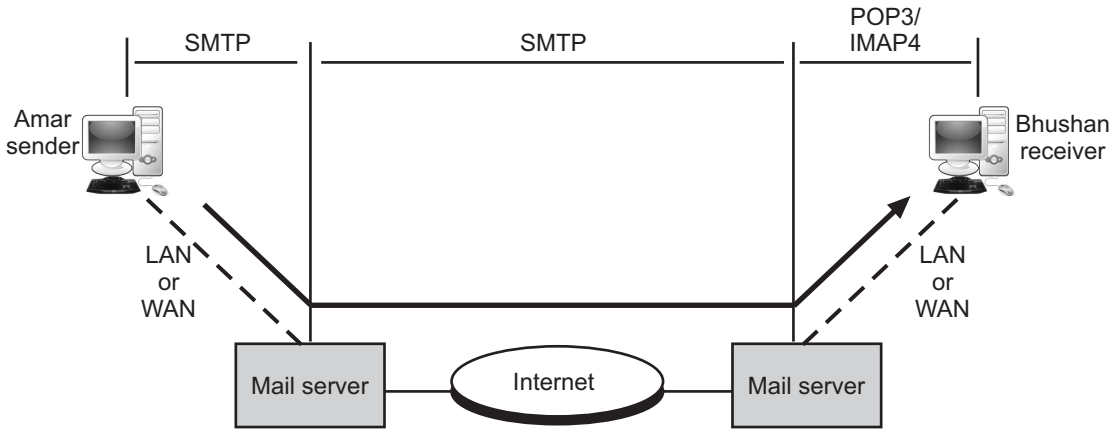


Fig. 1.27: SMTP, POP3 and IMAP4

Commands and Responses:

- SMTP uses commands and response to transfer messages between MTA client and MTA server.

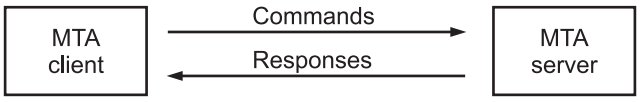


Fig. 1.28: Commands and Responses

- Commands are sent by client to server. Command consists of a keyword followed by zero or more arguments. SMTP uses 14 commands.
- Responses are sent from server to client. A response is a three digit code.
- Table 1.2 shows SMTP commands.

Table 1.2: SMTP Commands

Keyword	Argument (s)
HELO	Sender's host name
MAIL FROM	Sender of the message
RCPT TO	Intended recipient of message
DATA	Body of the mail
QUIT	—
RSET	—
VRFY	Name of recipient to be verified
NOOP	—
TURN	—
EXPN	Mailing list to be expanded
HELP	Command name
SEND FROM	Intended recipient of the message
SMOL FROM	Intended recipient of the message
SMAL FROM	Intended recipient of the message

Table 1.3: SMTP Responses

Code	Description
Positive Completion Reply	
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local, the message will be forwarded
Positive Intermediate Reply	
354	Start mail input
Transient Negative Completion Reply	
421	Service is not available
450	Mail box not available
451	Command aborted: local error
452	Command aborted: insufficient storage

Permanent Negative Completion Reply	
500	Syntax error, unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed, mail box unavailable
551	User not local
552	Requested action aborted, exceeded storage location
553	Requested action not taken, mail box name not allowed
554	Transaction failed.

Mail Transfer Phases:

- Mail transfer occurs in three phases: connection establishment, mail transfer and connection termination.
- Now, let us see the typical SMTP procedure with an example:

```
$ telnet mail.rediffmail.com 25
   Trying 70.168.78.100….
   connected to mail.rediffmail.com (70.168.78.100).
   ===========Connection Establishment===========
      220 mta 13.rediffmail.com SMTP server reday Monday,15 Nov. 2010…
            HELO mail·rediffmail.com
      250 mta 13.rediffmail.com
   ===========Mail Transfer===========
   MAIL FROM: patilra@rediffmail.com
      250 sender <patilra@rediffmail.com> OK
   RCPT TO: Shindesn@rediffmail.com
      250 Recipient <shindesn@rediffmail.com> OK
   DATA
      354 OK send data ending with <CRLF>.<CRLF>
   FROM: Patil RA
   TO: Shinde SN
      Hi, How are you?
   ===========Connection Termiation===========
      250 message received: mail@rediffmail.com
   QUIT
      221 mta 13.rediffmail.com SMTP server closing connection
   Connection closed by foreign host.
```

1.2.5 Message Access Agent: POP3 and IMAP4

- SMTP is used in the first and second stage of mail delivery. SMTP is push protocol, it pushes the message from the client to the server, as shown in Fig. 1.21.
- The third stage needs a pull protocol from receiver to mail server. The third stage uses a message access agent. Now, two message access protocols are available i.e., Post Office Protocol (POP Version 3) and Internet Mail Access Protocol (IMAP Version 4).
- SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) and IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side.
- Fig. 1.29 shows the position of these two protocols in the most common situation (fourth scenario in e-mail).

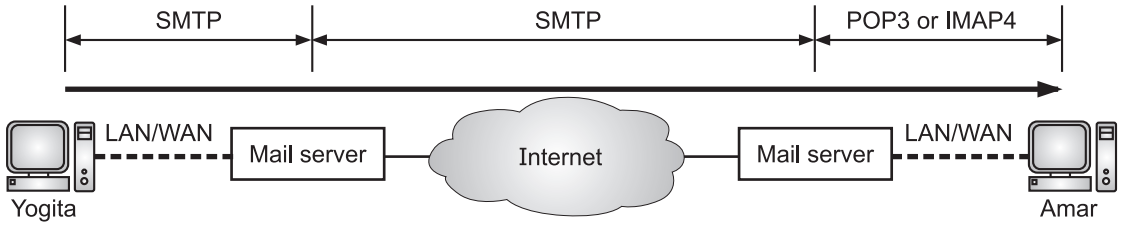


Fig. 1.29

- Let us see POP3 and IMAP4 in detail:

1. POP3:

- Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
- POP supports simple download-and-delete requirements for access to remote mailboxes. A POP3 server listens on well-known port 110.
- Post Office Protocol version 3 (POP3) is simple protocol with limited functionality. The client POP3 software is installed on the recipient, the server POP3 software is installed on the server.
- Mail access starts with the client, when the user wants to access e-mail from the mail server to mail box. Client opens TCP connection on port 110.
- It then sends its user name and password to access the mail box. User can then retrieve the mail messages.
- Fig. 1.30 shows example of downloading using POP3.
- POP3 has two modes, the delete mode and the keep mode. In delete mode, the mail is deleted from the mail box after each retrieval. In the keep mode, the mail remains in the mail box after retrieval.

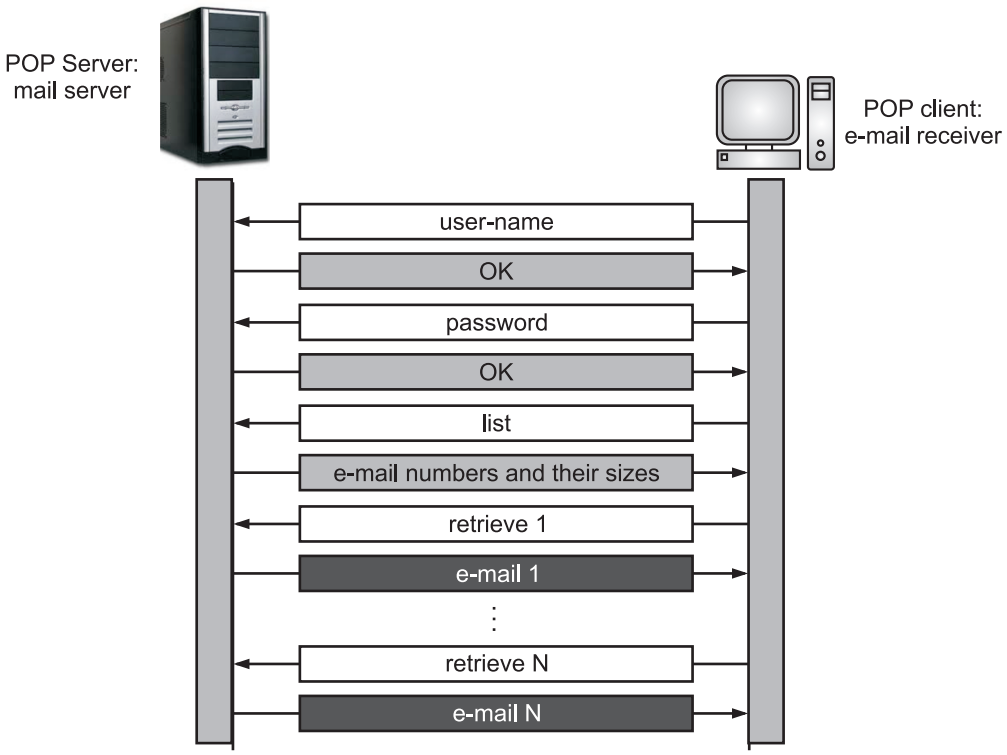


Fig. 1.30: Exchange of Commands and Responses in POP3

2. IMAP4:

- IMAP stands for Internet Mail Access Protocol. It was first proposed in 1986. The current version is Internet Mail Access Protocol, version 4 (IMAP4).
- Another mail access protocol is IMAP4 is similar to POP3 but is more powerful and more complex.
- POP3 not allows the user to organize mail on the server, the user cannot have different folders on the server.
- POP3 also does not allow the user to partially check the content of mail before downloading. All these drawbacks are overcome in IMAP4.
- IMAP4 provides following functions:
  - (i) User can check e-mail header before downloading.
  - (ii) User can search the contents of the e-mail for a specific string of characters before downloading.
  - (iii) User can partially download e-mail.
  - (iv) A user can create, delete or rename mailboxes on the mail server.
  - (v) User can create a hierarchy of mailboxes in a folder for storage.

Comparison between POP and IMAP:

Sr. No.	POP	IMAP
1.	Generally used to support single client.	Designed to handle multiple clients.
2.	Messages are accessed offline.	Messages are accessed online although it also supports offline mode.
3.	POP does not allow search facility.	It offers ability to search emails.
4.	All the messages have to be downloaded.	It allows selective transfer of messages to the client.
5.	Only one mailbox can be created on the server.	Multiple mailboxes can be created on the server.
6.	Not suitable for accessing non-mail data	Suitable for accessing non-mail data i.e. attachment.
7.	POP commands are generally abbreviated into codes of three or four letters. Example: STAT.	IMAP commands are not abbreviated, they are full. Example: STATUS.
8.	It requires minimum use of server resources.	Clients are totally dependent on server.
9.	Mails once downloaded cannot be accessed from some other location.	Allows mails to be accessed from multiple locations.
10.	The e-mails are not downloaded automatically.	Users can view the headings and sender of e-mails and then decide to download.
11.	POP requires less internet usage time.	IMAP requires more internet usage time.

1.3 FILE TRANSFER

- Transferring files from one computer to another is one of important task of network/internetworks.
- The greatest volume of data exchange in the Internet today is due to file transfer. For transferring file over a computer network the File Transfer Protocol (FTP) is used.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another in a computer network or Internet.

1.3.1 FTP

- FTP stands for File Transfer Protocol. FTP is the standard mechanism provided by TCP/IP for copying (transferring) a file from one host to another.
- FTP can transfer files between any computers that have an Internet connection, and also works between computers using totally different operating systems.
- Transferring files from a client computer to a server computer is called "uploading" and transferring from a server to a client is "downloading".

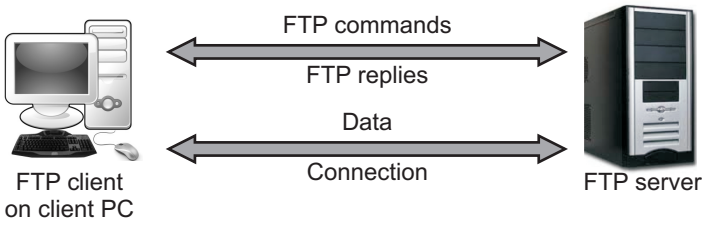


Fig. 1.31: Function of FTP

- While transferring files from one system to another, several problems can be arises, e.g. two systems may use different file name conventions, two systems may have different ways to represent text and data.
- They may have different directory structures etc. All these compatibility problems are solved by FTP.
- FTP is a client/server application. FTP establishes two connections between hosts. One connection for data transfer and other for control information (commands and responses).
- FTP uses the services of TCP. It needs two TCP connections. The well known port 21 is used for the control connection and the well known port 20 is used for data connection.
- Fig. 1.32 shows the basic model of FTP.
- The client has following three components:
  1. User interface.
  2. Client control process.
  3. Data transfer process.
- The server has following two components:
  1. Control process.
  2. Data transfer process.
- Control connection is made between control processes and data connection is made between data transfer processes. First control connection is established and then data connection.
- While the control connection is open, data connection can be opened and closed many times if numbers of files are transferred.

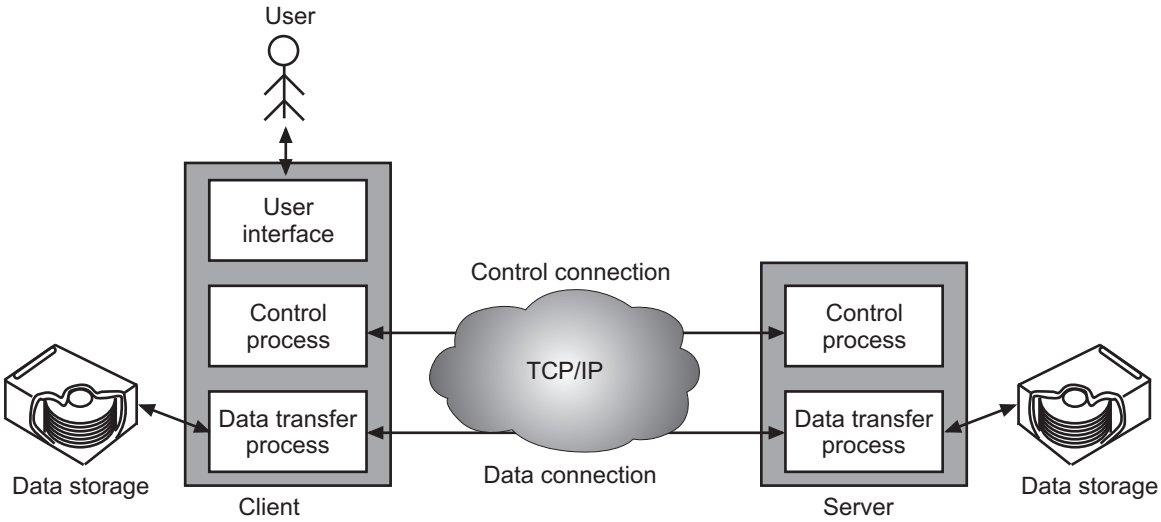


Fig. 1.32: Basic Model of FTP

- Communication with an FTP server is done through two connections, a control connection, and a data connection.
- FTP uses two well-known TCP ports for connections Port 21 is used for the control connection and port 20 is used for the data connection.

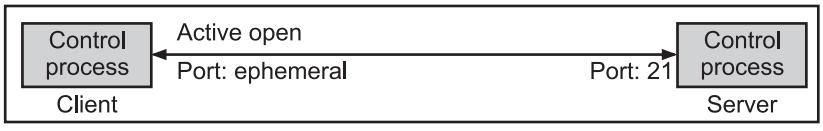
1.3.1.1 Control Connection

- There are following two steps for control connection:

  Step 1: The server issues a passive open on the well-known port 21 and waits for a client.

  Step 2: The client uses an ephemeral port and issues an active open.
- The connection remains open during the entire process. The service type, used by the IP protocol, is minimizing delay because this is an interactive connection between a user (human) and a server.
- The user types commands and expects to receive responses without significant delay. Fig. 1.33 shows the initial connection between the server and the client.

(a) First, Passive open by Server



(b) Later, Active open by Client

Fig. 1.33: Opening the Control connection

Communication over Control Connection:

- The control connection is always the first/initial connection established with an FTP server.
- The control connection's purpose is to allow clients to connect and to send commands to the server (and receive server responses).
- FTP uses 7 bit ASCII character set over the control connection. On control connection, communication is achieved through commands and responses.
- Every command or response is one short line, so we need not worry about file format or file structure. Every line is terminated with carriage return and line feed, end of line token.

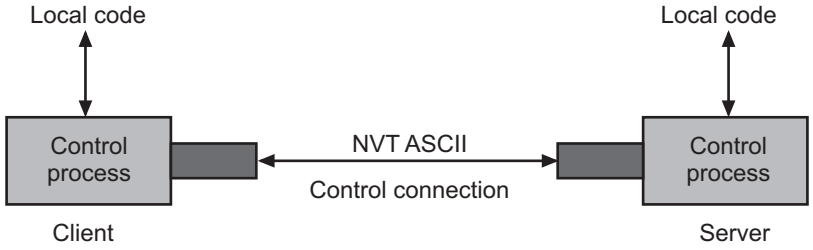


Fig. 1.34: Control Connection

1.3.1.2 Data Connection

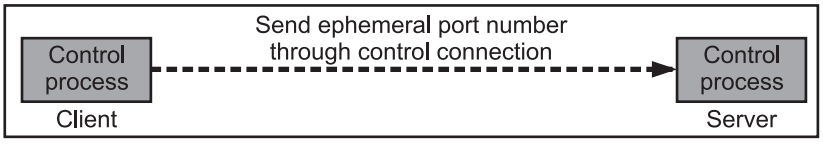
- The data connection uses the well-known port 20 at the server site. However, the creation of a data connection is different from what we have seen so far.
- The following steps shows how FTP creates a data connection:

  Step 1: The client, not the server, issues a passive open using an ephemeral port. This must be done by the client because it is the client that issues the commands for transferring files.

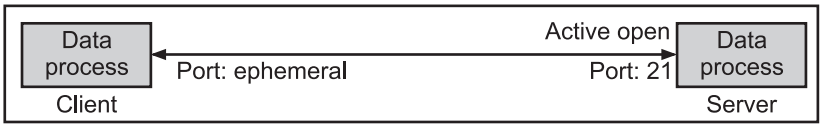
  Step 2: The client sends this port number to the server using the PORT command.

  Step 3: The server receives the port number and issues an active open using the well-known port 20 and the received ephemeral port number.
- The steps for creating the initial data connection are shown in Fig. 1.35.

(a) First, Passive open by Client



(b) Second, Sending of Ephemeral Port



(c) Third, Active open by Server

Fig. 1.35: Creating the Data Connection

Communication over Data Connection:

- Files are transferred using data connection. File transfer over data connection is under the control of control connection.
- File transfer in FTP means, a file is to be copied from server to the client (retrieving a file).
  - A file is to be copied from the client to the server (storing a file).
  - A list of directory or file names is to be sent from server to the client.
- The compatibility problem between client and server must be solved by defining three attributes of communication i.e., File type, Data structure and Transmission mode.

1. File Type: **(Oct. 17)**

- FTP can transfer one of the following types across data connection namely, ASCII file, EBCDIC file or image file.
  (i) The **ASCII file** is default format for transferring text files.
  (ii) If one of two machines uses EBCDIC encoding, the **EBCDIC file** can be transferred using EBCDIC encoding.
  (iii) The **image file** is the default format for transferring binary files.

2. Data Structure: **(Oct. 18)**

- FTP allows three different data structure of a file namely, File structure, Record structure and Page structure.
  (i) File Structure: File has no structure, it is continuous stream of bytes.
  (ii) Record Structure: File is divided into records.
  (iii) Page Structure: The file is divided into pages, each page having page number and page header.

3. Transmission Mode:

- FTP supports three transmission modes: Stream mode, Block mode and Compressed mode.
  (i) Stream Mode: Stream mode is default mode. Data are delivered from FTP to TCP as a continuous stream of bytes.
  (ii) Block Mode: In block mode the data can be delivered from FTP to TCP in blocks.
  (iii) Compressed Mode: If the file is big, data can be compressed using run-length encoding. In compression mode, consecutive appearances of a data unit are replaced by one occurrence and the number of repetitions. In a text file, this is usually spaces (blanks). In a binary file, null characters are usually compressed.

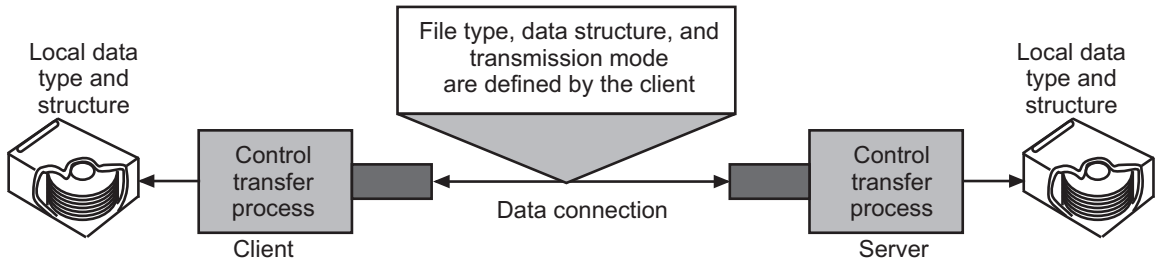


Fig. 1.36: Communication over Data Connection

1.3.2 Command Processing and File Transfer in FTP

- In this section we will study FTP command processing and file transfer.

Command Processing in FTP:

- The FTP command uses the File Transfer Protocol (FTP) to transfer files between the local host and a remote host or between two remote hosts.
- Commands, which are sent from the FTP client control process, are in the form of ASCII uppercase, which may or may not be followed by an argument.
- We can roughly divide the commands into six groups namely, access commands (USER, PASS, QUIT etc.), file management commands (RNTO, SMNT, LIST, CWD etc.), data formatting commands (TYPE, MODE etc.), port defining commands (PORT, PSAV etc.), file transferring commands (RETR, STOR, ALLO, STAT), and miscellaneous commands (HELP, SITE, SYST etc.).
- FTP uses the control connection to establish a communication between the client control process and the server control process.
- During this communication, the commands are sent from the client to the server and the responses are sent from the server to the client as shown in Fig. 1.37.

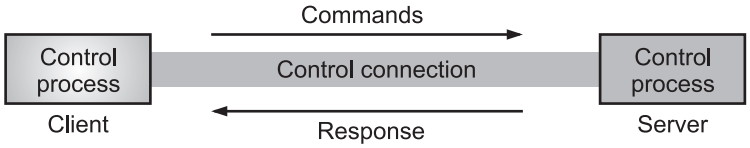


Fig. 1.37: Command processing in FTP

File Transfer in FTP:

- In FTP the file transfer occurs over the data connection under the control of the commands sent over the control connection.
- However, we should remember that file transfer in FTP means one of following three things (Refer Fig. 1.38):
  - A file is to be copied from the server to the client (download). This is called retrieving a file. It is done under the supervision of the RETR command.
  - A file is to be copied from the client to the server (upload). This is called storing a file. It is done under the supervision of the STOR command.

- A list of directory or file names is to be sent from the server to the client. The FTP treats a list of directory or file names as a file. It is sent over the data connection.

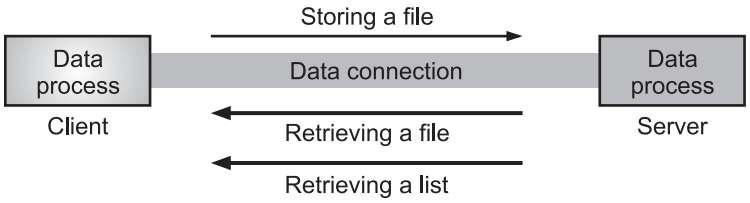


Fig. 1.38: File Transfer in FTP

1.3.3 Anonymous FTP

- To use FTP, a user needs account and password on the remote server. Anonymous FTP allows users without having account on server. Some sites have a set of files available for public access, to enable anonymous FTP.
- To access these files, user need not have account, he can use anonymous as user name and guest as the password.

PRACTICE QUESTIONS

Q.I Multiple Choice Questions:

1. Which is the top most layer in OSI model and TCP/IP model?
   (a) Session (b) Physical
   (c) Application (d) Transport
2. Consider following different activities related to email:
   m1: Send an email from a mail client to a mail server.
   m2: Download an email from mailbox server to a mail client.
   m3: Checking email in a web browser.
   Which is the application level protocol used in each activity?
   (a) m1: HTI m2: SMTP m3 POP (b) m1 SMTP m2: FTP m3: HTTP
   (c) m1: SMTP m2 POP m3: HTTP (d) m1. POP m2 SMTP m3 IMAP
3. What is the maximum size of data that the application layer can pass on to the TCP layer below?
   (a) Any Size (b) 2^{16} bytes- size of TCP header
   (c) 2^{16} bytes (d) 1500 bytes
4. Identify the correct order in which the following actions take place in an interaction between a web browser and a web server.
   (i) The web browser requests a webpage using HTTP.
   (ii) The web browser establishes a TCP connection with the web server.
   (iii) The web server sends the requested webpage using HTTP.

(iv) The web browser resolves the domain name using DNS.

(a) (iv), (ii), (i), (iii) (b) (i), (ii), (iii), (iv)

(c) (iv), (i), (ii), (iii) (d) (ii), (iv), (i), (iii)

5. Which is not an application layer protocol?

(a) HTTP (b) SMTP

(c) FTP (d) TCP

6. The packet of information at the application layer is called as,

(a) Packet (b) Message

(c) Segment (d) Frame

7. Application layer offers following which service,

(a) end to end (b) process to process

(c) Both (a) and (b) (d) None of the mentioned

8. E-mail is,

(a) Loss-tolerant application (b) Bandwidth-sensitive application

(c) Elastic application (d) None of the mentioned

9. Which of the following is an application layer service?

(a) Transport layer protocol (b) Maximum buffer size

(c) Both (a) and (b) (d) None of the mentioned

10. Pick the odd one out,

(a) File transfer (b) File download

(c) E-mail (d) Interactive games

11. Which of the following is an application layer service?

(a) Network virtual terminal (b) File transfer, access, and management

(c) Mail service (d) All of the mentioned

12. To deliver a message to the correct application program running on a host, the _____ address must be consulted.

(a) IP (b) MAC

(c) Port (d) None of the mentioned

13. Which is a time-sensitive service?

(a) File transfer (b) File download

(c) E-mail (d) Internet telephony

14. Transport services available to applications in one or another form,

(a) Reliable data transfer (b) Timing

(c) Security (d) All of the mentioned

15. Electronic mail uses which Application layer protocol?

(a) SMTP (b) HTTP

(c) FTP (d) SIP

16. The_____ translates internet domain and host names to IP address.
    (a) Domain Name System (DNS) (b) routing information protocol
    (c) network time protocol (d) internet relay chat
17. Which one of the following allows a user at one site to establish a connection to another site and then pass keystrokes from local host to remote host?
    (a) HTTP (b) FTP
    (c) IMAP (d) TCP
18. Application layer protocol defines,
    (a) types of messages exchanged
    (b) message format, syntax and semantics
    (c) rules for when and how processes send and respond to messages
    (d) All of the mentioned
19. Which one of the following protocol delivers/stores mail to receiver server?
    (a) SMTP (b) POP
    (c) IMAP (d) HTTP
20. The ASCII encoding of binary data is called as,
    (a) base 64 encoding (b) base 32 encoding
    (c) base 16 encoding (d) base 8 encoding
21. Which one of the following is an internet standard protocol for managing devices on IP network?
    (a) DHCP (b) SNMP
    (c) IMAP (d) HTTP
22. Which one of the following is not an application layer protocol?
    (a) media gateway protocol (b) dynamic host configuration protocol
    (c) resource reservation protocol (d) session initiation protocol
23. Which protocol is a signaling communication protocol used for controlling multimedia communication sessions?
    (a) Session initiation protocol (b) Session modelling protocol
    (c) Session maintenance protocol (d) Resource reservation protocol
24. Which one of the following is not correct?
    (a) Application layer protocols are used by both source and destination devices during a communication session
    (b) HTTP is a session layer protocol
    (c) TCP is an application layer protocol
    (d) All of the mentioned

25. When displaying a web page, the application layer uses the,
    (a) HTTP protocol (b) FTP protocol
    (c) SMTP protocol (d) TCP protocol
26. HTTP is _____ protocol.
    (a) application layer (b) transport layer
    (c) network layer (d) data link layer
27. Multiple objects can be sent over a TCP connection between client and server in a persistent HTTP connection.
    (a) True (b) False
28. In the network HTTP resources are located by,
    (a) Uniform Resource Identifier (URL) (b) Unique resource locator
    (c) Unique resource identifier (d) Union resource locator
29. HTTP client requests by establishing a _____ connection to a particular port on the server.
    (a) UDP (b) TCP
    (c) BGP (d) DHCP
30. In HTTP pipelining,
    (a) multiple HTTP requests are sent on a single TCP connection without waiting for the corresponding responses
    (b) multiple HTTP requests can not be sent on a single TCP connection
    (c) multiple HTTP requests are sent in a queue on a single TCP connection
    (d) multiple HTTP requests are sent at random on a single TCP connection
31. FTP server listens for connection on port number,
    (a) 20 (b) 21
    (c) 22 (d) 23
32. In FTP protocol, client contacts server using _____ as the transport protocol.
    (a) TCP (b) UDP
    (c) DHCP (d) SCTP
33. In Active mode FTP, the client initiates both the control and data connections.
    (a) True (b) False
34. The File Transfer Protocol is built on,
    (a) data centric architecture (b) service oriented architecture
    (c) client server architecture (d) connection oriented architecture
35. In File Transfer Protocol, data transfer cannot be done in,
    (a) stream mode (b) block mode
    (c) compressed mode (d) message mode

36. The entire hostname has a maximum of,
    (a) 255 characters (b) 127 characters
    (c) 63 characters (d) 31 characters
37. A DNS client is called as,
    (a) DNS updater (b) DNS resolver
    (c) DNS handler (d) None of the mentioned
38. Servers handle requests for other domains,
    (a) directly (b) by contacting remote DNS server
    (c) not possible (d) None of the mentioned
39. DNS database contains,
    (a) name server records (b) hostname-to-address records
    (c) hostname aliases (d) All of the mentioned
40. If a server has no clue about where to find the address for a hostname then,
    (a) server asks to the root server (b) server asks to its adjacent server
    (c) request is not processed (d) none of the mentioned
41. Which one of the following allows client to update their DNS entry as their IP address change?
    (a) dynamic DNS (b) mail transfer agent
    (c) authoritative name server (d) None of the mentioned
42. Wildcard domain names start with label,
    (a) @ (b) *
    (c) & (d) #
43. The right to use a domain name is delegated by domain name registers which are accredited by,
    (a) internet architecture board
    (b) internet society
    (c) internet research task force
    (d) internet corporation for assigned names and numbers
44. The domain name system is maintained by,
    (a) distributed database system (b) a single server
    (c) a single computer (d) None of the mentioned
45. Which one of the following is not true?
    (a) multiple hostnames may correspond to a single IP address
    (b) a single hostname may correspond to many IP addresses
    (c) a single hostname may correspond to a single IP address
    (d) None of the mentioned

46. When the mail server sends mail to other mail servers it becomes,
    (a) SMTP server (b) SMTP client
    (c) Peer (d) Master
47. If we have to send multimedia data over SMTP it has to be encoded into,
    (a) Binary (b) Signal
    (c) ASCII (d) Hash
48. In SMTP, the command to write receiver's mail address is written with the command,
    (a) SEND TO (b) RCPT TO
    (c) MAIL TO (d) RCVR TO
49. Simple mail transfer protocol (SMTP) utilizes _____ as the transport layer protocol for electronic mail transfer.
    (a) TCP (b) UDP
    (c) DCCP (d) SCTP
50. SMTP uses which of the following TCP port?
    (a) 22 (b) 23
    (c) 21 (d) 25
51. Which is a symbolic string associated with an IP address?
    (a) Domain Name (b) Domain Name
    (c) Domain Address Name (d) None of the mentioned
52. Which contains the DNS database?
    (a) Name host (b) Name client
    (c) Name server (d) None of the mentioned
53. Which is collection of nodes (sub domains) under the main domain?
    (a) Server (b) Zone
    (c) Domain (d) Address
54. Which allows us to send the message in electronic mode over the internet?
    (a) SMS (b) email
    (c) MMS (d) DNS
55. The domain name space is divided into,
    (a) generic domains (b) country domains
    (c) inverse domain (d) All of the mentioned
56. MIME is acronym of,
    (a) Multipurpose Internet Mail Extensions
    (b) Multiple Internet Mail Extensions
    (c) Multipurpose Intranet Mail Extensions
    (d) All of the mentioned

57. Which is an application-layer Internet standard protocol used by e-mail clients to retrieve e-mail from a mail server?
    (a) SMTP (b) HTTP
    (c) POP (d) FTP
58. Which address is a unique logical address assigned to a machine over the computer network?
    (a) IP (b) TCP
    (c) UDP (d) HTTP
59. DNS generic domain contains,
    (a) .com (commercial) (b) .edu (educational)
    (c) .org (organization) (d) All of the mentioned
60. Which domains use two characters country abbreviations (e.g. au for Australia)?
    (a) generic domains (b) country domains
    (c) inverse domain (d) All of the mentioned
61. DNS response message consists of,
    (a) a header, question records (b) answer records, authoritative records
    (c) additional records (d) All of the mentioned
62. IMAP is an internet protocol that works on managing and retrieving emails on the _____ server from a local client.
    (a) local (b) remote
    (c) Both (a) and (b) (d) None of the mentioned
63. Which protocol is used for receiving emails from remote servers?
    (a) POP3 (b) IMAP4
    (c) FTP (d) SMTP
64. Which provides services to user in email?
    (a) End Agent (EA) (b) End User (EU)
    (c) User Agent (UA) (d) None of the mentioned
65. MIME headers are, and?
    (a) MIME-Version, Content-Type, (b) Content-Type-Encoding, Content-Id
    (c) Content-Description (d) All of the mentioned
66. The mail transfer is done by,
    (a) message transfer users (b) message transfer addresses
    (c) message transfer agents (d) None of the mentioned
67. Which protocol is the standard mechanism provided by TCP/IP for copying (transferring) a file from one host to another?
    (a) FTP (b) TCP
    (c) SMTP (d) MIME

Answers

1. (c)	2. (c)	3. (a)	4. (a)	5. (d)	6. (b)	7. (a)	8. (c)	9. (c)	10. (d)
11. (d)	12. (c)	13. (d)	14. (d)	15. (a)	16. (a)	17. (c)	18. (d)	19. (a)	20. (a)
21. (b)	22. (c)	23. (a)	24. (d)	25. (a)	26. (a)	27. (a)	28. (a)	29. (b)	30. (a)
31. (b)	32. (a)	33. (b)	34. (c)	35. (d)	36. (a)	37. (b)	38. (b)	39. (d)	40. (a)
41. (a)	42. (b)	43. (d)	44. (a)	45. (c)	46. (b)	47. (c)	48. (b)	49. (a)	50. (d)
51. (a)	52. (c)	53. (b)	54. (b)	55. (d)	56. (a)	57. (c)	58. (a)	59. (d)	60. (b)
61. (d)	62. (b)	63. (a)	64. (c)	65. (d)	66. (c)	67. (a)			

Q.II Fill in the Blanks:

1. _____ is a client/server application program used to help other application programs and to map a host name in the application layer to an IP address in the network layer.
2. _____ provides unique identification and source to destination delivery for a host on the Internet.
3. A FQDN is the complete _____ for a specific computer, or host, on the Internet.
4. _____ is responsible for creating, maintaining and updating the zone file.
5. FTP used for transmitting the files from one _____ to another.
6. DNS has two types of messages namely _____ and _____.
7. The DNS server responds with the IP _____ of the desired file transfer server.
8. Communication with an FTP server is done through two connections, a _____ connection and _____ connection.
9. FTP uses two well-known TCP ports for connections port _____ is used for the control connection and port _____ is used for the data connection.
10. The _____ mode is default mode of FTP.
11. Identification is a _____ bit field used by the client to match the response with the query.
12. The first component of e-mail system is _____.
13. The process of DNS _____ involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1).
14. _____ is an Internet standard that extends the format of email messages to support text in character sets other than ASCII, as well as attachments of audio, video, images, and application programs.
15. _____ uses commands and response to transfer messages between MTA client and MTA server.
16. The DNS is a system used to convert a computer's _____ name into an IP address on the Internet.

17. The domain name space of the Internet is organized into a hierarchical layout of sub-domains below the DNS _____ domain.
18. FTP uses 7 bit ASCII _____ set over the control connection.
19. The _____ domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients.
20. DNS is a client/server network communication protocol in which DNS clients send _____ to the server while DNS servers send responses to the client.
21. FTP is the protocol that actually lets us to transfer _____.
22. _____ uses two sets of characters, one for data and one for control.
23. A DNS _____ is responsible for initiating and sequencing the queries that ultimately lead to a full resolution (translation) of the resource sought, e.g., translation of a domain name into an IP address.
24. _____ FTP allows users without having account on server.
25. The _____ layer provide user interfaces and support for services such as DNS, e-mail, remote file access and transfer, access to system resources etc. services.
26. _____ address (32-bit) is a unique logical address assigned to a machine over the network.
27. _____ refers to a web address which uniquely identifies a document over the Internet.
28. Name server contains the DNS _____.
29. _____ is a TCP/IP protocol that specifies how computers exchange electronic mail.
30. _____ is collection of nodes (sub domains) under the main domain.
31. _____ servers and other message transfer agents use SMTP to send and receive mail messages.
32. _____ server is the top level server which consists of the entire DNS tree.
33. The _____ connection is always the first/initial connection established with an FTP server.
34. A _____ that maps each address to a unique name can be organized in two ways: flat or hierarchical.
35. Each node in the tree has a _____ (a string with a maximum of 63 characters).
36. If a label is not terminated by a _____ string, it is called a Partially Qualified Domain Name (PQDN).
37. Mapping a name to an address or an address to a name is called name address _____.
38. The protocol that defines the communication between MTA client and MTA server is called _____.

39. _____ is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
40. In FTP the file transfer occurs over the _____ connection under the control of the commands sent over the control connection.
41. _____ is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection.
42. The server maintains a database called _____ for every zone.

Answers

1. DNS	2. network layer	3. domain name	4. Primary server
5. host	6. query, response	7. address	8. control, data
9. 20, 21	10. Stream	11. 16	12. User Agent (UA)
13. resolution	14. MIME	15. SMTP	16. host
17. root	18. character	19. inverse	20. requests
21. files	22. NVT	23. resolver	24. Anonymous
25. application	26. IP	27. URL	28. database
29. SMTP	30. Zone	31. Mail	32. Root
33. control	34. name space	35. label	36. null
37. resolution	38. SMTP	39. POP3	40. data
41. IMAP	42. zone file		

Q.III State True or False:

1. The generic domains define registered host according to their generic behavior.
2. The names assigned to machines can be carelessly selected.
3. DNS has two types of messages with different formats.
4. In a time-sharing environment, all of the processing must be done by the central computer.
5. MIME uses more than one TCP connections.
6. Question section consisting of one or more resource records.
7. IMAP is a TCP/IP protocol that specifies how computers exchange electronic mail.
8. FTP is the standard mechanism provided by TCP/IP for copying (transferring) a file from one host to another.
9. HTTP works as a combination of FTP and TCP.
10. A web browser can be used to upload or download files on FTP servers.
11. DNS translates human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example, 192.0.2.44).
12. MIME enables its users to exchange several kinds of data files over the Internet, including images, audio, and video.

13. Primary Server stores a file about its zone. It has authority to create, maintain, and update the zone file.
14. IMAP is a protocol used to log in to local computer on the internet.
15. The data connection of FTP uses the well-known port 20 at the server site.
16. Primary Server transfers complete information about a zone from another server which may be primary or secondary server.
17. Domain Name is a symbolic string associated with an IP address. A full domain name is a sequence of labels separated by dots (.).
18. If a label is terminated by a null string, it is called a Fully Qualified Domain Name (FQDN).
19. The NVT is a virtual device which maps the local terminal characteristics to a well-defined NVT interface.
20. IMAP supports three transmission modes namely, Stream mode, Block mode and Compressed mode.
21. In FTP through control connection, we can transfer a line of command or line of response at a time.
22. The mail transfer is done by Message Transfer Agents (MTA). To send mail, a system must have client MTA and to receive mail, a system must have server MTA.
23. The FTP is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
24. FTP is a client/server application.
25. The domain name itself consists of the label, concatenated with the name of its parent node on the right, separated by a dot.
26. Domain name resolvers determine the domain name servers responsible for the domain name in question by a sequence of queries starting with the right-most (top-level) domain label.
27. The domain name space is a hierarchy has multiple levels (from 0 to 127), with a root at the top.
28. When a host requires mapping of name to an address or an address to a name, it calls DNS client called a resolver.
29. POP3 used to support single client.
30. Multipurpose Internet Mail Extensions (MIME) is a protocol that allows non-ASCII data to be sent through e-mail.
31. The query message consists of a header and question records.
32. The current version of IMAP is Internet Mail Access Protocol, version 4 (IMAP4).
33. SMTP is push protocol it pushes the message from the client to the server.
34. FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another in a computer network or Internet.

35. In compressed mode the data can be delivered from FTP to TCP in blocks.
37. DNS resolver sends a request to the DNS server to obtain the IP address of a hostname.

Answers

1. (T)	2. (F)	3. (F)	4. (T)	5. (F)	6. (F)	7. (F)	8. (T)	9. (F)	10. (T)
11. (T)	12. (T)	13. (T)	14. (F)	15. (T)	16. (F)	17. (T)	18. (T)	19. (T)	20. (F)
21. (T)	22. (T)	23. (F)	24. (T)	25. (T)	26. (T)	27. (T)	28. (T)	29. (T)	30. (T)
31. (T)	32. (T)	33. (T)	34. (T)	35. (F)	36. (T)	37. (T)			

Q.IV Answer the following Questions:

(A) Short Answer Questions:

1. What is DNS?
2. Define domain.
3. Give the purpose of DNS.
4. What is the function of POP3?
5. What is name space?
6. What are FQDN and PQDN?
7. Define zone.
8. What is root server?
9. List types of domains.
10. Define resolution.
11. What is caching?
12. What is the purpose of UA?
13. List MIME headers.
14. What is SMTP?
15. Give role of FTP.
16. List modes for FTP.
17. List types of name space.
18. What is anonymous FTP?
19. Give need for MIME.
20. What is email?
21. What is the purpose of IMAP?

(B) Long Answer Questions:

1. Define DNS? How it works? Explain in detail.
2. What is name space? Describe flat name space and hierarchical name space.
3. Write short note on: DNS in internet.

4. What is User Agent? Describe the services provided by user agent.
5. What is the function of MIME? Explain MIME headers diagrammatically.
6. Explain message transfer agent SMTP in detail.
7. With the help of example describe generic, country and inverse domains.
8. What is FTP? How does communication takes place over control connection and over data connection?
10. Explain architecture of email with different scenarios.
11. What is anonymous FTP?
12. Explain MTA POP and IMAP in detail. Also compare them.
13. Explain the format of e-mail diagrammatically.
14. Write a note on: FTP transmission modes.
15. Explain the terms label, domain name, zone, name space related to DNS.

UNIVERSITY QUESTIONS AND ANSWERS

April 2016

1. Write a short note on SMTP. **[5 M]**

Ans. Refer to Section 1.2.4.

2. Discuss DNS in detail. **[5 M]**

Ans. Refer to Section 1.1.

April 2017

1. What is generic domain? **[1 M]**

Ans. Refer to Section 1.1.4, Point (1).

2. Write a short note on SMTP. **[5 M]**

Ans. Refer to Section 1.2.4.

October 2017

1. Which file types can be transferred on FTP? **[1 M]**

Ans. Refer to Section 1.3.1.2, Point (1).

2. Write a short note on SMTP. **[5 M]**

Ans. Refer to Section 1.2.4.

April 2018

1. What is DNS? **[1 M]**

Ans. Refer to Section 1.1.

October 2018

1. What are the different data structures supported by FTP? **[1 M]**

Ans. Refer to Section 1.3.1.2, Point (2).

2. What is address resolution? Explain recursive and iterative resolution in DNS. **[5 M]**

Ans. Refer to Section 1.1.5.

April 2019

1. What is address resolution? **[1 M]**

Ans. Refer to Section 1.1.5.

2. What are the services provided by user agent? **[5 M]**

Ans. Refer to Section 1.2.1.

3. Explain hierarchical name space. **[5 M]**

Ans. Refer to Section 1.1.1, Point (2).

❖❖❖

CHAPTER 2

Multimedia

Objectives...

- To understand Basic Concepts of Multimedia
- To learn Streaming Stored Audio/Video
- To study RTP, RTCP etc.
- To learn Streaming Live Audio/Video
- To learn VoIP with SIP and H.323

2.0 INTRODUCTION

- Multimedia has become an extremely powerful field in today's computer and mobile environments due to their myriad use.
- The word multimedia, originating from the Latin word 'multus (means numerous or many)' and 'medium (means middle or center)'.
- Multimedia means combination of multiple media contents like text, video, audio, images, animation and interactive media.
- The word multimedia combination of two words, 'multi and media'. The word 'multi' means many and the word 'media' (plural of medium) means A pathway or communication channel through which information can be transmitted or send.
- Multimedia is technology concerned with the computer controlled integration of text, graphics, still and moving images (video), animation, audio, and any other media where every type of information can be represented, stored, transmitted and processed digitally.
- Multimedia is a media that uses multiple forms of interactive content (text, audio, video, graphic, animation etc.) and information processing.
- Multimedia is the seamless integration of text, audio, video, images and animation within a single digital information environment.
- Major components of a multimedia computer system includes **Text** (visual expression of alphanumeric letters, numbers and symbols used to communicate ideas and information to others through a human language system), **Graphics** (to generate, represent, process, manipulate and display photographs, clipart, illustrations, pictures, other types of still images), **Animation** (process of making a static image look like it is moving), **Audio or Sound** (refers to the aural content created through the electronic

capture and reproduction of sound), **Video** (refers to the moving pictures with sound such as a picture in television).

- Multimedia is applied in the different fields like Digital Library, E-learning, Movie making, Animated Films, E-shopping, Video games, Video conferencing and so on.
- We can divide audio and video services into three broad categories namely streaming stored audio/video, streaming live audio/video, and interactive audio/video.
- Streaming means a user can listen (or watch) the file after the downloading has started. Streaming refers to any media content such as live or recorded - delivered to computers and mobile devices via the Internet and played back or listen in real time.
- Streaming stored audio/video refers to on-demand requests for compressed audio/video files. Streaming live audio/video refers to the broadcasting of radio and TV programs through the Internet. Interactive audio/video refers to the use of the Internet for interactive audio/video applications.

2.1 DIGITIZING AUDIO AND VIDEO

- Digital audio or sound is used to record, store, manipulate, generate and reproduce sound using audio signals that have been encoded in digital form. In simple word, the sound used in multimedia application is digital audio.
- Digital video is a representation of moving visual images (video) using a digital video signals that have been encoded in digital form.
- Both audio and video are used to enhance the multimedia applications in various ways. Before audio or video signals can be sent or transmitted on the Internet, they need to be digitized.

Digitizing Audio:

- Audio or sound is a physical phenomenon produced by the vibration of matter such as a violin string, a hand clapping etc.
- As the matter vibrates, the neighboring molecules in the air vibrate in the form of wave. When such a wave reaches a human ear and heard the sound.
- When sound is fed into a microphone, an electronic analog signal is generated that represents the sound amplitude as a function of time. The signal is called an analog audio signal.
- An analog signal like audio can be digitized to produce a digital signal. According to the Nyquist theorem, if the highest frequency of the signal is f, we need to sample the signal 2f times per second.
- There are other methods for digitizing an audio signal, but the principle is the same. Voice is sampled at 8,000 samples per second with 8 bits per sample and this result in a digital signal of 64 kbps.
- Music is sampled at 44,100 samples per second with 16 bits per sample and this result in a digital signal of 705.6 kbps for monaural and 1.411 Mbps for stereo.

Digitizing Video:

- Video refers to the moving picture, accompanied by sound such as a picture in television. A video consists of a sequence of frames.
- If the frames are displayed on the screen fast enough, we get an impression of motion. The reason is that our eyes cannot distinguish the rapidly flashing frames as individual ones.
- There is no standard number of frames per second; in North America 25 frames per second is common. However, to avoid a condition known as flickering, a frame needs to be refreshed.
- The TV industry repaints each frame twice. This means 50 frames need to be sent, or if there is memory at the sender site, 25 frames with each frame repainted from the memory.
- Each frame is divided into small grids, called picture elements or pixels. For black-and-white TV, each 8-bit pixel represents one of 256 different gray levels.
- For a color TV, each pixel is 24 bits, with 8 bits for each primary color (RGB (Red, Green and Blue)).
- We can calculate the number of bits in a second for a specific resolution. In the lowest resolution a color frame is made of 1,024 × 768 pixels. This means that we need,

  $2 \times 25 \times 1{,}024 \times 768 \times 24 = 944$ Mbps
- Above data rate needs a very high data rate technology such as SONET (Synchronous Optical NETwork). To send video using lower-rate technologies, we need to compress the video.

2.1.1 Audio and Video Compression

- In multimedia to send audio or video over the Internet requires compression. Before learning the audio compression and video compression let us, first understand the concept of data compression.
- One of the most evident and important challenges of using multimedia is the necessity to compress data. Data compression is the art or science of representing information in a compact form.
- Compression is a reduction in the number of bits needed to represent data. Compressing data can save storage capacity, speed file transfer, and decrease costs for storage hardware and network bandwidth.
- The data in the form of text, audio, video, images, animation and so on. The reason we need data compression is that more and more of information that we generate and use in digital form.
- Data compression is the process of modifying, encoding or converting the bits structure of data in such a way that it consumes less space on disk.

- Compression is used to save disk space and reduce the time needed to transfer files over the Internet. Any particular compression is either lossy or lossless.
- Lossy compression involves some loss of information and the data that can be compressed using lossy compression cannot be recovered or restored to its original form.
- Lossless compression involves no loss of information. If the data have been losslessly compressed, the original data can be recovered or restore exactly from the compressed data.

Audio Compression:

- Uncompressed audio is bulky and number of time not appropriate for transmission over network. Audio compression is a technique used to compress audio signals based on signal processing of audio sequences.
- Audio compression can be used for speech or music. For speech, we need to compress a 64-kHz digitized signal; for music, we need to compress a 1.411-MHz signal.
- Audio data compression has the potential to reduce the storage requirement and transmission bandwidth of audio signals.
- Audio compression is a form of data compression designed to reduce the size of audio data files.
- Audio data compression in which the amount of data in a recorded waveform is reduced for transmission. This is used in MP3 encoding, internet radio, and so on.
- Encoding is the process of converting a stream of uncompressed digital audio to a compressed format.
- Following are the two categories of techniques are used for audio compression:
  1. **Predictive Encoding:** In this encoding, the differences between the samples are encoded instead of encoding all the sampled values. Predictive encoding compression is normally used for speech. Several standards have been defined such as GSM (13 kbps), G.729 (8 kbps), and G.723.3 (6.4 or 5.3 kbps).
  2. **Perceptual Encoding (MP3):** Perceptual encoding is the most common compression technique used to create CD-quality audio. This type of audio needs at least 1.411 Mbps; this cannot be sent over the Internet without compression. MP3 (MPEG audio layer 3), a part of the MPEG standard uses perceptual encoding technique. MP3 as a file format commonly designates files containing an elementary stream of MPEG-1 Audio encoded data. Perceptual encoding is based on the science of psychoacoustics, which is the study of how people perceive sound. The idea is based on some flaws in our auditory system: some sounds can mask other sounds. Masking can happen in frequency and time. In frequency masking, a loud sound in a frequency range can partially or totally mask a softer sound in another frequency range. For example, we cannot hear what our dance partner says in a room where a loud heavy metal band is performing. In temporal masking, a loud sound can numb our ears for a short time even after the sound has stopped. MP3 uses both frequency and temporal masking, to compress audio

signals. The technique analyzes and divides the spectrum into several groups. Zero bits are allocated to the frequency ranges that are totally masked. A small number of bits are allocated to the frequency ranges that are partially masked. A larger number of bits are allocated to the frequency ranges that are not masked. MP3 produces three data rates, 96 kbps, 128 kbps, and 160 kbps. The data rate is based on the range of the frequencies in the original analog audio.

Video Compression:

- Video compression is the process of encoding a video file in such a way that it consumes less space than the original file and is easier to transmit over the network or Internet.
- The compressed video must have a much smaller size compared to the uncompressed video. This allows the video to be saved in a smaller file or sent over a network more quickly.
- Video compression is a type of compression technique that reduces the size of video file formats by eliminating redundant and non-functional data from the original video file.
- Video is composed of multiple frames and each frame is one image or picture. We can compress video by first compressing images. Two most common standards in the today's market are JPEG and MPEG.
- JPEG stands for Joint Photographic Experts Group (JPEG) used to compress images. MPEG stands for Moving Picture Experts Group (MPEG) used to compress video.

Image Compression (JPEG):

- Image compression is the process of encoding or converting an image file in such a way that it consumes less storage space than the original file.
- Image compression is the art/science of efficient coding of picture data to reduce the number of bits required to represent an image/picture.
- If the picture is not in color (gray scale), each pixel can be represented by an 8-bit integer (256 levels). If the picture is in color, each pixel can be represented by 24 bits (3 × 8 bits), with each 8 bits representing red, blue, or green (RBG).
- In JPEG, a gray scale picture is divided into blocks of 8 × 8 pixels as shown in Fig. 2.1.

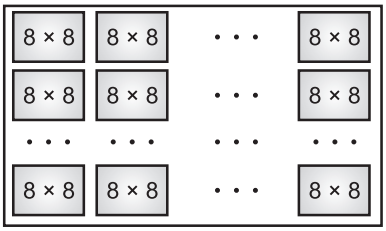


Fig. 2.1: JPEG Gray Scale Image

- The purpose of dividing the picture into blocks is to decrease the number of calculations because, as we will see shortly, the number of mathematical operations for each picture is the square of the number of units.

- The whole idea of JPEG is to change the picture into a linear (vector) set of numbers that reveals the redundancies.
- The important goal of image compression technique is that reduces the size of an image file without affecting or degrading its quality.
- The redundancies (lack of changes) can then be removed by using one of the text compression methods. A simplified scheme of the JPEG process is shown in Fig. 2.2.

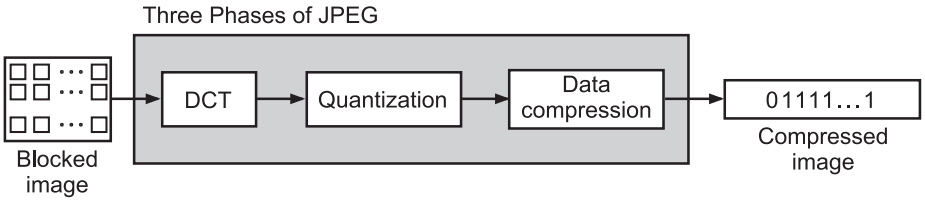


Fig. 2.2: JPEG Process

- Three phases of JPEG process are explained detailed below:

Phase 1: Discrete Cosine Transform (DCT)

- In DCT phase, each block of 64 pixels goes through a transformation. The transformation changes the 64 values so that the relative relationships between pixels are kept but the redundancies are revealed.
- We do not give the formula here, but we do show the results of the transformation for three cases.

  Case 1: In case 1, we have a block of uniform gray, and the value of each pixel is 20. When we do the transformations, we get a nonzero value for the first element (upper left corner); the rest of the pixels have a value of 0. The value of T(0, 0) is the average (multiplied by a constant) of the P(x, y) values and is called the dc value (direct current, borrowed from electrical engineering). The rest of the values, called ac values, in T(m, n) represent changes in the pixel values. But because there are no changes, the rest of the values are 0s as shown in Fig. 2.3.

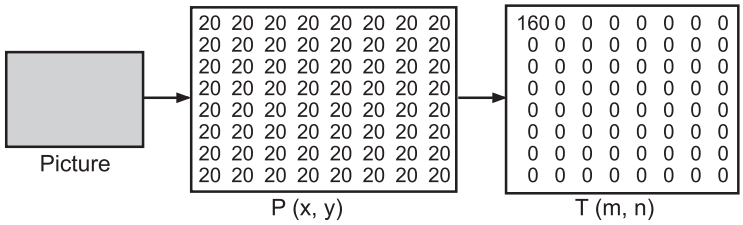


Fig. 2.3: Case 1 (Uniform Gray Scale)

Case 2: In case 2, we have a block with two different uniform gray scale sections. There is a sharp change in the values of the pixels (from 20 to 50). When we do the transformations, we get a dc value as well as nonzero ac values. However, there are only a few nonzero values clustered around the dc value. Most of the values are 0 as shown in Fig. 2.4.

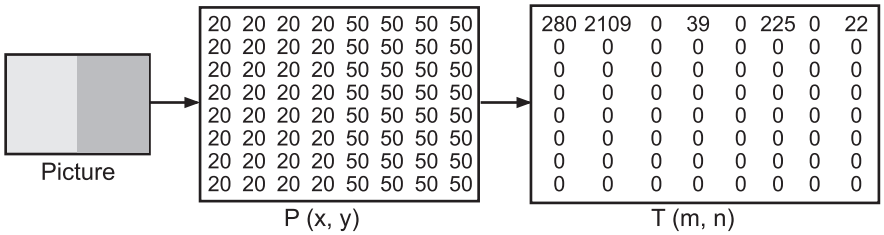


Fig. 2.4: Case 2 (Two Sections)

Case 3: In case 3, we have a block that changes gradually i.e., there is no sharp change between the values of neighboring pixels. When we do the transformations, we get a dc value, with many nonzero ac values also as shown in Fig. 2.5. We can say the following:

- The transformation creates table T from table P.
- The dc value is the average value (multiplied by a constant) of the pixels.
- The ac values are the changes.
- Lack of changes in neighboring pixels creates 0s.

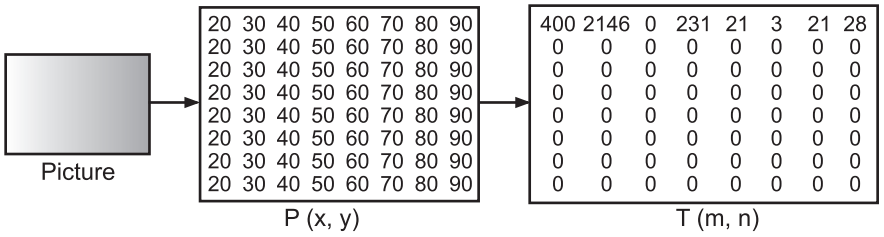


Fig. 2.5: Case 3 (Gradient Gray Scale)

Phase 2: Quantization

- Quantization, involved in image processing, is a lossy compression technique achieved by compressing a range of values to a single quantum value.
- After the T table is created, the values are quantized to reduce the number of bits needed for encoding. Previously in quantization, we dropped the fraction from each value and kept the integer part.
- Here, we divide the number by a constant and then drop the fraction. This reduces the required number of bits even more. In most implementations, a quantizing table (8 by 8) defines how to quantize each value.
- The divisor depends on the position of the value in the T table. This is done to optimize the number of bits and the number of 0s for each particular application.
- Note that the only phase in the process that is not completely reversible is the quantizing phase. We lose some information here that is not recoverable.
- As a matter of fact, the only reason that JPEG is called lossy compression is because of this quantization phase.

Phase 3: Compression

- After quantization, the values are read from the table, and redundant 0s are removed. However, to cluster the 0s together, the table is read diagonally in a zigzag fashion rather than row by row or column by column.
- The reason is that if the picture changes smoothly, the bottom right corner of the T table is all 0s. Fig. 2.6 shows the process of reading the table.

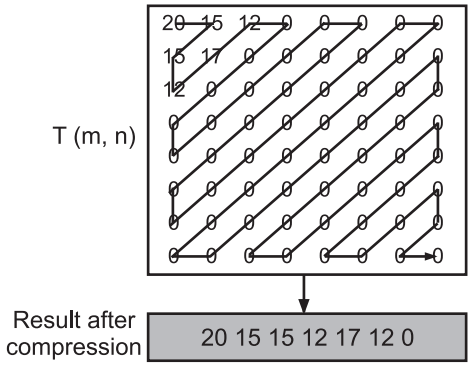


Fig. 2.6: Reading the Table

Video Compression (MPEG):

- Video compression is the process of reducing the total number of bits needed to represent a given image or video sequence.
- The MPEG method is used to compress video. In principle, a motion picture is a rapid flow of a set of frames, where each frame is an image.
- In other words, a frame is a spatial combination of pixels, and a video is a temporal combination of frames that are sent one after another.
- Compressing video, then, means spatially compressing each frame and temporally compressing a set of frames.
- The **spatial compression** of each frame is done with JPEG (or a modification of it). Each frame is a picture that can be independently compressed.
- In **temporal compression**, redundant frames are removed. When we watch television, we receive 50 frames per second. However, numbers of the consecutive frames are almost the same.
- For example, when someone is talking, most of the frame is the same as the previous one except for the segment of the frame around the lips, which changes from one frame to another.
- To temporally compress data, the MPEG method first divides frames into three categories namely, I-frames, P-frames and B-frames. Fig. 2.7 shows a sample sequence of frames.

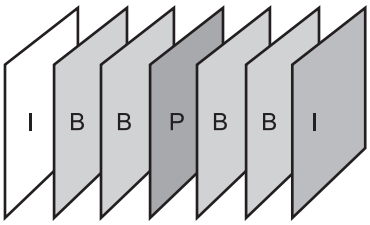


Fig. 2.7: MPEG Frames

- An **I-frame (Intracoded-frame)** is an independent frame that is not related to any other frame (not to the frame sent before or to the frame sent after). They are present at regular intervals (e.g., every ninth frame is an I-frame).
- An I-frame must appear periodically to handle some sudden change in the frame that the previous and following frames cannot show. Also, when a video is broadcast, a viewer may tune at any time.
- If there is only one I-frame at the beginning of the broadcast, the viewer who tunes in late will not receive a complete picture.
- I-frames are independent of other frames and cannot be constructed from other frames.
- A **P-frame (Predicted-frame)** is related to the preceding I-frame or P-frame. In other words, each P-frame contains only the changes from the preceding frame.
- The changes, however, cannot cover a big segment. For example, for a fast-moving object, the new changes may not be recorded in a P-frame.
- P-frames can be constructed only from previous I-frame or P-frame. P-frames carry much less information than other frame types and carry even fewer bits after compression.
- A **B-frame (Bidirectional-frame)** is related to the preceding and following I-frame or P-frame. In other words, each B-frame is relative to the past and the future. Note that a B-frame is never related to another B-frame.
- Fig. 2.8 shows how I-, P- and B-frames are constructed from a series of seven frames.

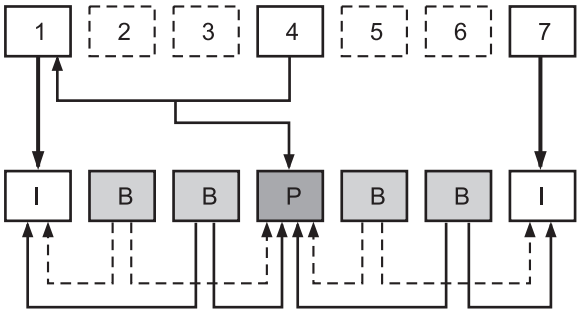


Fig. 2.8: Construction of MPEG Frames

- MPEG has gone through versions like MPEG1 was designed for a CD-ROM with a data rate of 1.5 Mbps. MPEG2 was designed for high-quality DVD with a data rate of 3 to 6 Mbps.
- MPEG Audio Layer-3 is used for audio compression and creates almost CD quality sound. MPEG-4 is multimedia standards for the computers, mobile devices and the web.
- MPEG-7 describes multimedia content. MPEG-21 is supposed to become a standard as a multimedia framework.

2.2 STREAMING STORED AUDIO/VIDEO

- In stored audio/video streaming, the files are compressed and stored on a server and a client downloads the files through the Internet.
- Stored audio/video streaming is sometimes referred to as on-demand audio/video. In stored audio/video streaming, clients request compressed audio/video files, which are resident on servers.
- Examples of audio files are songs, symphonies, books on tape, and famous lectures. Examples of stored video files are movies, TV shows and music video clips.
- Downloading stored audio and video files from a Web server can be different from downloading other types of files.
- To understand the concept, let us discuss following three approaches, each with a different complexity.

1. First Approach (Using a Web Server):

- Fig. 2.9 shows the first approach of streaming audio/video using Web server.
- A compressed audio or video file can be downloaded as a text file. The client i.e., browser can use the services of HTTP and send a GET message to download the file.
- The Web server can send the compressed file to the browser. The browser can then use a help application, normally called a media player, to play the file.
- The first approach of stored audio and video streaming is very simple and does not involve streaming.
- However, it has a drawback. An audio and/or video file is usually large even after compression. An audio file may contain tens of megabits and a video file may contain hundreds of megabits.
- In this approach of stored audio and video streaming, the file needs to download completely before it can be played.
- Using contemporary data rates, the user needs some seconds or tens of seconds before the file can be played.

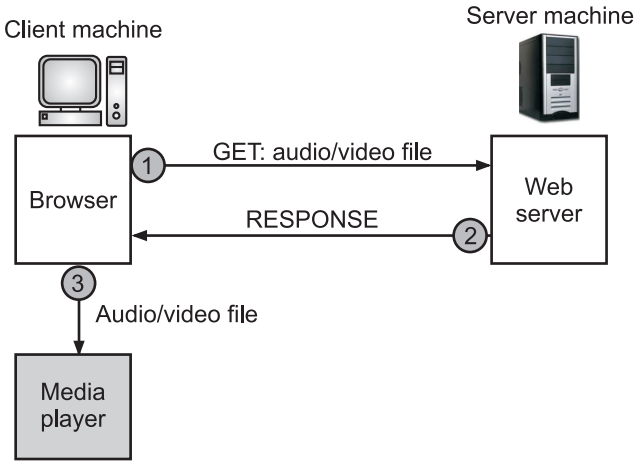


Fig. 2.9: First Approach of Streaming Audio/Video using Web Server

2. Second Approach (Using a Web Server with Metafile):

- Fig. 2.10 shows the steps in second approach of stored audio and video streaming.
- In this approach, the media player is directly connected to the Web server for downloading the audio/video file.
- The Web server stores two files namely, the actual audio/video file and a metafile that holds information about the audio/video file.
- The steps in Fig. 2.10 are given below:

  Step 1: The HTTP client accesses the Web server using the GET message.

  Step 2: The information about the metafile comes in the response.

  Step 3: The metafile is passed to the media player.

  Step 4: The media player uses the URL in the metafile to access the audio/video file.

  Step 5: The Web server responds.

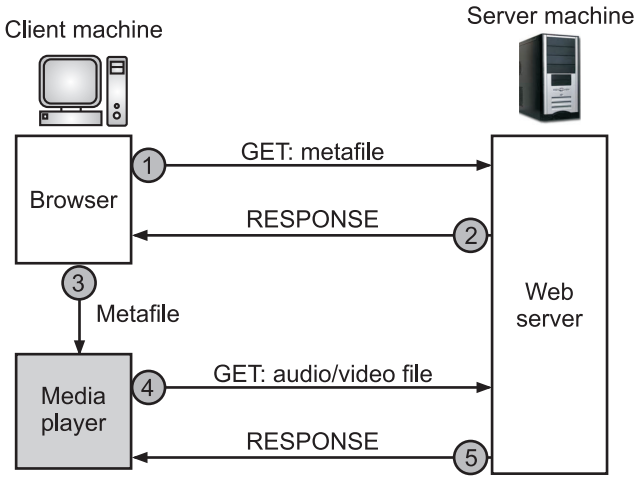


Fig. 2.10: Second Approach of Streaming Audio/Video using a Web Server with a Metafile

3. Third Approach (Using a Media Server):

- The problem with the second approach of stored audio/video is that the browser and the media player both use the services of HTTP.
- HTTP is designed to run over TCP. This is appropriate for retrieving the metafile, but not for retrieving the audio/video file.
- The reason is that TCP retransmits a lost or damaged segment, which is counter to the philosophy of streaming.
- We need to dismiss TCP and its error control; we need to use UDP (User Datagram Protocol).
- However, HTTP, which accesses the Web server, and the Web server itself are designed for TCP; we need another server, a media server.
- Fig. shows above concept and the steps are given below:

  Step 1: The HTTP client accesses the Web server using a GET message.

  Step 2: The information about the metafile comes in the response.

  Step 3: The metafile is passed to the media player.

  Step 4: The media player uses the URL in the metafile to access the media server to download the file. Downloading can take place by any protocol that uses UDP.

  Step 5: The media server responds.

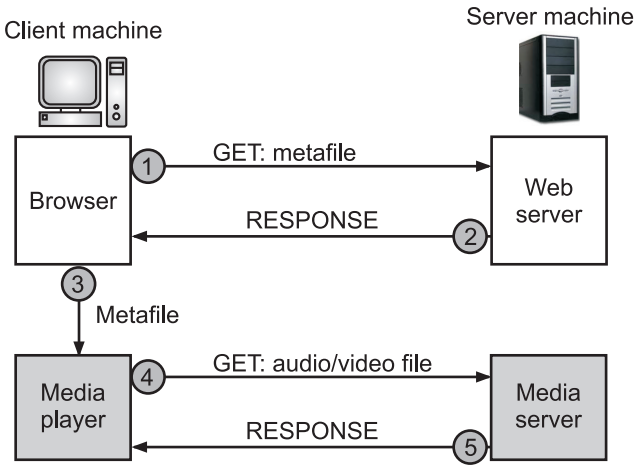


Fig. 2.11: Third Approach of Streaming Audio/Video using Media Server

Fourth Approach (Using a Media Server and RTSP):

- The RTSP (Real-Time Streaming Protocol) is a control protocol designed to add more functionalities to the streaming process.
- Using RTSP, we can control the playing of audio/video. RTSP is an out-of-band control protocol that is similar to the second connection in FTP.

- Fig. 2.12 shows a media server and RTSP. The steps are given below:

  Step 1: The HTTP client accesses the Web server using a GET message.

  Step 2: The information about the metafile comes in the response.

  Step 3: The metafile is passed to the media player.

  Step 4: The media player sends a SETUP message to create a connection with the media server.

  Step 5: The media server responds.

  Step 6: The media player sends a PLAY message to start playing (downloading).

  Step 7: The audio/video file is downloaded using another protocol that runs over UDP.

  Step 8: The connection is broken using the TEARDOWN message.

  Step 9: The media server responds.

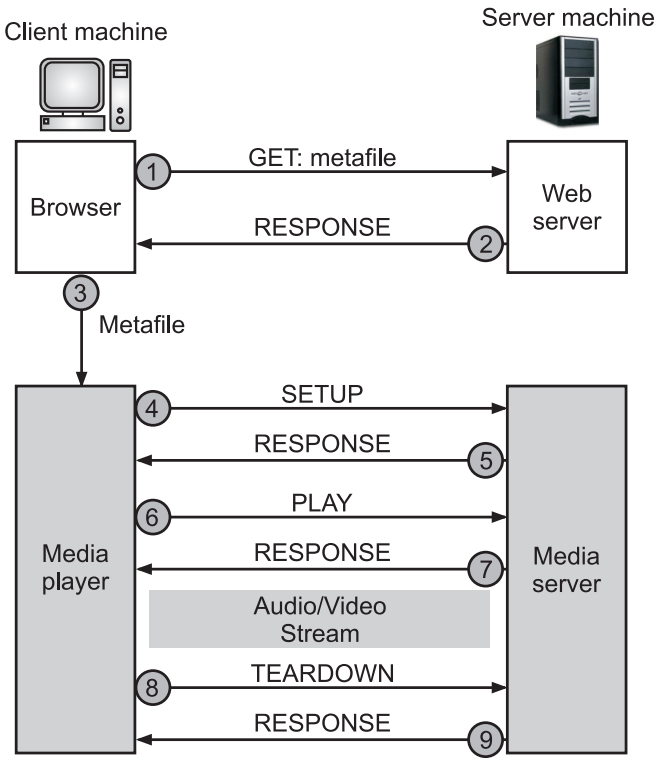


Fig. 2.12: Fourth Approach of Streaming Audio/Video using a Media Server and RTSP

- The media player can send other types of messages such as, a PAUSE message temporarily stop the downloading; downloading can be resumed with a PLAY message.

2.3 STREAMING LIVE AUDIO/VIDEO

- Streaming is a process in which the end-user obtains the entire file for the content before watching or listening to it. Live streaming refers to online streaming media simultaneously recorded and broadcast in real-time.
- Streaming live audio/video, a user listens to broadcast audio and video through the Internet.
- An example of this type of application is the Internet radio. Another examples are Internet TeleVision (ITV), Internet Protocol TeleVision (IPTV).
- Some radio stations broadcast their programs only on the Internet; many broadcast them both on the Internet and on the air.
- Internet TV is not popular yet, but many people believe that TV stations will broadcast their programs on the Internet in the future.
- Streaming live audio/video is similar to the broadcasting of audio and video by radio and TV stations. Instead of broadcasting to the air, the stations broadcast through the Internet.
- Live streaming is better suited to the multicast services of IP and the use of protocols such as UDP and RTP (Real-time Transport Protocol).
- The RTP is a network protocol for delivering audio and video over IP networks. RTP typically runs over User Datagram Protocol (UDP).
- However, presently, live streaming is still using TCP and multiple unicasting instead of multicasting. There is still much progress to be made in this area.
- In short, streaming live audio/video refers to the broadcasting of radio and TV programs through the Internet.

2.4 REAL-TIME INTERACTIVE AUDIO/VIDEO

- In real-time interactive audio/video, people use the Internet to interactively communicate with one another.
- Examples of interactive audio/video application includes Internet telephony (online telephony) or Voice over IP (VoIP) and Internet teleconferencing (or video conferencing) which allows people to communicate visually and orally.

2.4.1 Characteristics

- Some characteristics of real-time audio/video communication are given below:

1. Time Relationship:

- Real-time data on a packet-switched network require the preservation of the time relationship between packets of a session.

- For example, let us assume that a real-time video server creates live video images and sends them online. The video is digitized and packetized.
- There are only three packets, and each packet holds 10 s of video information. The first packet starts at 00:00:00, the second packet starts at 00:00:10, and the third packet starts at 00:00:20.
- Also imagine that it takes 1 s (an exaggeration for simplicity) for each packet to reach the destination (equal delay).
- The receiver can play back the first packet at 00:00:01, the second packet at 00:00:11, and the third packet at 00:00:21.
- Although there is a 1-s time difference between what the server sends and what the client sees on the computer screen, the action is happening in real time.
- The time relationship between the packets is preserved. The 1-s delay is not important. Fig. 2.13 shows the idea.

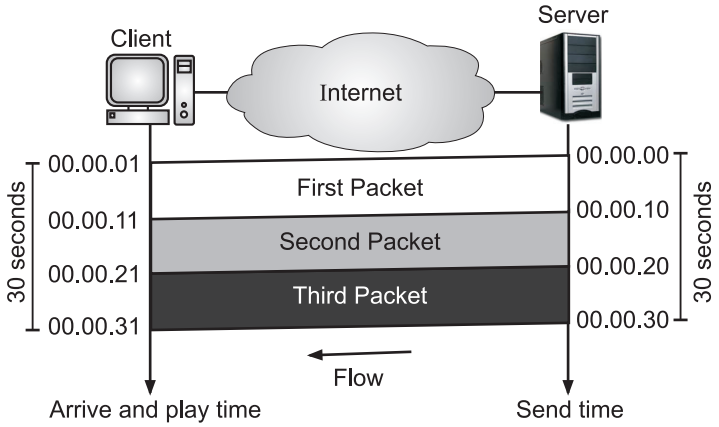


Fig. 2.13: Time Relationship

- But what happens if the packets arrive with different delays? For example, the first packet arrives at 00:00:01 (1-s delay), the second arrives at 00:00:15 (5-s delay), and the third arrives at 00:00:27 (7-s delay).
- If the receiver starts playing the first packet at 00:00:01, it will finish at 00:00:11. However, the next packet has not yet arrived; it arrives 4 s later.
- There is a gap between the first and second packets and between the second and the third as the video is viewed at the remote site. This phenomenon is called jitter.
- Fig. 2.14 shows the situation. Jitter is introduced in real-time data by the delay between packets.

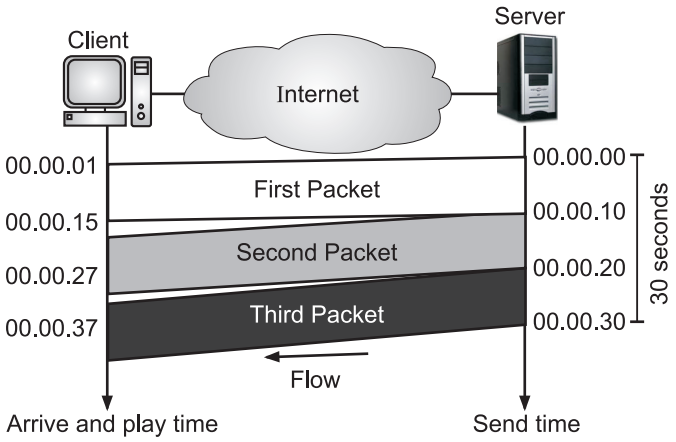


Fig. 2.14: Jitter

2. Timestamp:

- One solution to jitter is the use of a timestamp. We can timestamp the packets and separate the arrival time from the playback time.
- If each packet has a timestamp that shows the time it was produced relative to the first (or previous) packet, then the receiver can add this time to the time at which it starts the playback.
- In other words, the receiver knows when each packet is to be played. Imagine the first packet in the previous example has a timestamp of 0, the second has a timestamp of 10, and the third a timestamp of 20.
- If the receiver starts playing back the first packet at 00:00:08, the second will be played at 00:00:18, and the third at 00:00:28. There are no gaps between the packets. Fig. 2.15 shows the situation.

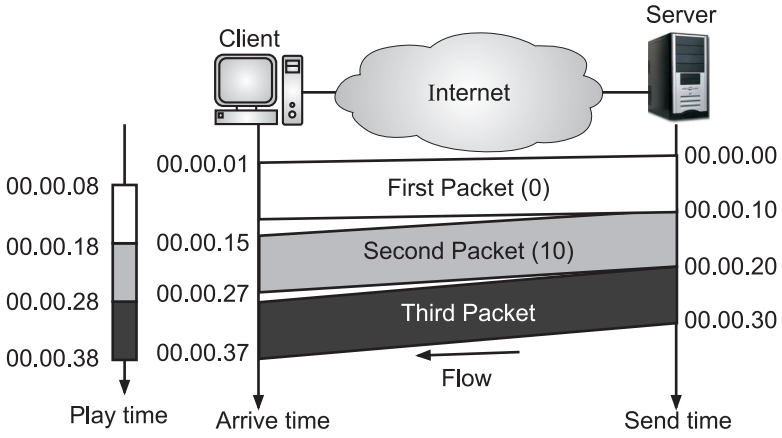


Fig. 2.15: Timestamp

3. Playback Buffer:

- To be able to separate the arrival time from the playback time, we need a buffer to store the data until they are played back. The buffer is referred to as a playback buffer.
- A playback buffer is required for real-time traffic. When a session begins (the first bit of the first packet arrives), the receiver delays playing the data until a threshold is reached.
- In the previous example, the first bit of the first packet arrives at 00:00:01; the threshold is 7 s, and the playback time is 00:00:08.
- The threshold is measured in time units of data. The replay does not start until the time units of data are equal to the threshold value.
- Data are stored in the buffer at a possibly variable rate, but they are extracted and played back at a fixed rate.
- Note that the amount of data in the buffer shrinks or expands, but as long as the delay is less than the time to play back the threshold amount of data, there is no jitter.
- Fig. 2.16 shows the buffer at different times for our example.

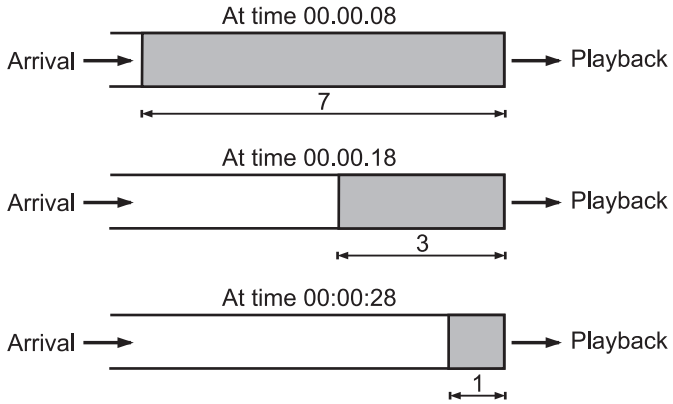


Fig. 2.16: Playback Buffer

4. Ordering:

- In addition to time relationship information and timestamps for real-time traffic, one more feature is needed. We need a sequence number for each packet.
- A sequence number on each packet is required for real-time traffic. The timestamp alone cannot inform the receiver if a packet is lost.
- For example, suppose the timestamps are 0, 10, and 20. If the second packet is lost, the receiver receives just two packets with timestamps 0 and 20.
- The receiver assumes that the packet with timestamp 20 is the second packet, produced 20 s after the first.

- The receiver has no way of knowing that the second packet has actually been lost. A sequence number to order the packets is needed to handle this situation.

5. **Multicasting:**

- Real-time traffic needs the support of multicasting. Multimedia plays a primary role in audio and video conferencing.
- The traffic can be heavy, and the data are distributed using multicasting methods. Conferencing requires two-way communication between receivers and senders.

6. **Translation:**

- Sometimes real-time traffic needs translation. Translation means changing the encoding of a payload to a lower quality to match the bandwidth of the receiving network.
- A translator is a computer that can change the format of a high-bandwidth video signal to a lower-quality narrow bandwidth signal.
- This is needed, for example, for a source creating a high-quality video signal at 5 Mbps and sending to a recipient having a bandwidth of less than 1 Mbps.
- To receive the signal, a translator is needed to decode the signal and encode it again at a lower quality that needs less bandwidth.

7. **Mixing:**

- If there is more than one source that can send data at the same time (as in a video or audio conference), the traffic is made of multiple streams.
- To converge the traffic to one stream, data from different sources can be mixed. Mixing means combining several streams of traffic into one stream.
- A mixer mathematically adds signals coming from different sources to create one single signal.

2.5 RTP

- A protocol is designed to handle real-time traffic (like audio and video) on the Internet, is known as Real-time Transport Protocol (RTP).
- RTP does not have a delivery mechanism like multicasting, port numbers etc. RTP must be used with UDP.
- The RTP is a transport layer protocol in TCP/IP reference model used for delivering audio and video over IP networks.
- RTP is used in communication that involves streaming media, such as telephony, video teleconference applications. The main contributions of RTP are time-stamping, sequencing, and mixing facilities.
- RTP is designed for end-to-end, real-time transfer of streaming media. The protocol provides facilities for jitter compensation and detection of packet loss and out-of-order delivery, which are common especially during UDP transmissions on an IP network.

- RTP is used in conjunction with other protocols such as H.323 (defines the protocols to provide audio-visual communication sessions on any packet network.) and RTSP (Real Time Streaming Protocol (designed for use in entertainment and communications systems to control streaming media servers)).
- The RTP is used to deliver streaming audio and video media over the internet, thereby enabling the Voice over Internet Protocol (VoIP).

2.5.1 RTP Packet Format

- Fig. 2.17 shows the format of the RTP packet header.
- The format of the RTP packet header is very simple and general enough to cover all real-time applications. An application that needs more information adds it to the beginning of its payload.

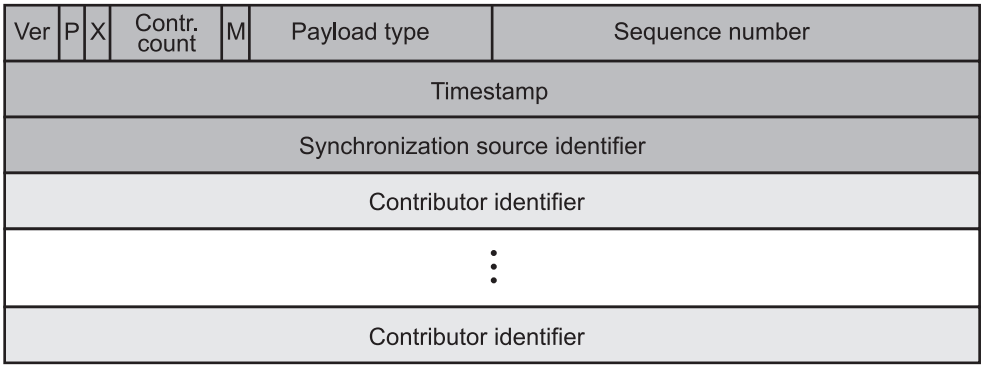


Fig. 2.17: RTP Packet Header Format

- The explanation of each field of the RTP packet header is given below:
  1. **Ver:** This 2-bit field defines version number. The current version is 2.
  2. **P:** The length of this field is 1-bit. If value f this field is 1, then it denotes presence of padding at end of packet and if value is 0, then there is no padding.
  3. **X:** The length of this field is also 1-bit. If value of this field is set to 1, then it's indicates an extra extension header between data and basic header and if value is 0 then, there is no extra extension.
  4. **Contributor Count**: This 4-bit field indicates number of contributors. Here, maximum possible number of contributor is 15 as a 4-bit field can allows number from 0 to 15.
  5. **M:** The length of this field is 1-bit and it is used as end marker by application to indicate end of its data.
  6. **Payload Types:** This field is of length 7-bit to indicate type of payload. Some common types of payload are given in following table:

Payload Type	Encoding Name
0	PCM micro Audio
1	1016
2	G721 audio
3	GSM audio
5-6	DV14 audio
7	LPC Audio
8	PCMA Audio
9	G722 Audio
10-11	L16 Audio
14	MPEG Audio
15	G728 Audio
26	Motion JPEG
31	H.216
32	MPEG1 video
33	MPEG2 video

7. **Sequence Number:** The length of this field is 16 bits. It is used to give serial numbers to RTP packets. It helps in sequencing. The sequence number for first packet is given a random number and then every next packet's sequence number is incremented by 1. This field mainly helps in checking lost packets and order mismatch.
8. **Timestamp:** The length of this field is 32-bit. It is used to find relationship between times of different RTP packets. The timestamp for first packet is given randomly and then time stamp for next packets given by sum of previous timestamp and time taken to produce first byte of current packet. The value of 1 clock tick is varying from application to application.
9. **Synchronization Source Identifier:** This is a 32-bit field used to identify and define the source. The value for this source identifier is a random number that is chosen by source itself. This mainly helps in solving conflict arises when two sources started with the same sequencing number.
10. **Contributor Identifier:** This is also a 32-bit field used for source identification where there is more than one source present in session. The mixer source use Synchronization source identifier and other remaining sources (maximum 15) use Contributor identifier.

2.6 RTCP

- RTCP stands for Real-time Transport Control Protocol. RTCP is defined in RFC 3550.
- The RTP allows only one type of message, which carries data from the source to the destination. But in some cases, we need some other type of messages in a session.
- The messages that can control the transmission and quality of data as well as also allow the recipients so that they can send feedback to the source or sources. A protocol designed for this purpose, which is known as RTCP.
- RTCP is used to provide control and statistical information about an RTP media streaming session.
- This lets control and statistics packets be separated logically and functionally from the media streaming while using the underlying packet delivery layer to transmit the RTCP signals as well as the RTP and media contents.
- RTCP is the feedback mechanism, and is used often in advanced implementations of RTP. RTCP works together with RTP and is a control protocol to monitor the media (quality) in RTP session.
- RTCP uses an odd-numbered UDP port number that follows the port number selected for RTP.
- The primary function of RTCP is to provide feedback on the quality of service (QoS) in media distribution by periodically sending statistics information such as transmitted octet and packet counts, packet loss, packet delay variation, and round-trip delay time to participants in a streaming multimedia session.

2.6.1 RTCP Messages

- RTCP has five types of messages namely, Sender Report, Receiver Report, Source Description Message, Bye Message and Application-Specific Message as shown in Fig. 2.18.
- The number next to each box in Fig. 2.18 defines the type of the message.

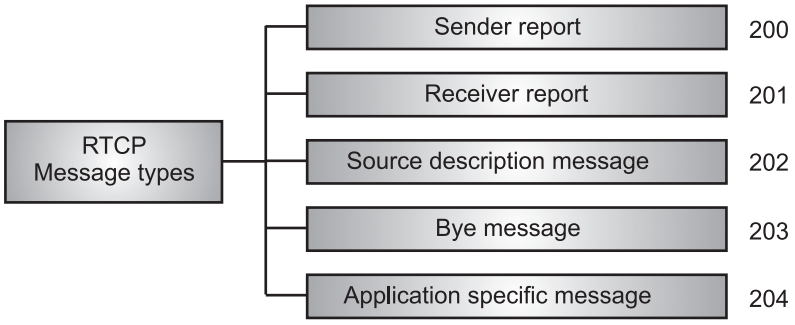


Fig. 2.18: Types of RTCP Messages

- The explanation of RTCP messages in Fig. 2.18 given below:

1. **Sender Report:**

- The sender report is sent periodically by the active senders in a conference to report transmission and reception statistics for all RTP packets sent during the interval.
- The sender report includes an absolute timestamp, which is the number of seconds elapsed since midnight January 1, 1900. The absolute timestamp allows the receiver to synchronize different RTP messages.
- It is particularly important when both audio and video are transmitted (audio and video transmissions use separate relative timestamps).

2. **Receiver Report:**

- The receiver report is for passive participants, those that do not send RTP packets.
- The report informs the sender and other receivers about the quality of service.

3. **Source Description Message:**

- The source periodically sends a source description message to give additional information about itself.
- This information can be the name, e-mail address, telephone number and address of the owner or controller of the source.

4. **Bye Message:**

- A source sends a bye message to shut down a stream. It allows the source to announce that it is leaving the conference.
- Although other sources can detect the absence of a source, this message is a direct announcement. It is also very useful to a mixer.

5. **Application-Specific Message:**

- The application-specific message is a packet for an application that wants to use new applications (not defined in the standard). It allows the definition of a new message type.
- The application-specific message provides a mechanism to design application-specific extensions to the RTCP protocol.

2.6.2 RTCP Packet Format

- Fig. 2.19 shows packet format of RTCP.

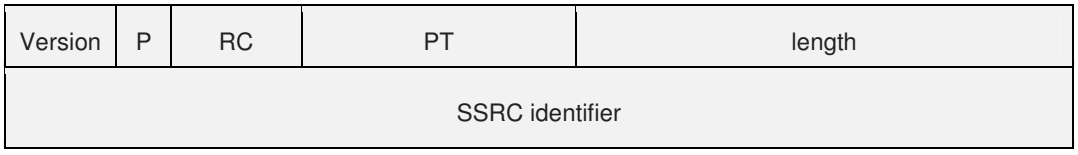


Fig. 2.19: RTCP Packet Header Format

- The explanation of each field of the RTCP packet header is given below:
  1. **Version** (2 bits) identifies the version of RTP, which is the same in RTCP packets as in RTP data packets. The version defined by this specification is two (2).

2. **P (Padding)** (1 bits) Indicates if there are extra padding bytes at the end of the RTP packet. Padding may be used to fill up a block of certain size, for example as required by an encryption algorithm. The last byte of the padding contains the number of padding bytes that were added (including itself).
3. **RC (Reception report Count)** (5 bits), the number of reception report blocks contained in this packet. A value of zero is valid.
4. **PT (Packet Type)** (8 bits) contains a constant to identify RTCP packet type.
5. **Length** (16 bits) indicates the length of this RTCP packet (including the header itself) in 32-bit units minus one.
6. **SSRC** (32 bits) Synchronization Source Identifier uniquely identifies the source of a stream.

2.7 VOICE OVER IP

- Traditionally Internet had been used for exchanging messages but due to advancement in technology, its service quality has increased manifold.
- It is now possible to deliver voice communication over IP networks using VoIP by converting voice data into packets.
- One real-time interactive audio/video application is Voice over IP (VoIP) also called as Internet telephony (means telephone services over Internet).
- The idea is to use the Internet as a telephone network with some additional capabilities.
- Instead of communicating over a circuit-switched network, this application allows communication between two parties over the packet-switched Internet.
- Voice over IP has been implemented with set of protocols like Session Initiation Protocol (SIP), Session Description Protocol (SDP), H.323 etc., based on open standards in applications such as VoIP phones, mobile applications, and web-based communications.
- Voice over Internet Protocol (VoIP) or IP telephony is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.
- Two protocols have been designed to handle this type of communication namely SIP and H.323.

Benefits of VoIP:

1. The VoIP's versatility allows greater freedom around voice communications.
2. VoIP provides many advanced features, such as digital faxing, visual voicemail, and group inboxes that improve overall productivity or service.
3. VoIP is increased accessibility. VoIP allows users to make calls from anywhere to anywhere on the globe using mobile, tablet, computer or desk phone.

4. VoIP has low cost relative to the cost of traditional phone services.
5. VoIP is easy to access and operate, offering enhanced availability.
6. VoIP provides high scalability. It easier to add or delete phone numbers with VoIP.

Disadvantages of VoIP:

1. VoIP requires reliable Internet connation.
2. Power outages have a huge effect on the viability of the VoIP system.
3. Latency issues can affect VoIP far more than traditional telephony services.
4. Security is a main concern with VoIP. The most prominent security issues over VoIP are identity and service theft, viruses and malware, denial of service, spamming, call tampering and phishing attacks.

2.7.1 SIP

- SIP is an acronym for Session Initiation Protocol. SIP is an application layer protocol that establishes, manages, and terminates a multimedia session (call).
- It can be used to create two-party, multiparty, or multicast sessions. SIP is designed to be independent of the underlying transport layer; it can run on either UDP, TCP or SCTP.
- The Session Initiation Protocol (SIP) is a signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications.
- SIP is used for signaling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls, in private IP telephone systems, in instant messaging over Internet Protocol (IP) networks as well as mobile phone calling over LTE (VoLTE).
- The protocol defines the specific format of messages exchanged and the sequence of communications for cooperation of the participants.
- SIP is a text-based protocol, incorporating many elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP).
- A call established with SIP may consist of multiple media streams, but no separate streams are required for applications, such as text messaging, that exchange data as payload in the SIP message.
- SIP is a protocol to establish, modify and terminate multimedia sessions like IP telephony.
- All systems that need multimedia sessions are registered and provided SIP address, much like IP address. Using this address, caller can check callee's availability and invite it for a VoIP session accordingly.
- SIP facilitates multiparty multimedia sessions like video conferencing involving three or more people. In a short span of time SIP has become integral to VoIP and largely replaced H.323.

SIP Messages:

- SIP is a text-based protocol like HTTP. Like HTTP, SIP, uses messages. Each message has a header and a body. The header consists of several lines that describe the structure of the message, caller's capability, media type and so on.
- Fig. 2.20 shows six types of SIP messages.
- The caller initializes a session with the **INVITE** message. After the callee answers the call, the caller sends an **ACK** message for confirmation.
- The **BYE** message terminates a session. The **OPTIONS** message queries a machine about its capabilities.
- The **CANCEL** message cancels an already started initialization process. The **REGISTER** message makes a connection when the callee is not available.

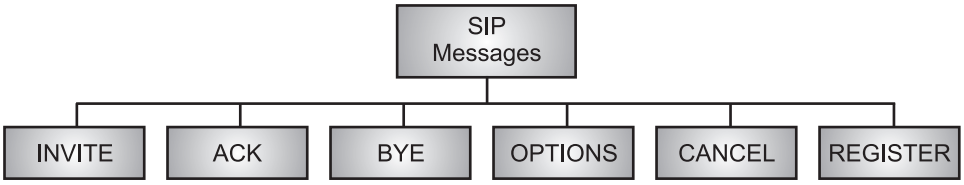


Fig. 2.20: SIP Messages

SIP Addresses:

- In a regular telephone communication a telephone number identifies the sender and another telephone number identifies the receiver.
- SIP is very flexible. In SIP, an e-mail address, an IP address, a telephone number, and other types of addresses can be used to identify the sender and receiver.
- However, the address needs to be in SIP format (also called scheme). Fig. 2.21 shows some common formats of SIP addresses.

Fig. 2.21: SIP Addresses

SIP Simple Session:

- Fig. 2.22 shows a simple session using SIP.
- A simple session using SIP consists of three modules namely, establishing, communicating and terminating.
  1. **Establishing a Session:** Establishing a session in SIP requires a three-way handshake. The caller sends an INVITE message, using UDP, TCP, or SCTP to begin the communication. If the callee is willing to start the session, she sends a reply message. To confirm that a reply code has been received, the caller sends an ACK message.

2. **Communicating:** After the session has been established, the caller and the callee can communicate using two temporary ports.
3. **Terminating the Session:** The session can be terminated with a BYE message sent by either party.

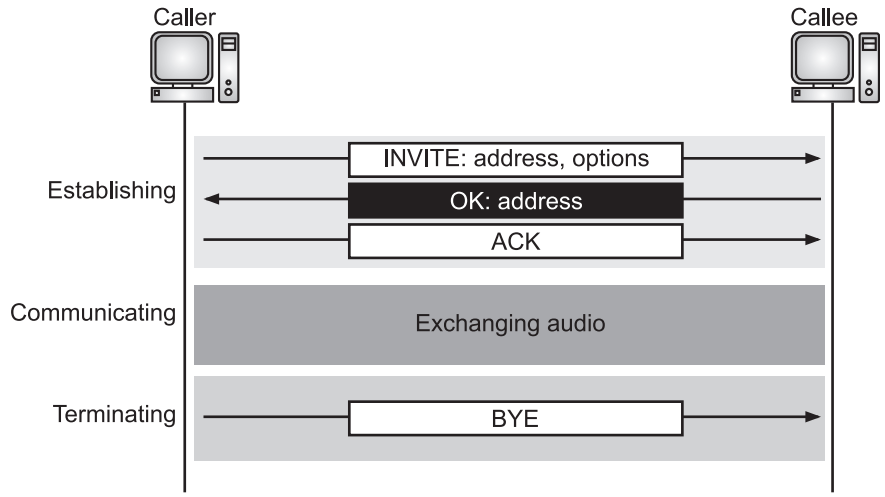


Fig. 2.22: Simple Session on SIP

Tracking the Callee in SIP:

- What happens if the callee is not sitting at his/her terminal? He/she may be away from his/her system or at another terminal. He/she may not even have a fixed IP address if DHCP is being used.
- SIP has a mechanism (similar to one in DNS) that finds the IP address of the terminal at which the callee is sitting. To perform this tracking, SIP uses the concept of registration.
- SIP defines some servers as registrars. At any moment a user is registered with at least one registrar server; this server knows the IP address of the callee.
- When a caller needs to communicate with the callee, the caller can use the e-mail address instead of the IP address in the INVITE message.
- The message goes to a proxy server. The proxy server sends a lookup message (not part of SIP) to some registrar server that has registered the callee.
- When the proxy server receives a reply message from the registrar server, the proxy server takes the caller's INVITE message and inserts the newly discovered IP address of the callee. This message is then sent to the callee.
- Fig. 2.23 shows the process of tracking the callee in SIP.

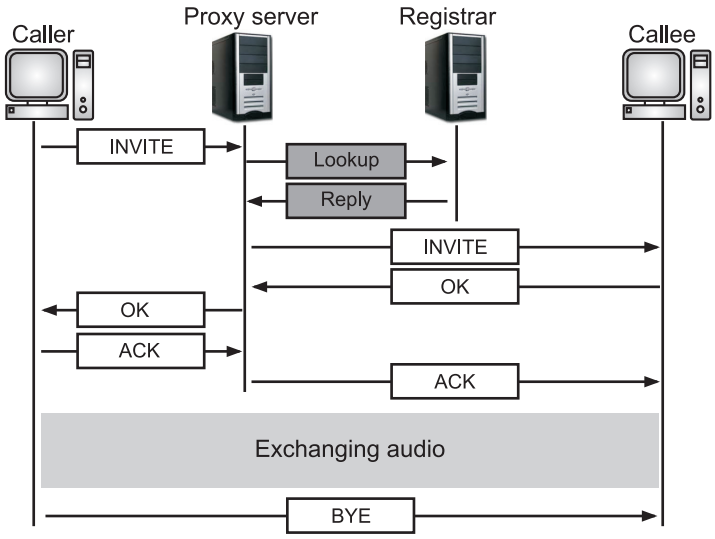


Fig. 2.23: Tracking the Callee in SIP

2.7.2 H.323

- H.323 is a standard designed by ITU (International Telecommunication Union) to allow telephones on the public telephone network to talk to computers (called terminals in H.323) connected to the Internet.
- H.323 is a VoIP standard for defining the components, protocols and procedures to provide real-time multimedia sessions including audio, video and data transmissions over packet switched networks.
- H.323 was the first VoIP standard to adopt the Internet Engineering Task Force (IETF) standard Real-time Transport Protocol (RTP) to transport audio and video over IP networks.

Architecture of H.323:

- H.323 allows telephones on the general public telephone network to speak to computers connected to internet.
- Fig. 2.24 shows the general architecture of H.323.
- At the center, there is gateway placed which connects the Internet to the telephone network. Gateway translates a message from one protocol to another.
- The gateway transforms a telephone network message into an Internet message. The gatekeeper server on the Local Area Network (LAN) plays the role of the registrar server.
- A gatekeeper provides a number of services to terminals, gateways and MCU (Multipoint Control Unit (video conferencing hardware)) devices.
- The services of gatekeeper include endpoint registration, address resolution, admission control, user authentication, and so forth.

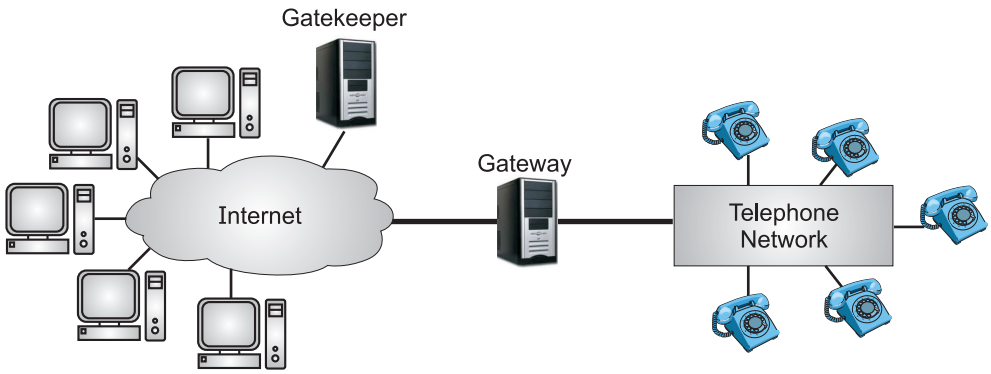


Fig. 2.24: H.323 Architecture

Protocols of H.323:

- To maintain audio or video communication, H.323 uses a number of protocols. The various protocols used by H.323 are as shown in the Fig. 2.25.
- H.323 uses G.711 or G.723.1 for compression. It uses a protocol named H.245 which allows the parties to negotiate the compression method.
- Protocol Q.931 is used for establishing and terminating connections. Another protocol called H.225, or RAS (Registration/Administration/Status), is used for registration with the gatekeeper. RTP is used for actual data transmission.

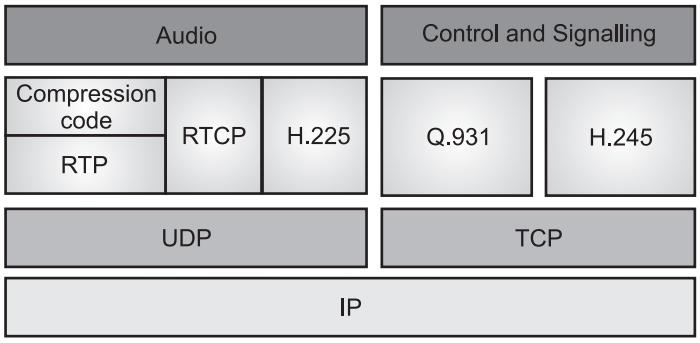


Fig. 2.25: Protocols of H.323

Operation of H.323:

- Fig. 2.26 shows the operation of a telephone communication using H.323. Following steps used by a terminal to communicate with a telephone.

  Step 1: The terminal sends a broadcast message to the gatekeeper. The gatekeeper responds with its IP address.

  Step 2: The terminal and gatekeeper communicate, using H.225 to negotiate bandwidth.

Step 3: The terminal, the gatekeeper, gateway, and the telephone communicate using Q.931 to set up a connection.

Step 4: The terminal, the gatekeeper, gateway, and the telephone communicate using H.245 to negotiate the compression method.

Step 5: The terminal, gateway, and the telephone exchange audio using RTP under the management of RTCP.

Step 6: The terminal, the gatekeeper, gateway, and the telephone communicate using Q.931 to terminate the communication.

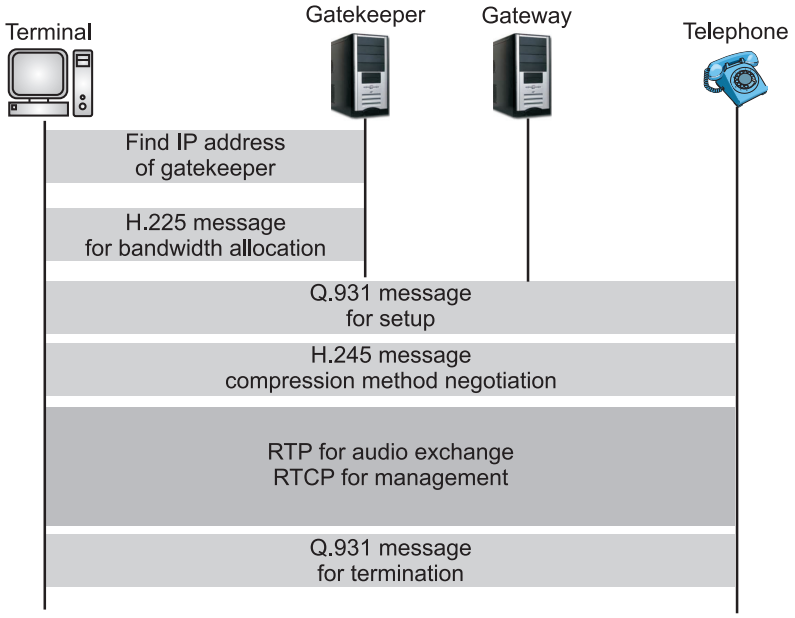


Fig. 2.26: Operation of H.323

PRACTICE QUESTIONS

Q.I Multiple Choice Questions:

1. What is multimedia?
   (a) combination of multiple files contents like text, binary etc.
   (b) combination of multiple media contents like text, video, audio, images, animation etc.
   (c) Both (a) and (b)
   (d) None of the mentioned
2. In which type of streaming multimedia file is delivered to the client, but not shared?
   (a) real-time streaming (b) progressive download
   (c) compression (d) none of the mentioned

3. Which one of the following is the characteristic of a multimedia system?
   (a) high storage (b) high data rates
   (c) Both (a) and (b) (d) None of the mentioned
4. The delay that occur during the playback of a stream is called as,
   (a) stream delay (b) playback delay
   (c) jitter (d) event delay
5. Multimedia is applied in the different fields such as,
   (a) Digital Library (b) Animated Films
   (c) E-learning (d) All of the mentioned
6. Real time streaming protocol is used,
   (a) to control streaming media servers
   (b) for establishing and controlling media sessions between endpoints
   (c) to provide real time control of playback of media files from the server
   (d) All of the mentioned
7. Multimedia media contains,
   (a) Text, Graphics (b) Audio, Video
   (c) Animation (d) All of the mentioned
8. Video or audio content is streamed (i.e. transmitted) over the Internet in which form.
   (a) compact (b) zip
   (c) compressed (d) None of the mentioned
9. Streaming stored audio/video refers to,
   (a) on-demand requests for compressed audio/video files
   (b) to the broadcasting of radio and TV programs through the Internet
   (c) to the use of the Internet for interactive audio/video applications
   (d) All of the mentioned
10. The sound used in multimedia application is,
    (a) digital voice (b) digital video
    (c) digital animation (d) digital audio
11. How many types of video compressions?
    (a) 2 (b) 3
    (c) 4 (d) 6
12. Which image files is a lossy format?
    (a) GIF (b) MPEG
    (c) JPEG (d) PNG

13. Interactive audio/video refers to,
    (a) on-demand requests for compressed audio/video files
    (b) to the broadcasting of radio and TV programs through the Internet
    (c) to the use of the Internet for interactive audio/video applications
    (d) All of the mentioned
14. Which file creates a perfect reproduction of the original images?
    (a) Shockwave (b) TIFF
    (c) GIF (d) JPG
15. Which is used to save disk space and reduce the time needed to transfer files over the Internet?
    (a) Streaming (b) Compression
    (c) Both (a) and (b) (d) All of the mentioned
16. JPEG stands for,
    (a) Joint Photo Experts Gross
    (b) Joint Photographic Experts Gross
    (c) Joint Processor Experts Group
    (d) Joint Photographic Expression Group
17. GIF means,
    (a) Graphic Information File (b) Graphic Interchange Format
    (c) Graphic Information Format (d) Graphic Interchange File
18. Which compressions provide some loss of quality?
    (a) Lossy (b) Loss less
    (c) Cel based (d) Object based
19. Which of the following is a computer based presentation technique?
    (a) Slides (b) Tutorial
    (c) Multimedia (d) Data processing
20. Which is a form of data compression designed to reduce the size of audio data files?
    (a) Video compression
    (b) Image compression
    (c) Audio compression
    (d) All of the mentioned
21. Which encoding compression is normally used for speech.,
    (a) Perceptual (b) Streaming
    (c) Predictive (d) All of the mentioned

22. Which compression is the process of encoding a video file in such a way that it consumes less space than the original file and is easier to transmit over the network or Internet?
    (a) Audio (b) Image
    (c) Both (a) and (b) (d) Video
23. Which compression is the process of encoding or converting an image file in such a way that it consumes less storage space than the original file?
    (a) Video (b) Audio
    (c) Both (a) and (b) (d) Image
24. In which streaming, the files are compressed and stored on a server and a client downloads the files through the Internet.
    (a) live audio/video (b) stored audio/video
    (c) interactive audio/video (d) None of the mentioned
25. Examples of live audio/video include,
    (a) Internet radio
    (b) Internet TeleVision (ITV)
    (c) Internet Protocol TeleVision (IPTV)
    (d) All of the mentioned
26. The major difference between a multimedia file and a regular file is,
    (a) the size (b) the attributes
    (c) the ownership (d) rate at which the file must be accessed
27. Video is represented as a series of images formally known as,
    (a) pics (b) shots
    (c) frames (d) snaps
28. The faster the frames are displayed,
    (a) the rougher the video appears
    (b) the smoother the video appears
    (c) it gets blurry
    (d) None of the mentioned
29. Which buffer is required for real-time traffic?
    (a) playback
    (b) timestamp
    (c) Both (a) and (b)
    (d) None of the mentioned

30. Which means changing the encoding of a payload to a lower quality to match the bandwidth of the receiving network?
    (a) Translation (b) Mixing
    (c) Ordering (d) Buffering
31. Multimedia files stored on a remote server are delivered to a client across the network using a technique known as,
    (a) download (b) streaming
    (c) flowing (d) leaking
32. Which protocol is used in communication that involves streaming media, such as telephony, video teleconference applications?
    (a) RTP (b) SIP
    (c) H.232 (d) All of the mentioned
33. Which protocol is designed for end-to-end, real-time transfer of streaming media?
    (a) RTP (b) SIP
    (c) H.323 (d) All of the mentioned
34. RTCP stands for,
    (a) Real-time Transfer Control Protocol
    (b) Real-time Transport Control Protocol
    (c) Real-time Transport Connection Protocol
    (d) Real-timestamp Transport Control Protocol
35. The media file is streamed to the client but is only played and not stored by the client in,
    (a) progressive download
    (b) regular download
    (c) real time streaming
    (d) virtual time streaming
36. Real time streaming is most useful for,
    (a) short video clips
    (b) long video clips
    (c) extremely short and low quality videos
    (d) None of the mentioned
37. The real-time interactive audio/video application is,
    (a) Voice over IP (VoIP)
    (b) Internet telephony
    (c) Both (a) and (b)
    (d) All of the mentioned

38. SIP is an acronym for,
    (a) Signal Initiation Protocol (b) Session Initiation Protocol
    (c) Session Initiatal Protocol (d) None of the mentioned
39. Gap between _____ packets at the receiver cause a phenomenon is known as Jitter.
    (a) Compression (b) consecutive
    (c) Controlling (d) Conferencing
40. To receive the signal, a translator is needed to decode the signal and encode it again at,
    (a) High quality (b) Lower quality
    (c) Same Quality (d) Bad Quality
41. Session initiation Protocol (SIP), is very
    (a) Independent (b) Flexible
    (c) Dependent (d) Complex
42. Establishing a session is SIP requires a three way,
    (a) Protocols (b) System
    (c) Ports (d) Handshake
43. Moving Pictures Experts Group (MPEG) is used to compress,
    (a) Frames (b) Images
    (c) Audio (d) Video
44. Which is a text-based protocol?
    (a) RTP (b) SIP
    (c) RTCP (d) H.323
45. The most common compression technique that is used to create CD-quality audio is based on the perceptual encoding technique is called as,
    (a) Predictive encoding (b) Perceptual encoding
    (c) MPEG (d) JPEG
46. In audio and video compression, each frame is divided into small grids, called picture elements or
    (a) Frame (b) Packets
    (c) Pixels (d) Mega Pixels
47. Live streaming is still using Transmission Control Protocol (TCP) and multiple unicasting instead of
    (a) unicasting (b) multicasting
    (c) layered control (d) protocol control

48. Moving Picture Experts Group (MPEG-2), was designed for high-quality DVD with data rate of,
    (a) 3 to 6 Mbps (b) 4 to 6 Mbps
    (c) 5 to 6 Mbps (d) 6 to 6 Mbps
49. Joint Photographic Experts Group (JPEG) is used to compress,
    (a) music (b) pictures
    (c) images (d) frames
50. Real-time traffic needs the support of,
    (a) unicasting (b) multicasting
    (c) layered control (d) protocol Control
51. Which is a VoIP standard for defining the components, protocols and procedures to provide real-time multimedia sessions including audio, video and data transmissions over packet switched networks?
    (a) RTP (b) SIP
    (c) RTCP (d) H.323

Answers

1. (b)	2. (a)	3. (c)	4. (c)	5. (d)	6. (d)	7. (d)	8. (c)	9. (a)	10. (d)
11. (a)	12. (c)	13. (b)	14. (c)	15. (b)	16. (c)	17. (b)	18. (a)	19. (c)	20. (c)
21. (c)	22. (d)	23. (d)	24. (b)	25. (d)	26. (d)	27. (c)	28. (b)	29. (a)	30. (a)
31. (b)	32. (a)	33. (a)	34. (b)	35. (c)	36. (b)	37. (c)	38. (b)	39. (b)	40. (b)
41. (b)	42. (d)	43. (d)	44. (b)	45. (b)	46. (c)	47. (b)	48. (a)	49. (c)	50. (b)
51. (d)									

Q.II Fill in the Blanks:

1. _____ means combination of multiple media contents like text, video, audio, images, animation and interactive media.
2. A video consists of a sequence of _____.
3. Data _____ is the process of modifying, encoding or converting the bits structure of data in such a way that it consumes less space on disk.
4. _____ compression is the process of reducing the total number of bits needed to represent a given image or video sequence.
5. _____ compression is the process of encoding or converting an image file in such a way that it consumes less storage space than the original file.
6. After _____, the values are read from the table, and redundant 0s are removed.
7. An _____ is an independent frame that is not related to any other frame.
8. The purpose of dividing the picture into blocks is to _____ the number of calculations.

9. H.323 is a standard designed by _____ to allow telephones on the public telephone network to talk to computers connected to the Internet.
10. In real-time _____ audio/video, people use the Internet to interactively communicate with one another.
11. SIP has a mechanism (similar to one in DNS) that finds the IP address of the terminal at which the _____ is sitting.
12. The _____ -specific message provides a mechanism to design application-specific extensions to the RTCP protocol.
13. _____ refers to the moving pictures with sound such as a picture in television.
14. Digital audio or sound is used to record, store, manipulate, generate and reproduce sound using audio signals that have been encoded in _____ form.
15. _____ compression can be used for speech or music.
16. _____ audio/video streaming is sometimes referred to as on-demand audio/video.
17. Streaming _____ audio/video, a user listens to broadcast audio and video through the Internet.
18. A _____ is a computer that can change the format of a high-bandwidth video signal to a lower-quality narrow bandwidth signal.
19. A _____ mathematically adds signals coming from different sources to create one single signal.
20. A protocol is designed to handle real-time traffic (like audio and video) on the Internet, is known as _____.
21. _____ is used to provide control and statistical information about an RTP media streaming session.
22. _____ is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.
23. The _____ is a signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications.
24. _____ is a VoIP standard for defining the components, protocols and procedures to provide real-time multimedia sessions including audio, video and data transmissions over packet switched networks.

Answers

1. Multimedia	2. frames	3. compression	4. Video
5. Image	6. quantization	7. I-frame	8. decrease
9. ITU	10. interactive	11. callee	12.application
13. Video	14. digital	15. Audio	16. Stored
17. live	18. translator	19. mixer	20. RTP
21. RTCP	22. VoIP	23. SIP	24. H.323

Q.III State True or False:

1. Audio or sound is a physical phenomenon produced by the vibration of matter such as a violin string, a hand clapping etc.
2. The purpose of dividing the picture into blocks is to increase the number of calculations.
3. Predictive encoding compression is normally used for video.
4. One solution to jitter is the use of a timestamp.
5. An I-frame must appear periodically to handle some sudden change in the frame that the previous and following frames cannot show
6. Contributor Count is 8-bit field indicates number of contributors.
7. RTCP has three types of messages.
8. Real-time data on a packet-switched network require the preservation of the time relationship between packets of a session.
9. The receiver report is for active participants.
10. Voice over Internet Protocol (VoIP) or IP telephony is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.
11. The RTP allows only one type of message, which carries data from the source to the destination.
12. VoIP allows users to make phone calls over the Internet. This modern technology is capable of converting analog voice signals into digital packets of information.
13. Digital audio or sound is a representation of sound recorded in, or converted into, digital form
14. Lossless compression is a form of compression that loses data during the compression process.
15. RTP is generally used with a signaling protocol, such as SIP, which sets up connections across the network.
16. Streaming live audio/video refers to the broadcasting of radio and TV programs through the Internet.
17. We can timestamp the packets and separate the arrival time from the playback time.
18. H.322 provides out-of-band statistics and control information for any given RTP session.
19. To be able to separate the arrival time from the playback time, we need a playback buffer to store the data until they are played back.
20. Streaming stored audio/video refers to on-demand requests for compressed audio/video files.

21. The SIP provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video.
22. A P-frame (Predicted-frame) is related to the preceding I-frame or P-frame.
23. Multimedia is a media that uses multiple forms of interactive content (text, audio, video, graphic, animation etc.) and information processing.
24. Text is visual expression of alphanumeric letters, numbers and symbols used to communicate ideas and information to others through a human language system.
25. Audio compression is a technique used to compress audio signals based on signal processing of audio sequences.
26. The RTP is used to deliver streaming audio and video media over the internet, thereby enabling the Voice over Internet Protocol (VoIP).
27. SIP is an application layer protocol that establishes, manages, and terminates a multimedia session (call).
28. Perceptual encoding is the most common compression technique used to create CD-quality audio.
29 Before audio or video signals can be sent or transmitted on the Internet, they need to be digitized.
30. Interactive audio/video refers to the use of the Internet for interactive audio/video applications.
31. Image compression is the art/science of efficient coding of picture data to reduce the number of bits required to represent an image/picture.
32. In DCT phase, each block of 64 pixels goes through a transformation.
33. In stored audio/video streaming, the files are compressed and stored on a server and a client downloads the files through the Internet.
34. The RTSP is a control protocol designed to add more functionalities to the streaming process.
35. SIP is a VoIP standard for defining the components, protocols and procedures to provide real-time multimedia sessions including audio, video etc.
36. The RTP is a network protocol for delivering audio and video over IP networks.

Answers

1. (T)	2. (F)	3. (F)	4. (T)	5. (T)	6. (F)	7. (F)	8. (T)	9. (F)	10. (T)
11. (T)	12. (T)	13. (T)	14. (F)	15. (T)	16. (T)	17. (T)	18. (F)	19. (T)	20. (T)
21. (F)	22. (T)	23. (T)	24. (T)	25. (T)	26. (T)	27. (T)	28. (T)	29. (T)	30. (T)
31. (T)	32. (T)	33. (T)	34. (T)	35. (F)	36. (T)				

Q.IV Answer the following Questions:

(A) Short Answer Questions:

1. What is multimedia?
2. List media types for multimedia.
3. What is animation?
4. Define video and audio.
5. What is the function of SIP?
6. What is compression?
7. What is live video?
8. Define graphic.
9. Give purpose of RTP?
10. What is H.323?
11. What is VoIP?
12. What is RTCP?
13. What is the purpose playback buffer?
14. Define streaming.
15. What real time interactive audio/video?

(B) Long Answer Questions:

1. Define multimedia? Explain in detail.
2. How to digitize audio and video?
3. What is audio compression? List its categories.
4. What is image compression? Explain JPEG image compression.
5. Define video compression. Describe MPEG video compression in detail.
6. What is streaming stored audio/video? Explain with its approaches.
7. Define the terms timestamp, ordering, multicasting, translation and playback buffer.
8. What is RTP? Explain its packet format with diagram.
10. Write short note on: Streaming live audio/video.
11. Describe RTCP with message types. Also give packet format of RTCP.
12. Explain VoIP with its advantages and disadvantages.
13. Describe SIP with its messages and addresses.
14. Explain H.323 architecture diagrammatically.
15. With the help of diagram describe operation of H.323.
16. What is SIP session? Explain with the example.

17. Compare SIP and RTP.
18. What is compression? How to compress audio and video? Explain in detail.
19. Compare SIP and H.323. Any four points.
20. Differentiate between RTP and RTCP.
21. Explain working of VoIP diagrammatically.
22. Describe the following terms:
    (i) Text
    (ii) Audio
    (iii) Graphics
    (iv) Animation
    (v) Video.

❖❖❖

CHAPTER 3

Cryptography and Network Security

Objectives...

- To understand Concept of Network Security
- To learn Concept of Cryptography
- To study Security Services

3.0 INTRODUCTION

- Today, the use of computer with Internet is increasing rapidly. At the same time security challenges are also increasing.
- A number of software tools are available which help the attackers/interceptors to attack computers easily.
- Therefore, security becomes an important issue in computer field, when data/information is transmitted on a computer network. No one can deny the importance of security in computer networks.
- Network security is an emerging field which helps to protect the computer from various attacks.
- Computer security means to protect information. Network security means protection of data on the network during data transmission.
- Computer security deals with prevention and detection of unauthorized actions by users of a computer.
- Network security issues include protecting data from unauthorized access, protecting data from damage and development and implementing policies and procedures for recovery from breaches and data losses.
- Security in networking is based on cryptography. Cryptography is the science and art of achieving security by encoding messages to make them non-readable.
- The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.
- Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

3.1 CRYPTOGRAPHY (April 16, 18, Oct. 17)

- Today, we are living in the information age. We need to keep information about every aspect of our lives.
- In other words, information is an asset that has a value like any other asset. As an asset, information needs to be secured from attacks.
- An attack is any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent.
- To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (avaliability).
- Cryptography is technique of securing information through use of codes so that only those users for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information.
- The word 'cryptography' was coined by combining two Greek words, 'krypto' meaning hidden or secret and 'graphene' meaning writing. So, Cryptography, a word with Greek origins, means "secret writing."
- Cryptography is an art and science of transforming messages so as to make them secure and immune to attacks.
- Cryptography involves the process of encryption and decryption of messages using secret keys. The process of cryptography is shown in Fig. 3.1.
- Encryption is a process which transforms the original message into an unrecognizable or unreadable form.
- The sender requires an encryption algorithm and a key to transform the plaintext (original message) into a ciphertext (encrypted message),
- Decryption is a process of converting encoded/encrypted message to its original form. The receiver uses a decryption algorithm and a key to transform the ciphertext back to original plaintext.

Fig. 3.1: Cryptography

- The word steganography, with origin in Greek, means "covered writing," in contrast with cryptography, which means "secret writing." **(April 16, 17)**

- Cryptography means concealing the contents of a message by enciphering; steganography means concealing the message itself by covering it with something else.
- The terminology used in cryptography is given below:
  1. **Plaintext and Ciphertext:** The original message, before being transformed is called plaintext. After the message is transformed, it is called ciphertext. It is the scrambled message produced as output. It depends upon the plaintext and the key.
  2. **Encryption Algorithm:** The encryption algorithm is the algorithm that performs various substitutions and transformations on the plaintext. Encryption is the process of changing plaintext into cipher text. We refer to encryption and decryption algorithms as ciphers. A cipher (or cypher) is an algorithm for performing encryption or decryption, a series of well-defined steps that can be followed as a procedure. **(April 16, 17)**
  3. **Decryption Algorithm:** The process of changing Ciphertext into plain text is known as decryption. Decryption algorithm is essentially the encryption algorithm run in reverse. It takes the Ciphertext and the key and produces the original plaintext.
  4. **Key:** A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. It also acts as input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key. Thus, a key is a number or a set of number that the algorithm uses to perform encryption and decryption.

3.1.1 Encryption Model **(April 16)**

- Cryptography is the art and science of achieving security by encoding messages to make them non-readable.
- Cryptanalysis is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.
- Cryptology is a combination of cryptography and cryptanalysis. In the early days, cryptography is used to be performed by using manual techniques.
- Today, computers perform these cryptographic functions making the process faster and secure.
- Cleartext or plaintext signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.
- When a plaintext message is codified using any suitable scheme, the resulting message is called as ciphertext.
- Encryption model involves transforming plaintext messages into ciphertext messages that are to be decrypted only by the intended receiver.

- Both sender and receiver agree upon a secrete key to be used in encrypting and decrypting. Usually the secrete key is transmitted via public key encryption methods.
- In the traditional encryption model, there should be at least two parties to perform secure communication.
- Let us take the sender name as Yogita and the receiver name as Amar. Yogita wants to communicate a message with Amar in a secure way.
- In order to do that, the original intelligible message called plaintext is converted into an unintelligible message by Yogita and is sent to Amar.
- To convert the plain-text into ciphertext, the encryption operation takes two parameters as input. They are the original intelligible message (P) and a key (K).
- The key is some bits of information which is generated from a source called key generator.
- The key is generated independently of the plaintext and is used to convert intelligible message from the original unintelligible message (vice versa).
- The encryption algorithm uses an encryption function which will produce different ciphertext values for the same plaintext value using different key values.
- Fig. 3.2 shows a conventional encryption model that consists of three components, namely the sender (Yogita), the receiver (Amar) and the attacker (Eavesdropper).
- The main objective of this model is to enable Yogita and Amar to communicate over an insecure channel in such a way that the attacker (Eavesdropper) should not understand the original plaintext.
- Initially, Yogita is generating the plaintext P and sends it to the encryption algorithm. The encryption algorithm uses an encryption function to convert the plaintext P into the ciphertext C using a key value K.
- After computing the ciphertext, Yogita transmits it through insecure channel. At the receiver side (Amar), the ciphertext is converted back into the original plaintext using the same key with the help of a decryption algorithm.
- According to Kerckhoffs principle, the encryption method is assumed to be known to the attacker (Eavesdropper). However, both the sender and receiver keeps the key as secret.
- As shown in Fig. 3.2, the plaintext P and the key K are given as input to the encryption algorithm to produce the ciphertext C and it can be represented as given below:

  $$C = E_K(P)$$

  where, P = plaintext, K = encryption and decryption key, E = encryption algorithm, C = ciphertext.
- At the receiver side, the ciphertext C and the key K are given as input to the decryption algorithm to produce the plaintext P and it can be represented as given below:

  $$P = D_K(C) = (D_K(E_K(P))) = P$$

  where, D = decryption algorithm

- During the transmission of the ciphertext, an attacker can capture the ciphertext and tries to perform the following actions:
  1. The attacker can find the original plaintext.
  2. The attacker can find the key from which he/she can read all messages that are encrypted with the same key in the future.
  3. Once the key is found, the attacker can modify the original plaintext into another message in such a way that Amar will believe that the message is coming from Yogita.
  4. The attacker makes Amar to believe that Amar is communicating with Yogita.

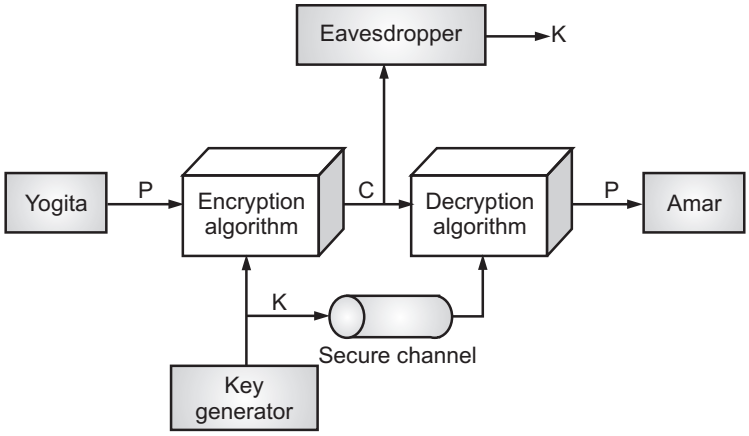


Fig. 3.2: Encryption Model

3.1.2 Basic Terms in Cryptography

- Cryptography also called as secret writing which is used to hide the original message. Cryptography is simply the mathematical "scrambling" of data.
- In this section we will study basic terms used in cryptography like plaintext, ciphertext, cryptograph, cryptology and so on.

1. Plaintext: **(April 19)**

- A message in its original form is called as plaintext. It is the data to be protected during transmission.
- Plaintext is the message to be encrypted (secret text). Data in readable format called as cleartext.

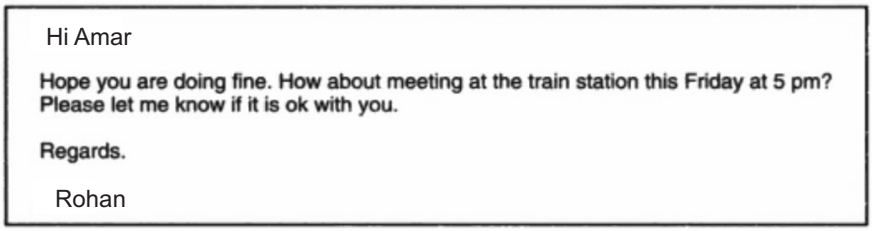


Fig. 3.3: Example of a Plaintext Message

2. Ciphertext: **(April 19)**

- A message in the disguise form is called as ciphertext. It is the encrypted text (Refer Fig. 3.4).
- Ciphertext is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key.

Fig. 3.4: Example of Ciphertext (Encrypted Data)

3. Cryptograph:

- Cryptography is art of codifying messages, so that they become unreadable. It is the science of using mathematics to encrypt and decrypt data.
- Cryptography is the art of secret writing. The user can secure his/her message using different techniques of cryptography. He/she can securely store or transmit the message using these techniques.
- Cryptography is the art and science of achieving security by encoding messages to make them non-readable/unreadable.
- Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

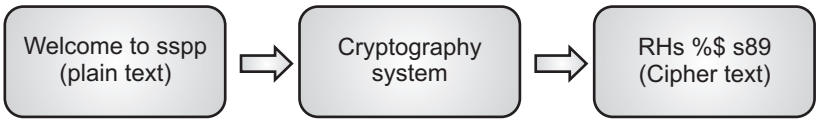


Fig. 3.5: Cryptography System

- Cryptographic systems or cryptosystems convert a plaintext message to a ciphertext message using a cryptographic key.
- The mechanism that applies the key to the message is called a cryptographic algorithm or a cipher. An algorithm for transforming plaintext to ciphertext is called as cipher.
- An algorithm is a step-by-step problem-solving procedure, for solving a problem in a finite number of steps.
- In the context of encryption, an algorithm is the mathematical formula or set of mathematical rules used to scramble and unscramble data.
- A key is specific string of data used to encrypt the plaintext or decrypt the ciphertext. Key is the secret information in a cryptographic operation.

- Some critical information used in the cipher, known only to sender and receiver is called as key.
- The process of converting plaintext to ciphertext using a cipher and a key is called as encryption. The process of converting ciphertext back into plaintext using a cipher and a key is called as description.
- Fig. 3.6 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 crypto-system is that at the end of the process, only the sender and the receiver will know the plaintext.
- Encryption algorithm is a crypto-graphic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
- Decryption algorithm is a crypto-graphic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext.
- The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.

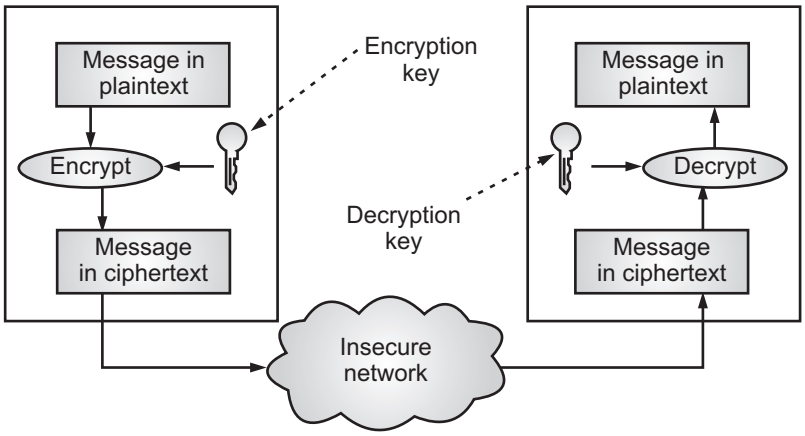


Fig. 3.6

- Encryption key 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 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.
- Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system Symmetric Key Encryption and Asymmetric Key Encryption.

Symmetric Key Encryption:

- The encryption process where same keys are used for encrypting and decrypting the information is known as symmetric key encryption.
- The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems.
- A few well-known examples of symmetric key encryption methods are Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

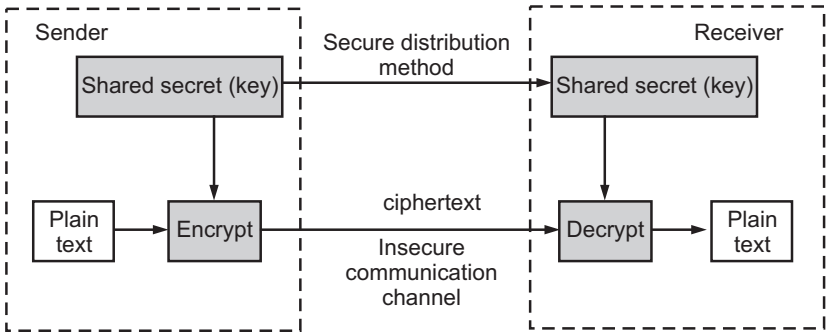


Fig. 3.7: Symmetric Key Encryption

Asymmetric Key Encryption:

- The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption.
- Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible.

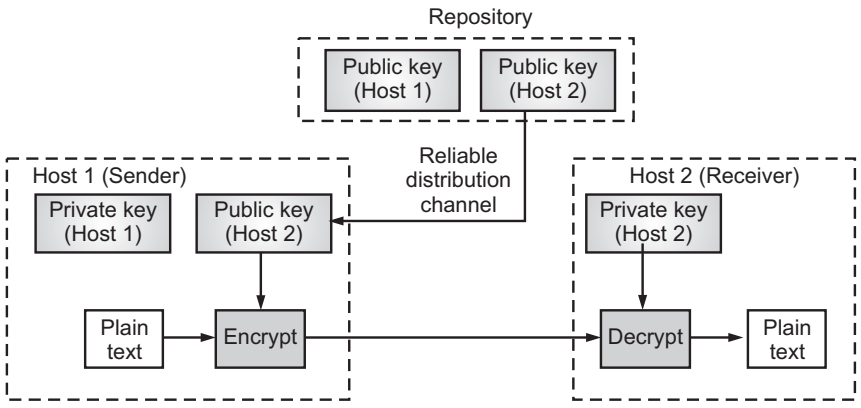


Fig. 3.8: Asymmetric Key Encryption

4. Cryptanalysis:

- The study of principles and methods of transforming ciphertext back into plaintext without knowledge of the key is called as cryptanalysis.
- Cryptanalysis is the process of studying cryptographic systems to look for weaknesses or leaks of information.

- Cryptanalysis is the technique of decoding message from non-readable format back to readable format by trial and error method.
- Cryptanalysis is the art of deciphering the encrypted message/data without knowing the key used for encryption.

5. Cryptology:

- It is the combination of cryptography and cryptanalysis.
- The union/combination of cryptography and cryptanalysis is called as cryptology.

6. Encryption: **(April 16, 19)**

- It is the process of converting plaintext into ciphertext using key.
- Encryption is a technique of translation of data (plaintext) into a secret code (ciphertext).

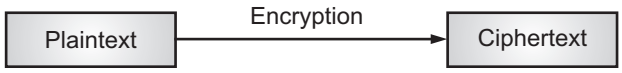


Fig. 3.9

7. Decryption: **(April 19)**

- It is the process of converting cipher text into plain text using key.
- Decryption is a technique of translation of decoded data (ciphertext) into original data (plaintext). A secret key is used for decryption.

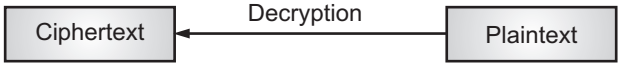


Fig. 3.10

- Fig. 3.11 shows the process of encryption and decryption.
- Encryption is a process of converting normal data or message into an unreadable/encrypted form whereas Decryption is a method of converting the unreadable/encrypted data into its original form.

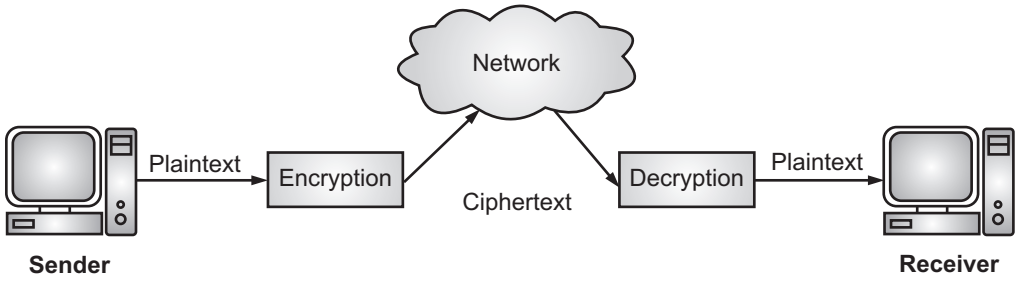


Fig. 3.11

8. Keys:

- A key in cryptography is a piece of information, usually a string of numbers or letters that are stored in a file, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data.

- A cryptographic key is a string of bits used by a cryptographic algorithm to transform plaintext into ciphertext or vice versa. This key remains private and ensures secure communication.
- A key is the core part of cryptography which is a set of values (numbers) that the cipher, as an algorithm, operates on.
- A cryptographic key is categorized according to how it will be used and what properties it has.
- For example, a key might have one of the properties like Symmetric, Public or Private. A key is a set of values (numbers) that the cipher, as an algorithm, operates on.
- Symmetric-key encryption uses the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.
- Asymmetric encryption uses two keys for encryption. Public key is available to anyone while the secret key is only made available to the receiver of the message.
- The key which is known to everyone is known as the public key. The key which is not known to everyone, which is kept as a secret, is known as a private key.
- A public key is usually used for the encryption process at the sender's side. The private key is used for the decryption process at the receiver side.
- In cryptography, a Pre-Shared Key (PSK) is a shared secret which was earlier shared between the two parties using a secure channel before it is used.

3.2 SYMMETRIC KEY CRYPTOGRAPHY

- Symmetric key cryptography (or symmetric encryption) is a type of encryption technique in which the same key is used both to encrypt and decrypt messages.

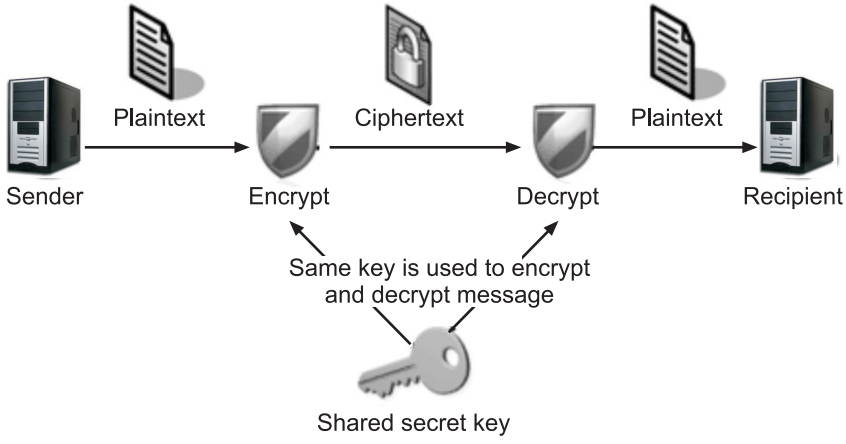


Fig. 3.12: Symmetric Cryptography

- Hence, symmetric key cryptography also called as single key/secret key/shared key cryptography.
- This key is shared between sender and receiver and known to only sender and receiver and no one else.
- In symmetric encryption the plaintext gets encrypted and then converted to the ciphertext using an encryption algorithm and a key.
- On reaching the intended receiver, the ciphertext gets converted back to plain text utilizing the same key that was applied for encryption and a decryption algorithm. The key used can be as easy as a secret number or just a string of letters.

Advantages:

1. **Simple:** This type of encryption is easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages.
2. **Fast:** Symmetric key encryption is much faster than asymmetric key encryption.
3. **Uses Less Computer Resources:** Single-key encryption does not require a lot of computer resources when compared to public key encryption.
4. **Prevents Widespread Message Security Compromise:** A different secret key is used for communication with every different party. If a key is compromised, only the messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.

Disadvantages:

1. **Need for Secure Communication Channel for Secret Key Exchange:** Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures it remains secret.
2. **Too Many Keys:** A new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys.
3. **Origin and Authenticity of Message Cannot be Guaranteed:** Since, both sender and receiver use the same key, messages cannot be verified to have come from a particular user. This may be a problem if there is a dispute.

3.2.1 Traditional Ciphers

- Traditional ciphers are called symmetric key ciphers or secret key ciphers because the same key is used for encryption and decryption and the key can be used for bidirectional communication.
- Fig. 3.13 shows the general idea behind a symmetric key cipher. In Fig. 3.13, an entity, Yogita can send a message to another entity, Amar, over an insecure channel with the assumption that an adversary, Sagar, cannot understand the contents of the message by simply eavesdropping over the channel.

- The original message from Yogita to Amar is called plaintext; the message that is sent through the channel is called the ciphertext.
- To create the ciphertext from the plaintext, Yogita uses an encryption algorithm and a shared secret key.
- To create the plaintext from ciphertext, Amar uses a decryption algorithm and the same secret key.
- We refer to encryption and decryption algorithms as ciphers. A key is a set of values (numbers) that the cipher, as an algorithm, operates on.

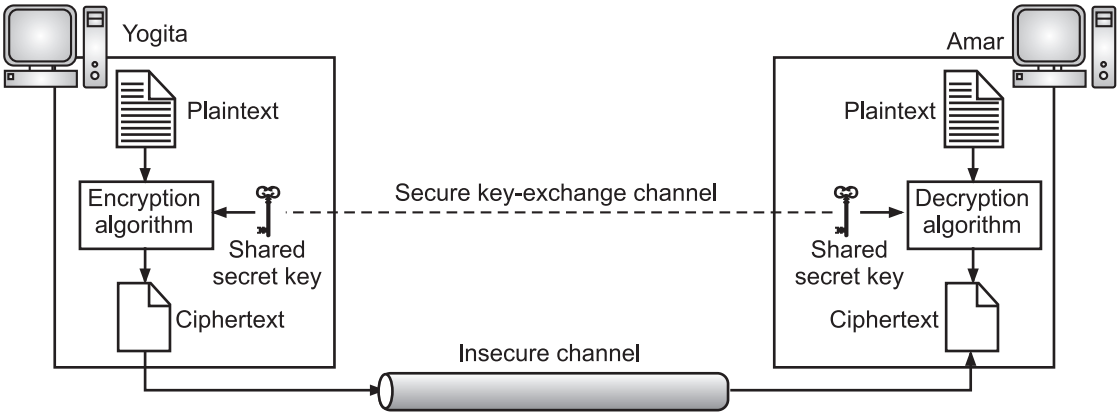


Fig. 3.13: General Idea behind Symmetric Key Cipher

- We can divide traditional symmetric key ciphers into two broad categories namely, substitution ciphers and transposition ciphers.

1. Substitution Cipher: **(April 16. Oct. 17)**

- In a substitution cipher, each letter or group of letters are replaced by another letter or group of letters to disguise it.
- A substitution cipher replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another.
- For example, we can replace letter X with letter Y, and letter A with letter Z. If the symbols are digits (0 to 9), we can replace 3 with 6, and 2 with 7.
- Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers.

Monoalphabetic Cipher:

- Monoalphabetic cipher is a substitution cipher. In a monoalphabetic cipher, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text.
- For example, if the algorithm says that letter A in the plaintext is changed to letter D, every letter A is changed to letter D.

- In monoalphabetic cipher, the relationship between letters in the plaintext and the ciphertext is one-to-one.
- The simplest monoalphabetic cipher is the additive cipher (or shift cipher). In cryptography, a shift cipher, also known as Caesar cipher (proposed by Julius Caesar). The name 'Caesar Cipher' is occasionally used to describe the Shift Cipher when the 'shift of three' is used.
- In additive cipher, the plaintext, ciphertext, and key are integers in modulo 26. Assume that the plaintext consists of lowercase letters (a to z), and that the ciphertext consists of uppercase letters (A to Z). To be able to apply mathematical operations on the plaintext and ciphertext, we assign numerical values to each letter (lower or uppercase), as shown in Fig. 3.14.
- In Fig. each character (lowercase or uppercase) is assigned an integer in modulo 26. The secret key between Yogita and Amar is also an integer in modulo 26.
- The encryption algorithm adds the key to the plaintext character; the decryption algorithm subtracts the key from the ciphertext character. All operations are done in modulo 26.
- The concept of shift cipher is to replace each alphabet by another alphabet which is 'shifted' by some fixed number between 0 and 25.

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Fig. 3.14

Process of Shift Cipher:

- In order to encrypt a plaintext letter, the sender positions the sliding ruler underneath the first set of plaintext letters and slides it to LEFT by the number of positions of the secret shift.
- The plaintext letter is then encrypted to the ciphertext letter on the sliding ruler underneath.
- The result of this process is depicted in the following illustration for an agreed shift of three positions. In this case, the plaintext 'tutorial' is encrypted to the ciphertext 'WXWRULDO'.
- Here, is the ciphertext alphabet for a Shift of 3.

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fig. 3.15

- On receiving the ciphertext, the receiver who also knows the secret shift, positions his sliding ruler underneath the ciphertext alphabet and slides it to RIGHT by the agreed shift number, 3 in this case.
- He then replaces the ciphertext letter by the plaintext letter on the sliding ruler underneath. Hence, the ciphertext 'WXWRULDO' is decrypted to 'tutorial'.
- To decrypt a message encoded with a Shift of 3, generate the plaintext alphabet using a shift of '-3' as shown in Fig. 3.16.

Ciphertext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Alphabet	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Fig. 3.16

- Caesar Cipher is not a secure cryptosystem because there are only 26 possible keys to try out. An attacker can carry out an exhaustive key search with available limited computing resources.

Example: By using Caesar cipher, transform the message 'Happy birthday to you'.

Solution:

Plaintext: Happy birthday to you

Key: Character + 3

Caesar cipher: kdssb eluwkgdb wr brx

Polyalphabetic Cipher:

- Polyalphabetic cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process.
- In polyalphabetic substitution, each occurrence of a character may have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.
- For example, "a" could be enciphered as "D" in the beginning of the text, but as "N" at the middle. Polyalphabetic ciphers have the advantage of hiding the letter frequency of the underlying language.
- To create a polyalphabetic cipher, we need to make each ciphertext character dependent on both the corresponding plaintext character and the position of the plaintext character in the message.
- This implies that our key should be a stream of subkeys, in which each subkey depends somehow on the position of the plaintext character that uses that subkey for encipherment.

2. Transposition Cipher: (April 16, 17, 18, Oct. 17, 18)

- Transposition ciphers differ from substitution ciphers. Transposition ciphers do not simply replace one alphabet with another. They also perform some permutation over to the plaintext alphabet.
- A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.
- A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext.
- A symbol in the eighth position in the plaintext may appear in the first position of the ciphertext. In other words, a transposition cipher reorders (transposes) the symbols.
- The next example is of common transposition method, the columnar transposition. In this method, one key is used which does not contain any repeated letters.
- Columnar transposition is a transposition technique where the plaintext is first written out in n-length rows. The key often represents a keyword of length n that defines the plaintext ordering of columns.
- The ordering could be done by sorting the keyword letters in alphabetical order or in any predefined order.
- Column transposition is a technique in which the message is written in the form of a matrix, row-by-row procedure from top to bottom and left to right.
- After that, the message is read out again column by column depending on the given key value during the encryption process. The row and column size are fixed based on the number of letters available in the plaintext.

Example: Plaintext : Please transfer one million dollar to my swiss bank account six two two.

Key: MEGABUCK.

Solution: Steps:

1. Write the key and give numbers to the alphabets.
2. Write the plaintext horizontally, in rows, padded to fill the matrix if the need be.
3. Write the ciphertext by columns, starting with the column whose key letter is lowest.

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
P	l	e	a	s	e	t	r
A	n	s	f	e	r	o	n
E	m	i	l	l	i	o	n
D	o	l	l	a	r	s	t
O	m	y	s	w	i	s	s
B	a	n	k	a	c	c	o
U	n	t	s	i	x	t	w
O	t	w	o	a	b	c	d

Ciphertext: AFLLSKSOSELAWAIATODSSCTCLNMOMANTESILYNTWRNNTS OWDPAEDOBUOERIRICXB

Example: Consider a plaintext : "How are you when you arrived ?" By using a key NCBTZQARX, use transposition cipher on the plaintext.

Solution: Use transposition cipher on the plaintext.

N	C	B	T	Z	Q	A	R	X
4	3	2	7	9	5	1	6	8
H	o	w	a	R	e	y	o	u
w	h	e	n	Y	o	u	a	r
r	i	v	e	D	a	b	c	d

Ciphertext: YUBWEVOHIHWREOAOACAHEURD

- The literature divides the symmetric ciphers into two broad categories namely, stream ciphers and block ciphers.
- In a stream cipher, encryption and decryption are done one symbol (such as a character or a bit) at a time.
- In stream cipher, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of ciphertext.
- In a block cipher, a group of plaintext symbols of size m (m > 1) are encrypted together, creating a group of ciphertext of the same size.
- Based on the definition, in a block cipher, a single key is used to encrypt the whole block even if the key is made of multiple values. In a block cipher, a ciphertext block depends on the whole plaintext block.

3.2.2 Modern Ciphers

- The traditional symmetric key ciphers are character oriented ciphers. With the advent of the computer, we need bit-oriented ciphers.
- Because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data.
- It is convenient to convert these types of data into a stream of bits, to encrypt the stream, and then to send the encrypted stream.
- In addition, when text is treated at the bit level, each character is replaced by 8 (or 16) bits, which means that the number of symbols becomes 8 (or 16) times larger.
- Mixing a larger number of symbols increases security. A modern block cipher can be either a block cipher or a stream cipher.

1. Modern Block Ciphers:

- In this cipher, the plaintext is processed in blocks (groups) of bits at a time; i.e. a block of plaintext bits is selected, a series of operations is performed on this block to generate a block of ciphertext bits.

- A symmetric key modern block cipher encrypts an n-bit block of plaintext or decrypts an n-bit block of ciphertext. The encryption or decryption algorithm uses a k-bit key.
- The decryption algorithm must be the inverse of the encryption algorithm, and both operations must use the same secret key so that Amar can retrieve the message sent by Yogita.
- Fig. 3.17 (a) shows the general idea of encryption and decryption in a modern block cipher.
- If the message has fewer than n bits, padding must be added to make it an n-bit block; if the message has more than n bits, it should be divided into n-bit blocks and the appropriate padding must be added to the last block if necessary. The common values for n are 64, 128, 256, and 512 bits.

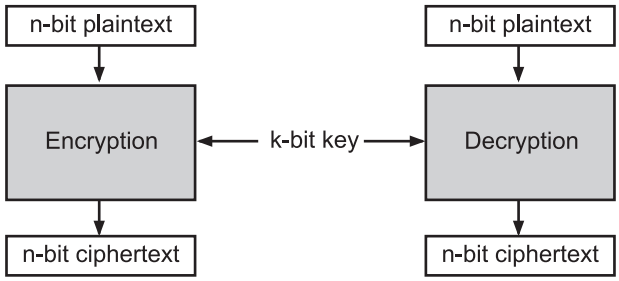


Fig. 3.17 (a): Modern Block Cipher

- Modern block ciphers normally are keyed substitution ciphers in which the key allows only partial mappings from the possible inputs to the possible outputs.
- Modern block ciphers are substitution ciphers when seen as a whole block. However, modern block ciphers are not designed as a single unit.
- To provide an attack-resistant cipher, a modern block cipher is made of a combination of transposition units (sometimes called P-boxes), substitution units (sometimes called S-boxes) and exclusive-or (XOR) operations, shifting elements, swapping elements, splitting elements and combining elements.
- Fig. 3.17 (b) shows the components of a modern block cipher.
- A **P-box (permutation box)** parallels the traditional transposition cipher for characters, but it transposes bits.
- We can find three types of P-boxes in modern block cipher namely, straight P-boxes, expansion P-boxes, and compression P-boxes.
- An **S-box (substitution box)** can be thought of as a miniature substitution cipher, but it substitutes bits.
- Unlike the traditional substitution cipher, an S-box can have a different number of inputs and outputs.

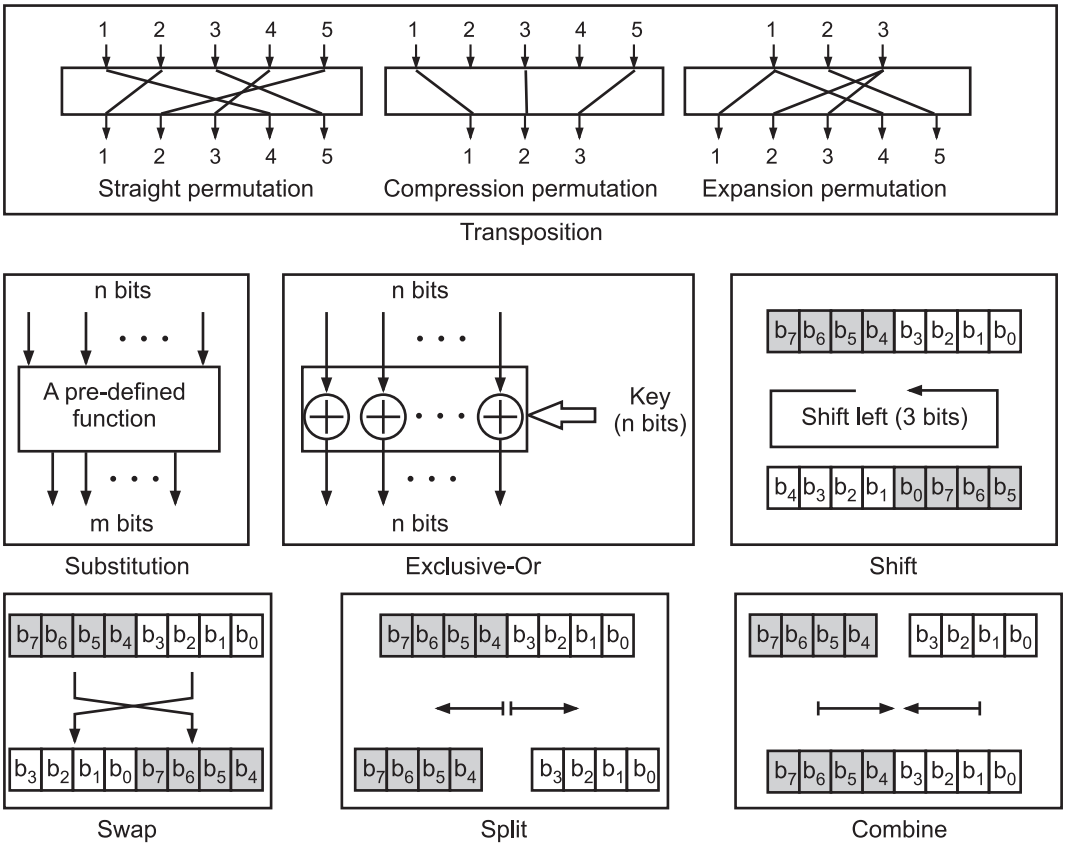


Fig. 3.17 (b): Components of a Modern Block Cipher

- An important component in most modern block ciphers is the **exclusive-or (XOR) operation**, in which the output is 0 if the two inputs are the same, and the output is 1 if the two inputs are different.
- In modern block ciphers, we use n exclusive-or operations to combine an n-bit data piece with an n-bit key. An exclusive-or operation is normally the only unit where the key is applied.
- Another component found in some modern block ciphers is the **circular shift operation**. Shifting can be to the left or to the right.
- The circular left-shift operation shifts each bit in an n-bit word k positions to the left; the leftmost k bits are removed from the left and become the rightmost bits.
- The **swap operation** in modern block cipher is a special case of the circular shift operation where the number of shifted bits k = n/2.
- Two other operations found in some modern block ciphers are split and combine. The **split operation** splits an n-bit word in the middle, creating two equal-length words.
- The **combine operation** normally concatenates two equal-length words to create an n-bit word.

2. Modern Stream Ciphers:

- we can also use modern stream ciphers like modern block ciphers. Stream ciphers are faster than block ciphers. Modern stream ciphers uses a block size of one bit.
- In a modern stream cipher, encryption and decryption are done r bits at a time. We have a plaintext bit stream P = p_n p_2p_1, a ciphertext bit stream C = c_n c_2c_1, and a key bit stream K = k_n k_2k_1, in which p_i , c_i , and k_i are r-bit words. Encryption is $c_i = E (k_i, p_i)$, and decryption is pi = D (k_i, c_i).
- The hardware implementation of a stream cipher is also easier. When we need to encrypt binary streams and transmit them at a constant rate, a stream cipher is the better choice to use. Stream ciphers are also more immune to the corruption of bits during transmission.
- The simplest and the most secure type of stream cipher is called the one-time pad, which was invented and patented by Gilbert Vernam in 1918.
- A one-time pad cipher uses a key stream that is randomly chosen for each encipherment. The encryption and decryption algorithms each use a single exclusive-or operation.
- Based on properties of the exclusive-or operation, the encryption and decryption algorithms are inverses of each other. It is important to note that in this cipher the exclusive-or operation is used one bit at a time.
- Note also that there must be a secure channel so that Yogita can send the key stream sequence to Amar as shown in Fig. 3.18.

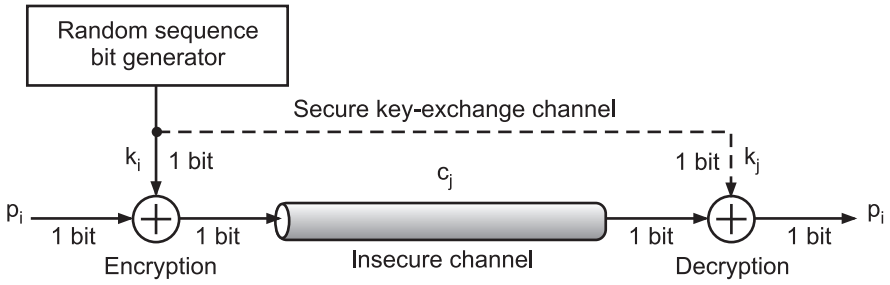


Fig. 3.18: One-time Pad Cipher

3.2.3 Modern Round Ciphers

- In this section we will study modern cipher such as AES.

Data Encryption Standard (DES):

- The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).
- DES is a symmetric key algorithm, which means that the same key is used for encrypting and decrypting data.

- The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data.
- General structure of DES is shown in Fig. 3.19. DES uses 16 rounds. The block size is 64-bit. DES is also called as Data Encryption Algorithm (DEA).
- At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit ciphertext; at the decryption site, DES takes a 64-bit ciphertext and creates a 64-bit block of plaintext. The same 56-bit cipher key is used for both encryption and decryption.

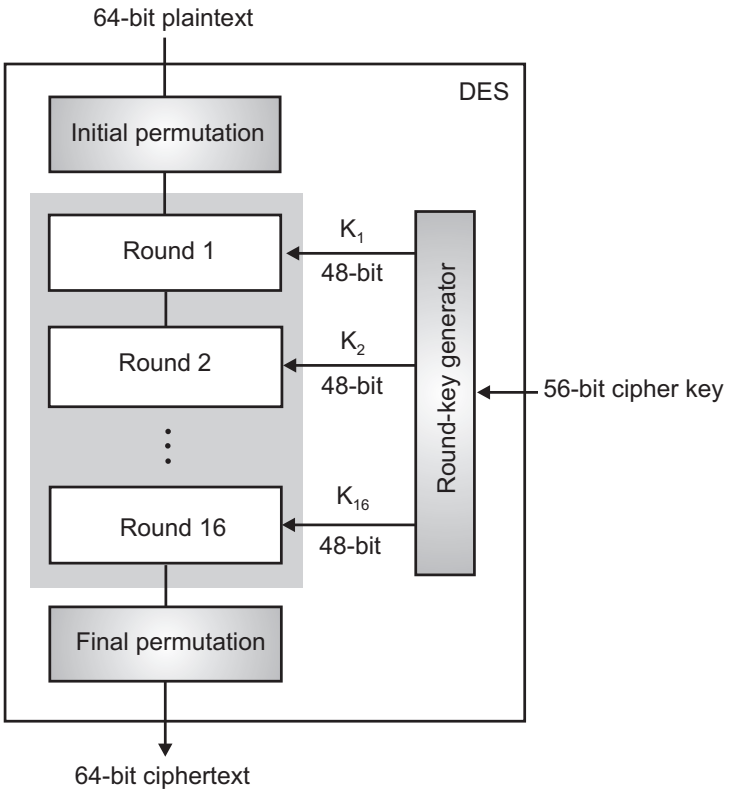


Fig. 3.19: Structure of DES

- DES contains Round function, Key schedule and any additional processing – initial and final permutation.

Initial and Final Permutation:

- The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES.
- The initial permutations takes a 64-bit input and permutes them according to a predefined rule. The final permutation is the inverse of the initial permutation.
- The initial and final permutations are shown in Fig. 3.20.

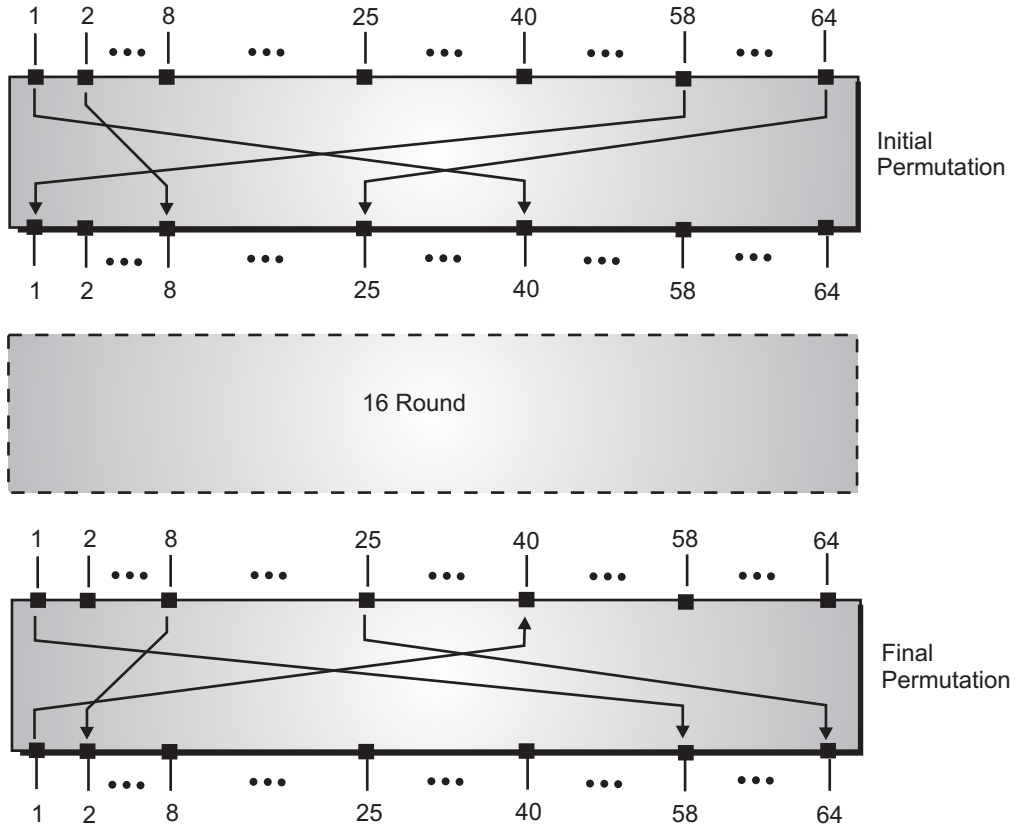


Fig. 3.20

DES Rounds:

- DES uses 16 rounds and each round of DES is an invertible transformation, as shown in Fig. 3.21.
- The round takes L_{I-1} and R_{I-1} from the previous round (or the initial permutation box) and creates L_I and R_I, which go to the next round (or final permutation box).
- Each round can have up to two cipher elements (mixer and swapper). Each of these elements is invertible. The swapper is obviously invertible. It swaps the left half of the text with the right half.

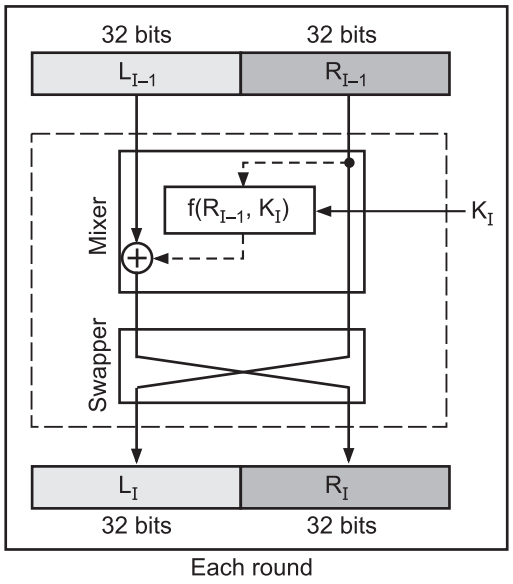


Fig. 3.21

- The mixer is invertible because of the XOR operation. All noninvertible elements are collected inside the function f (R_{I-1}, K_I).

DES Function:

- The heart of this cipher is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.
- DES function is made up of four sections: an expansion P-box, an exclusive-OR component (that adds key), a group of S-boxes, and a straight P-box, as shown in Fig. 3.22.
- **Expansion Permutation Box:** Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically shown in the Fig. 3.23.

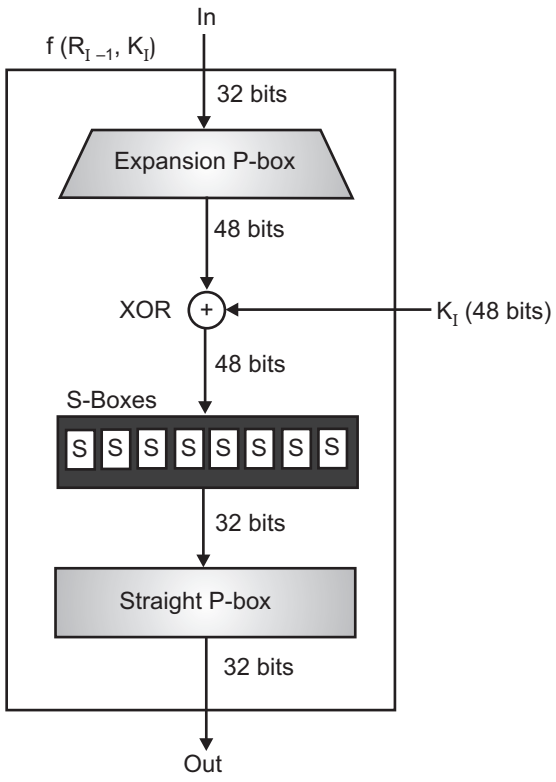


Fig. 3.22

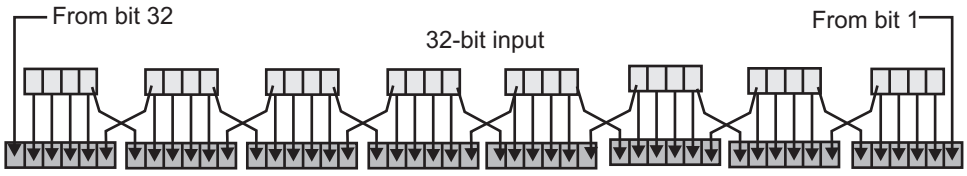


Fig. 3.23

- The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown in Fig. 3.24.

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Fig. 3.24

- **XOR (Whitener):** After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
- **Substitution Boxes:** The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output, (See Fig. 3.25).

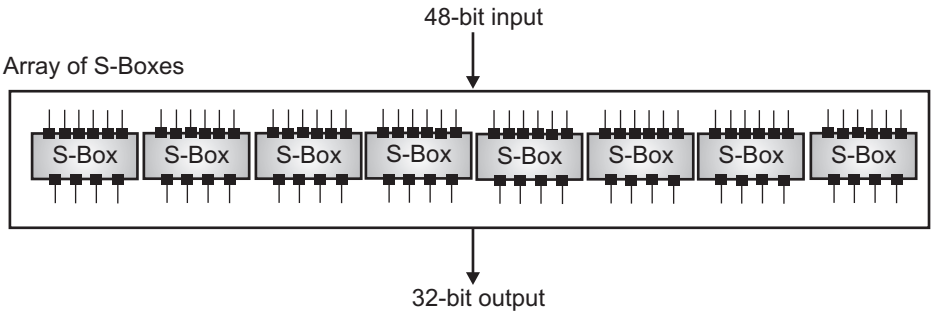


Fig. 3.25

- The S-box rule is illustrated in Fig. 3.26.

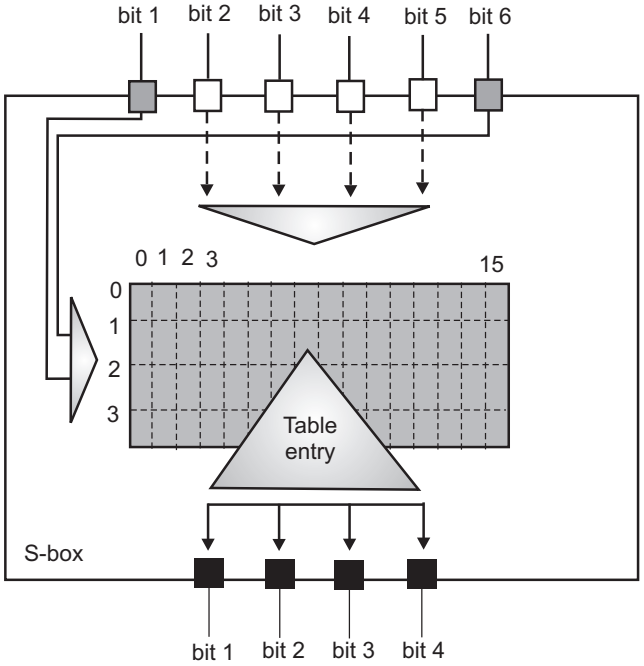


Fig. 3.26

- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.
- **Straight Permutation:** The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in Fig. 3.27.

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Fig. 3.27

Key Generation:

- The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.
- The process of key generation is depicted in the Fig. 3.28.

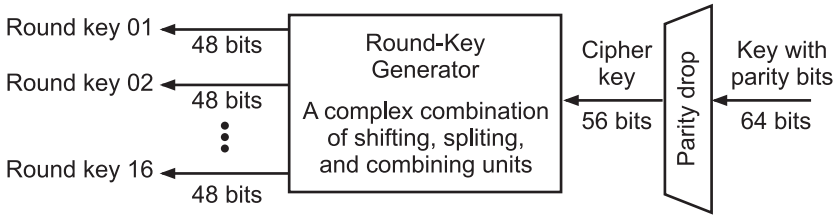


Fig. 3.28

- Consequently two main variations of DES have emerged, which are Double DES and Triple DES.
  1. In **double DES**, two symmetric keys were used for encryption and decryption, however double DES also had some limitations. With regard to this context, triple DES was introduced in the year 1999 by a team led by Walter Tuchman who was working at IBM.
  2. **Triple DES** resolved all the limitations of double DES by using three symmetric keys as well as two symmetric keys. Moreover, triple DES is extensively used in many of the Internet protocols in today's environment.

3.2.4 Block Cipher Modes of Operation

- In this section, we will discuss the different modes of operation of a block cipher. These are procedural rules for a generic block cipher.
- Interestingly, the different modes result in different properties being achieved which add to the security of the underlying block cipher. A block cipher processes the data blocks of fixed size.
- Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time.

Electronic Code Book (ECB) Mode:

- This mode is a most straightforward way of processing a series of sequentially listed message blocks.

Operation:

- The user takes the first block of plaintext and encrypts it with the key to produce the first block of ciphertext.
- He then takes the second block of plaintext and follows the same process with same key and so on so forth.

- The ECB mode is deterministic, that is, if plaintext block P_1, P_2, ..., P_m are encrypted twice under the same key, the output ciphertext blocks will be the same.
- In fact, for a given key technically we can create a codebook of ciphertexts for all possible plaintext blocks. Encryption would then entail only looking up for required plaintext and select the corresponding ciphertext.
- Thus, the operation is analogous to the assignment of code words in a codebook, and hence gets an official name – Electronic Codebook mode of operation (ECB). It is illustrated in Fig. 3.29.

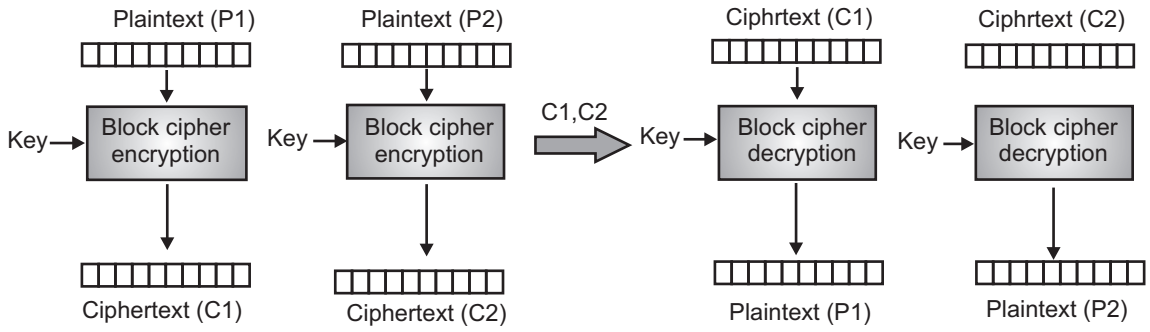


Fig. 3.29

Analysis of ECB Mode:

- In reality, any application data usually have partial information which can be guessed. For example, the range of salary can be guessed. A ciphertext from ECB can allow an attacker to guess the plaintext by trial-and-error if the plaintext message is within predictable.
- For example, if a ciphertext from the ECB mode is known to encrypt a salary figure, then a small number of trials will allow an attacker to recover the figure.
- In general, we do not wish to use a deterministic cipher, and hence the ECB mode should not be used in most applications.

Cipher Block Chaining (CBC) Mode:

- CBC mode of operation provides message dependence for generating ciphertext and makes the system non-deterministic.

Operation:

- The operation of CBC mode is depicted in the following illustration. The steps are as follows:
  - Load the n-bit Initialization Vector (IV) in the top register.

- XOR the n-bit plaintext block with data value in top register.
- Encrypt the result of XOR operation with under-lying block cipher with key K.
- Feed ciphertext block into top register and continue the operation till all plain-text blocks are processed.
- For decryption, IV data is XORed with first ciphertext block decrypted. The first ciphertext block is also fed into to register replacing IV for decrypting next ciphertext block.

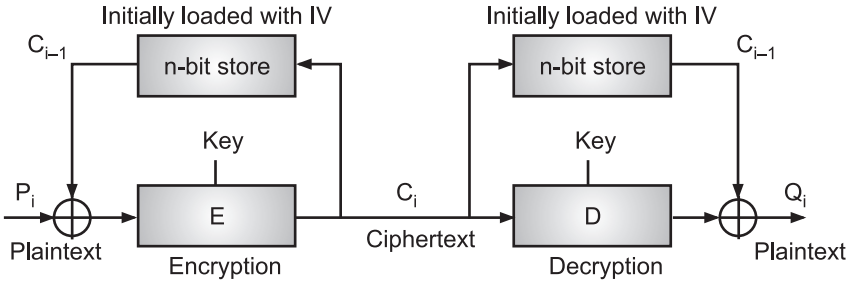


Fig. 3.30

Analysis of CBC Mode:

- In CBC mode, the current plaintext block is added to the previous ciphertext block, and then the result is encrypted with the key.
- Decryption is thus the reverse process, which involves decrypting the current ciphertext and then adding the previous ciphertext block to the result.
- Advantage of CBC over ECB is that changing IV results in different ciphertext for identical message. On the drawback side, the error in transmission gets propagated to few further block during decryption due to chaining effect.
- It is worth mentioning that CBC mode forms the basis for a well-known data origin authentication mechanism. Thus, it has an advantage for those applications that require both symmetric encryption and data origin authentication.

Cipher Feedback (CFB) Mode:

- In this mode, each ciphertext block gets 'fed back' into the encryption process in order to encrypt the next plaintext block.

Operation:

- The operation of CFB mode is depicted in the following illustration. For example, in the present system, a message block has a size 's' bits where $1 < s < n$.
- The CFB mode requires an initialization vector (IV) as the initial random n-bit input block. The IV need not be secret.
- Steps of operation are given below:
  - Load the IV in the top register.
  - Encrypt the data value in top register with underlying block cipher with key K.

- Take only 's' number of most significant bits (left bits) of output of encryption process and XOR them with 's' bit plaintext message block to generate ciphertext block.
- Feed ciphertext block into top register by shifting already present data to the left and continue the operation till all plaintext blocks are processed.
- Essentially, the previous ciphertext block is encrypted with the key, and then the result is XORed to the current plaintext block.
- Similar steps are followed for decryption. Pre-decided IV is initially loaded at the start of decryption.

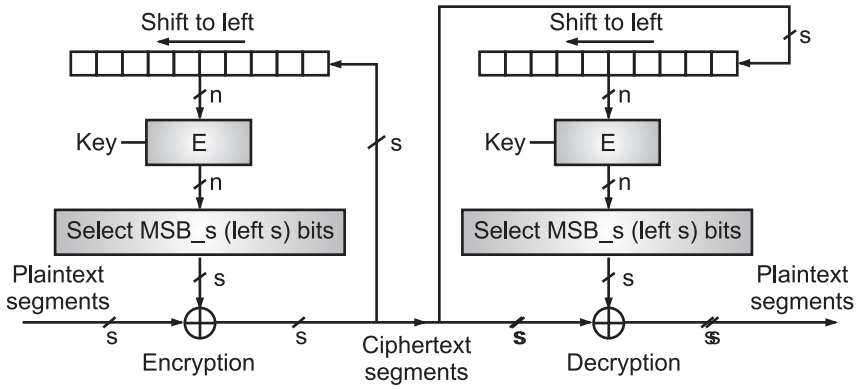


Fig. 3.31

Analysis of CFB Mode:

- CFB mode differs significantly from ECB mode, the ciphertext corresponding to a given plaintext block depends not just on that plaintext block and the key, but also on the previous ciphertext block. In other words, the ciphertext block is dependent of message.
- CFB has a very strange feature. In this mode, user decrypts the ciphertext using only the encryption process of the block cipher. The decryption algorithm of the underlying block cipher is never used.
- Apparently, CFB mode is converting a block cipher into a type of stream cipher. The encryption algorithm is used as a key-stream generator to produce key-stream that is placed in the bottom register. This key stream is then XORed with the plaintext as in case of stream cipher.
- By converting a block cipher into a stream cipher, CFB mode provides some of the advantageous properties of a stream cipher while retaining the advantageous properties of a block cipher.
- On the flip side, the error of transmission gets propagated due to changing of blocks.

Output Feedback (OFB) Mode:

- It involves feeding the successive output blocks from the underlying block cipher back to it. These feedback blocks provide string of bits to feed the encryption algorithm which act as the key-stream generator as in case of CFB mode.
- The key stream generated is XORed with the plaintext blocks. The OFB mode requires an IV as the initial random n-bit input block. The IV need not be secret.
- The operation is depicted in the Fig. 3.32.

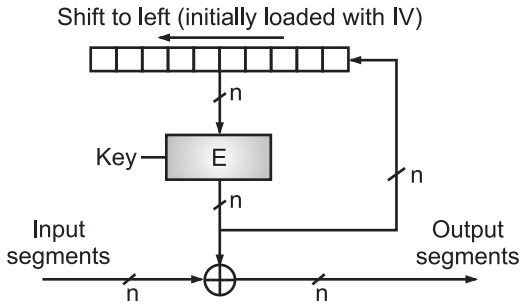


Fig. 3.32

Counter (CTR) Mode:

- It can be considered as a counter-based version of CFB mode without the feedback.
- In this mode, both the sender and receiver need to access to a reliable counter, which computes a new shared value each time a ciphertext block is exchanged. This shared counter is not necessarily a secret value, but challenge is that both sides must keep the counter synchronized.

Operation:

- Both encryption and decryption in CTR mode are depicted in the following illustration. Steps in operation are:
  - Load the initial counter value in the top register is the same for both the sender and the receiver. It plays the same role as the IV in CFB (and CBC) mode.
  - Encrypt the contents of the counter with the key and place the result in the bottom register.
  - Take the first plaintext block P1 and XOR this to the contents of the bottom register. The result of this is C1. Send C1 to the receiver and update the counter. The counter update replaces the ciphertext feedback in CFB mode.
  - Continue in this manner until the last plaintext block has been encrypted.

- The decryption is the reverse process. The ciphertext block is XORed with the output of encrypted contents of counter value. After decryption of each ciphertext block counter is updated as in case of encryption.

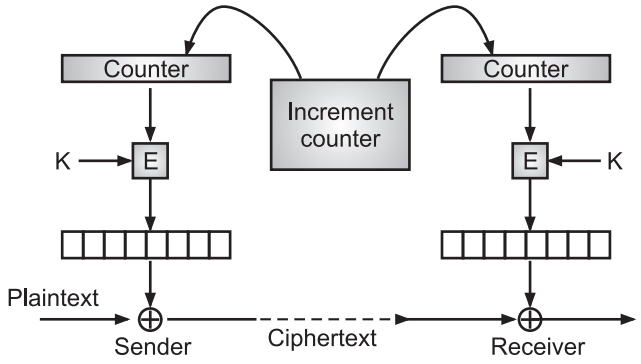


Fig. 3.33

Analysis of Counter Mode:

- It does not have message dependency and hence a ciphertext block does not depend on the previous plaintext blocks.
- Like CFB mode, CTR mode does not involve the decryption process of the block cipher. This is because the CTR mode is really using the block cipher to generate a key-stream, which is encrypted using the XOR function. In other words, CTR mode also converts a block cipher to a stream cipher.
- The serious disadvantage of CTR mode is that it requires a synchronous counter at sender and receiver. Loss of synchronization leads to incorrect recovery of plaintext.
- However, CTR mode has almost all advantages of CFB mode. In addition, it does not propagate error of transmission at all.

3.3 ASYMMETRIC KEY CRYPTOGRAPHY

- Asymmetric Encryption also called as Public Key Cryptography and it uses two different keys - a public key used for encryption and a private key used for decryption.
- This encryption technique utilizes a pair of keys (a public key and a private key) for the encryption and decryption processes. The public key is normally used for encryption while the private key is applied for decryption of the message.
- Whereas, the public key can be made freely available to any person who might be interested in sending a message, the private key remains a secret well kept by the receiver of the message.
- A message encrypted using a public key and an algorithm will be decrypted using the same algorithm plus a matching private key that corresponds to the public key used.

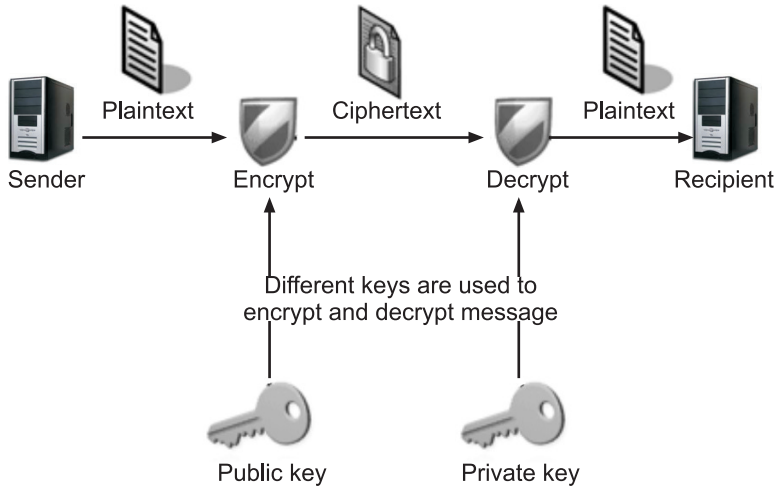


Fig. 3.34: Asymmetric Key Cryptography

Advantages:

1. **Convenience:** It solves the problem of distributing the key for encryption. Everyone publishes their public keys and private keys are kept secret.
2. **Provides for Message Authentication:** Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender.
3. **Detection of Tampering:** The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.
4. **Provide for Non-Repudiation:** Digitally signing a message is similar to physically signing a document. It is an acknowledgement of the message and thus the sender cannot deny it.

Disadvantages:

1. **Public Keys should/must be Authenticated:** No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.
2. **Slow:** Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages.
3. **Uses more Computer Resources:** It requires a lot more computer supplies compared to single- key encryption.
4. **Loss of Private key may be Irreparable:** The loss of a private key means that all received messages cannot be decrypted.

Comparison between Symmetric Key Cryptography and Asymmetric Key Cryptography:

Sr. No.	Symmetric Key Cryptography	Asymmetric Key Cryptography
1.	It uses a single key (secret key) for both encryption and decryption of data.	It uses two different keys public key for encryption and private key for decryption.
2.	Both the communicating parties share the same algorithm and the key.	Both the communicating parties should have at least one of the matched pair of keys.
3.	The processes of encryption and decryption are very fast.	The encryption and decryption processes are slower.
4.	Key distribution is a big problem.	Key distribution is not a problem.
5.	The size of encrypted text is usually same or less than the original text.	The size of encrypted text is usually more than the size of the original text.
6.	Based on substitution and permutation of symbols (characters or bits).	Based on applying mathematical functions to numbers.
7.	It can only be used for confidentiality, i.e., only for encryption and decryption of data.	It can be used for confidentiality of data as well as for integrity and non-repudiation checks (i.e., far digital signatures).
8.	DES and AES are the commonly used symmetric-encryption algorithms.	The most commonly used asymmetric-encryption algorithm is RSA.

3.3.1 RSA Encryption Algorithm

- RSA is an encryption algorithm, used to securely transmit messages over the internet. RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission.
- In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private).
- In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem".
- RSA cryptography (the RSA algorithm to be exact) is the most ubiquitous asymmetric encryption algorithm in the world.
- The RSA algorithm is the basis of a cryptosystem - a suite of cryptographic algorithms that are used for specific security services or purposes - which enables public key

encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet.

- We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

1. 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 and 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:

      $e^d = 1 \bmod (p - 1)(q - 1)$

    - The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example:

- An example of generating RSA Key pair is given below. (For ease of understanding, the primes p and 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 = $7 \times 13 = 91$.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and $(p - 1)(q - 1) = 6 \times 12 = 72$, 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:

  $d^e = 29 \times 5 = 145 = 1 \bmod 72$

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

2. Encryption and Decryption:

- Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.
- Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

RSA Encryption:

- Suppose the sender wish to send some text message to someone whose public key is (n, e). The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as:

  $C = P^e \bmod n$

- In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.
- Returning to our Key Generation example with plaintext P = 10, we get ciphertext C:

  $C = 10^5 \bmod 91$

RSA Decryption:

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a ciphertext C.
- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

  $\text{Plaintext} = C^d \bmod n$

- Returning again to our numerical example, the ciphertext C = 82 would get decrypted to number 10 using private key 29.

  $\text{Plaintext} = 82^{29} \bmod 91 = 10$

- Fig. 3.35 shows the general idea behind the procedure used in RSA.

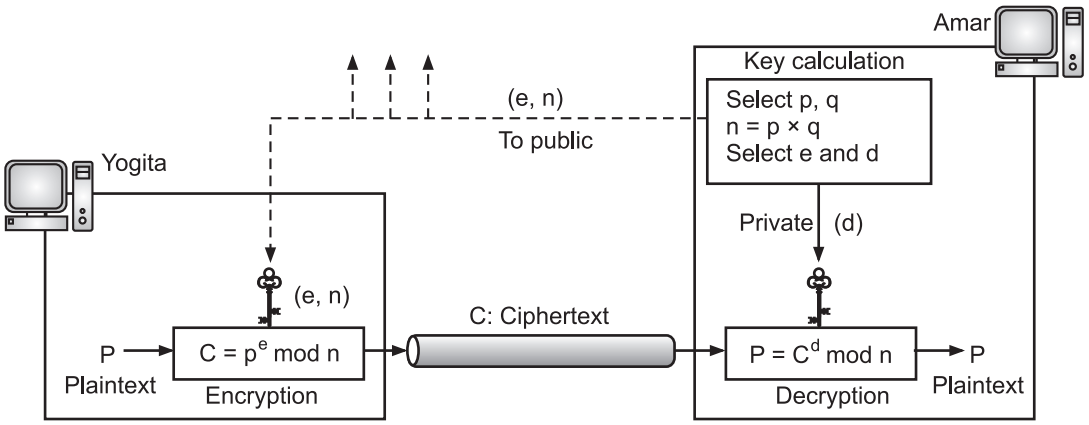


Fig. 3.35: Encryption, Decryption, and Key Generation in RSA

RSA Analysis:

- The security of RSA depends on the strengths of two separate functions. The RSA cryptosystem is most popular public-key cryptosystem strength of which is based on the practical difficulty of factoring the very large numbers.
  - **Encryption Function:** It is considered as a one-way function of converting plaintext into ciphertext and it can be reversed only with the knowledge of private key d.
  - **Key Generation:** The difficulty of determining a private key from an RSA public key is equivalent to factoring the modulus n. An attacker thus cannot use knowledge of an RSA public key to determine an RSA private key unless he can factor n. It is also a one way function, going from p and q values to modulus n is easy but reverse is not possible.
- If either of these two functions are proved non one-way, then RSA will be broken. In fact, if a technique for factoring efficiently is developed then RSA will no longer be safe.
- The strength of RSA encryption drastically goes down against attacks if the number p and q are not large primes and/ or chosen public key e is a small number.

3.4 SECURITY SERVICES

- Security is a fundamental component of every network design. When planning, building, and operating a network, you should understand the importance of a strong security policy.
- Network security consists of the policies adopted to prevent and monitor authorized access, misuse, modification, or denial of a computer network and network-accessible resources.

- Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
- Network security can provide one of the five services as illustrated in Fig. 3.36.
- Four of these network security services are related to the message exchanged i.e., message confidentiality, integrity, authentication, and non-repudiation. The fifth service of network security provides entity authentication or identification.

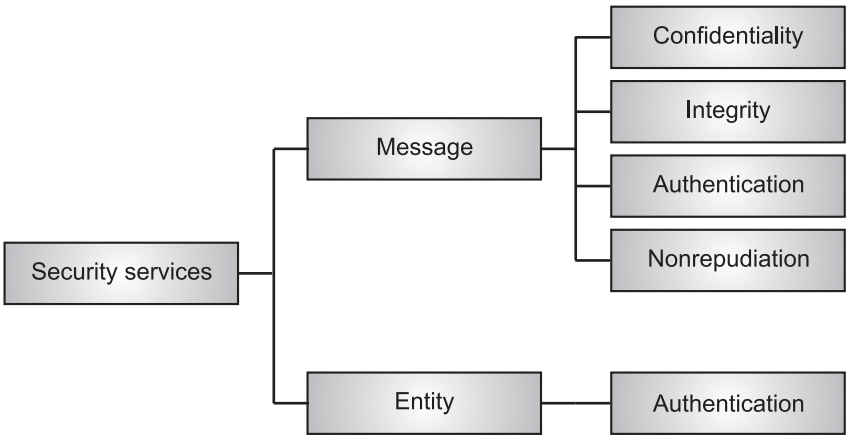


Fig. 3.36: Network Security Services

- Fig. 3.36 Shows following types of services:
  1. **Confidentiality:** The principle of confidentiality specifies that only the sender and the intended recipient(s) should be able to access the content of a message. Example of compromising the confidentiality is shown in Fig 3.37. In this example a confidential email message sent by A to B which is accessed by C, without the permission or knowledge of A and B. This type of attack is called as interception.

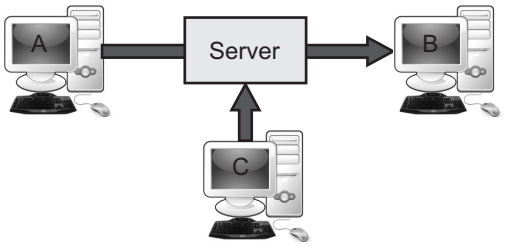


Fig. 3.37: Loss of Confidentiality

  2. **Integrity:** When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, the integrity of a message is lost. This type of attack is called as modification.

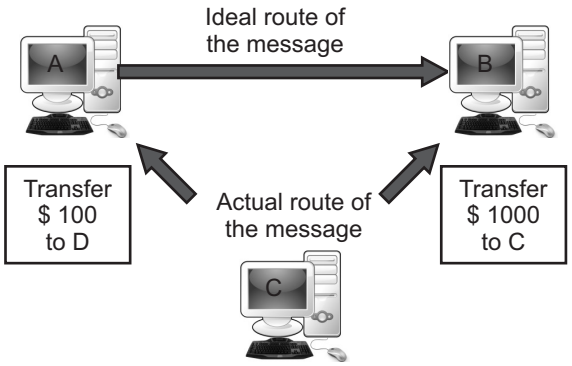


Fig. 3.38: Loss of Integrity

3. **Authentication:** Authentication mechanism help establish proof of identities. The authentication process ensures that the origin of an electronic message or document is correctly identified. For example, consider user C, posing as user A, sending a funds transfer request(from A's account to C's account) to bank B. The bank may transfer the funds from A's account to C's account, thinking that user A has requested for the fund transfer. This type of attack is called as fabrication.

Fig. 3.39: Absence of Authentication

4. **Non-repudiation:** There are situations where a user sends a message, and later on refuses that he/she sent that message. Consider user A send a funds transfer request to bank B. After the bank performs the funds transfer as per A's instructions, A could claim that he never sent funds transfer instructions to bank. Thus A denies funds transfer instruction. The principle of non-repudiation defeats such possibilities of denying something, having done it.
5. **Entity (User) Authentication:** In entity authentication or user authentication the entity or user is verified prior to access the system resources. Consider user A want to access his bank account needs to be authenticated during the logging process.

3.4.1 Message Confidentiality

- To achieve the message confidentiality or privacy one technique is used from thousands of years, i.e. encryption.

- In technical terms, the process of encoding plain text message into cipher text message is called encryption.

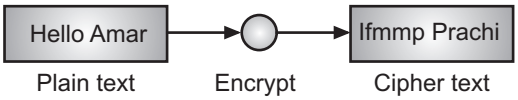


Fig. 3.40: Encryption

- The reverse process of transforming cipher text message back to plain text messages is called decryption.

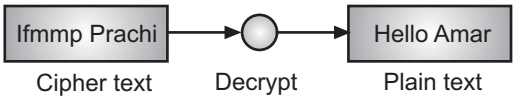


Fig. 3.41: Decryption

- In communication a plain text signifies a message that can be understood by the sender, the recipient, and also by anyone else who gets an access to that message.

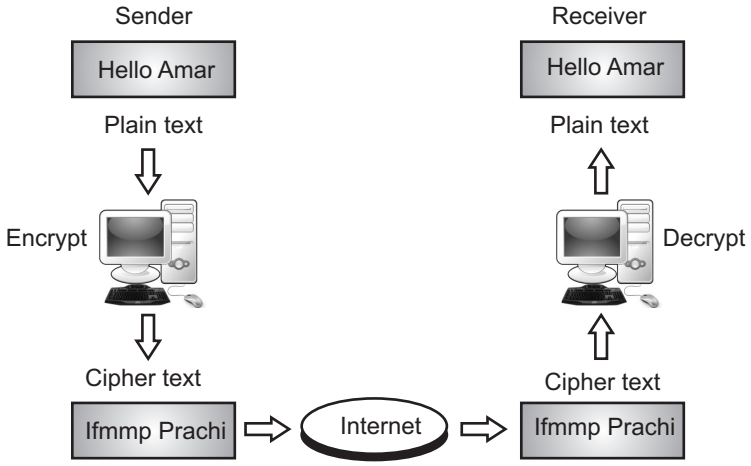


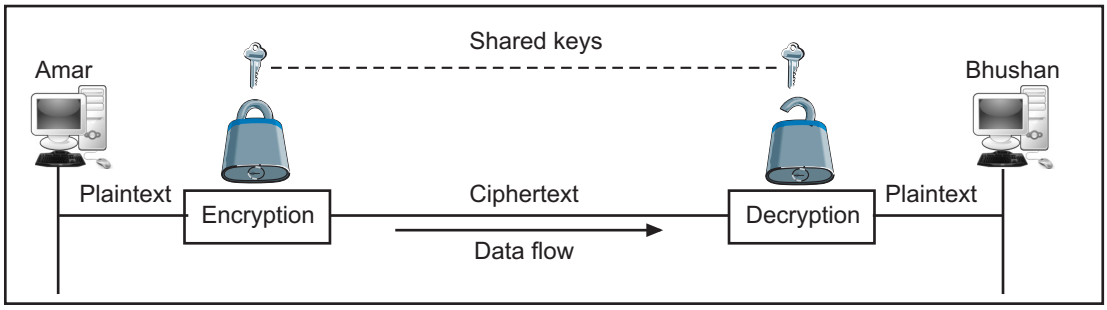
Fig. 3.42: Encryption and decryption in the real world

- When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.
- The message must be encrypted at the sender site and decrypted at the receiver site. This can be done using either symmetric-key cryptography or asymmetric-key cryptography.

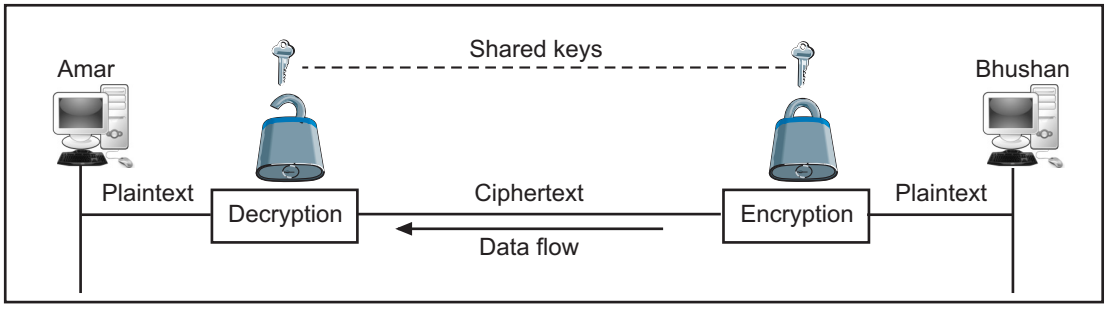
Confidentiality with Symmetric Key Cryptography:

- As we know, to achieve encryption we can use symmetric key or asymmetric key cryptography.
- In symmetric key cryptography, same key is used by sender for encryption and by receiver for decryption respectively. Here sender and receiver needs to share a secrete symmetric key.
- In the past when data exchange was between two specific persons, it was possible to personally exchange the secret keys.

- But now a days, communication by using computers and users seating at two different locations in the world, exchanging a key personally becomes highly impossible.
- A solution is required for key sharing. This can done using a session key. A session key is one that is used only for the duration of one session. This session key is exchanged using asymmetric key cryptography.
- Fig. 3.43 shows the use of session symmetric key for sending confidential message from Amar to Bhushan and vice versa.
- In the Fig. 3.43 one shared key is used in both directions. But using two different keys for each direction is more secured.
- For long message, symmetric key cryptography is very fast and more efficient than asymmetric key cryptography.
- Fig. 3.43 shows the use of a session symmetric key for sending confidential messages from Amar to Bhushan and vice versa.



(a) A Shared Secret Key can be used in Amar-Bhushan Communication



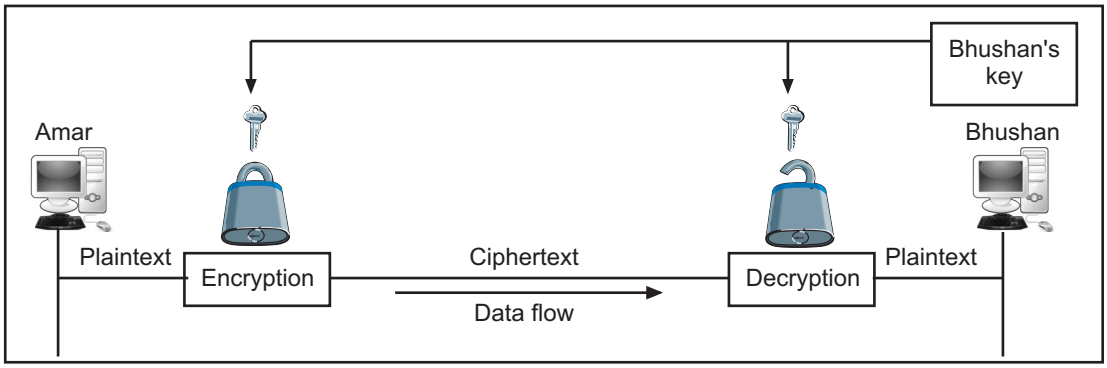
(b) A different Shared Secret key is recommended in Bhushan-Amar communication

Fig. 3.43

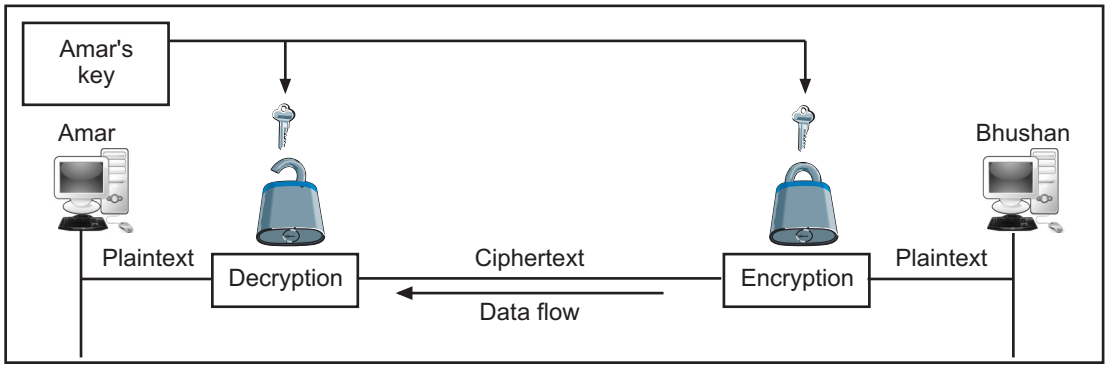
Confidentiality with Asymmetric Key Cryptography:

- Symmetric key cryptography is fast and efficient. However it suffers from a big disadvantage of the problem of key exchange.
- Asymmetric key cryptography solve this problem. Here, each communicating party uses two keys to form a key pair. One key (the private key) remains with the party, and the other key (the public key) is shared with everybody by announcing it publically.

- One key is used for encryption and only the other corresponding key must be used for decryption. No other key can decrypt the message, not even the original key used for encryption.
- Consider, Amar and Bhushan wants to do secure communication by using asymmetric key cryptography. Both of them needs a pair of key. Public key, known to all and private key known to themselves only.
- Asymmetric key cryptography works as follows:
  1. When Amar wants to send a message to Bhushan, he encrypts the message using Bhushan's public key. This is possible because Amar knows Bhushan's public key.
  2. Amar sends encrypted message to Bhushan.
  3. Bhushan decrypts Amar's message by using his own private key, which is known to him only.
  4. Similarly Bhushan can send a message to Amar, exactly reverse step take place.
- Fig. 3.44 message confidentiality using asymmetric keys.



(a) Bhushan's Keys are used in Amar-Bhushan Communication



(b) Amar's Keys are used in Bhushan-Amar Communication

Fig. 3.44

3.4.2 Message Integrity

- Message integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes of modifications in the data content during transmission, either maliciously or accident, in a transit.

Message and Message Digest:

- Message integrity describes the concept of ensuring that data has not been modified or altered in transit.
- One way to preserve the integrity of a document is through the use of a fingerprint. If Yogita needs to be sure that the contents of her document will not be changed, she can put her fingerprint at the bottom of the document.
- Sagar cannot modify the contents of this document or create a false document because she cannot forge Yogita's fingerprint.
- To ensure that the document has not been changed, Yogita's fingerprint on the document can be compared to Yogita's fingerprint on file.
- If they are not the same, the document is not from Yogita. The electronic equivalent of the document and fingerprint pair is the message and digest pair.
- To preserve the integrity of a message, the message is passed through an algorithm called a cryptographic hash function.
- The hash function creates a compressed image of the message, called a digest, which can be used like a fingerprint. Message digest ensures the integrity of the document.
- To check the integrity of a message, or document, Amar runs the cryptographic hash function again and compares the new digest with the previous one.
- If both are the same, Amar is sure that the original message has not been changed. Fig. 3.45 shows the idea of message and digest.
- Message digest is used to ensure the integrity of a message transmitted over an insecure channel (where the content of the message can be changed).

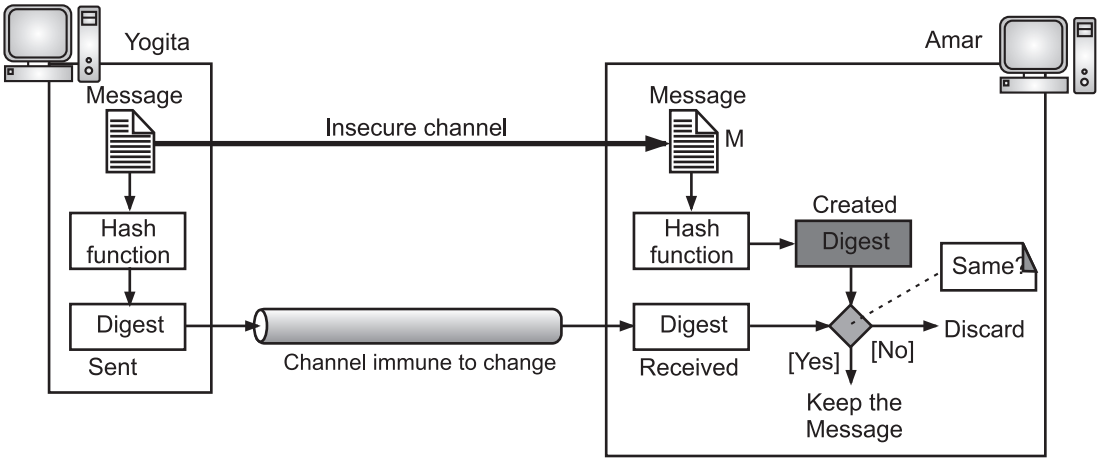


Fig. 3.45

- The two pairs (document/fingerprint) and (message/message digest) are similar, with some differences. The document and fingerprint are physically linked together.
- The message and message digest can be unlinked (or sent separately), and, most importantly, the message digest needs to be safe from change.

Hash Functions:

- A cryptographic hash function takes a message of arbitrary length and creates a message digest of fixed length.
- All cryptographic hash functions need to create a fixed-size digest out of a variable-size message. Creating such a function is best accomplished using iteration.
- Instead of using a hash function with variable-size input, a function with fixed-size input is created and is used a necessary number of times.
- The fixed-size input function is referred to as a compression function. It compresses an n-bit string to create an m-bit string where n is normally greater than m. The scheme is referred to as an iterated cryptographic hash function.
- Values returned by a hash function are called message digest or simply hash values. The Fig. 3.46 shows hash function.

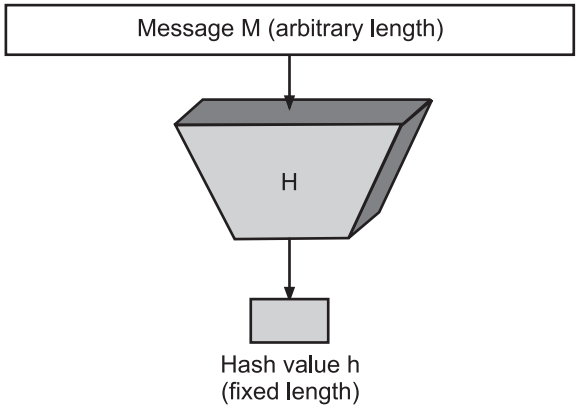


Fig. 3.46

- Several hash algorithms were designed by Ron Rivest and referred to as MD2, MD4, and MD5, where MD stands for Message Digest.
- The last version, MD5, is a strengthened version of MD4 that divides the message into blocks of 512 bits and creates a 128-bit digest. It turns out that a message digest of size 128 bits is too small to resist attack.
- MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file.
- For example, file servers often provide a pre-computed MD5 checksum for the files, so that a user can compare the checksum of the downloaded file to it.
- The Secure Hash Algorithm (SHA) is a standard that was developed by the National Institute of Standards and Technology (NIST). SHA has gone through several versions like SHA-0, SHA-1, SHA-2, and SHA-3.

3.4.3 Message Authentication

- A digest can be used to check the integrity of a message means the message has not been changed/altered/modified.
- To ensure the integrity of the message and the data origin authentication - that Yogita is the originator of the message, not somebody else - we need to include a secret held by Yogita (that Sagar does not possess) in the process; we need to create a Message Authentication Code (MAC).
- MAC provides message integrity and message authentication using a combination of a hash function and a secret key.

Message Authentication Code (MAC):

- A MAC is a cryptographic checksum on data that uses a session key to detect both accidental and intentional modifications of the data.
- MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.
- Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.
- In MAC, sender and receiver share same key where sender generates a fixed size output called cryptographic checksum or MAC and appends it to the original message.
- On receiver's side, receiver also generates the code and compares it with what he/she received thus ensuring the originality of the message.
- MAC is a short piece of information used to authenticate a message in other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed.
- The MAC value protects a message's data integrity, as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.
- The process of using MAC for authentication is shown in Fig. 3.47.
- Yogita uses a hash function to create a MAC from the concatenation of the key and the message, h(K + M). She sends the message and the MAC to Bob over the insecure channel.
- Amar separates the message from the MAC. He then makes a new MAC from the concatenation of the message and the secret key.
- Amar then compares the newly created MAC with the one received. If the two MACs match, the message is authentic and has not been modified by an adversary.

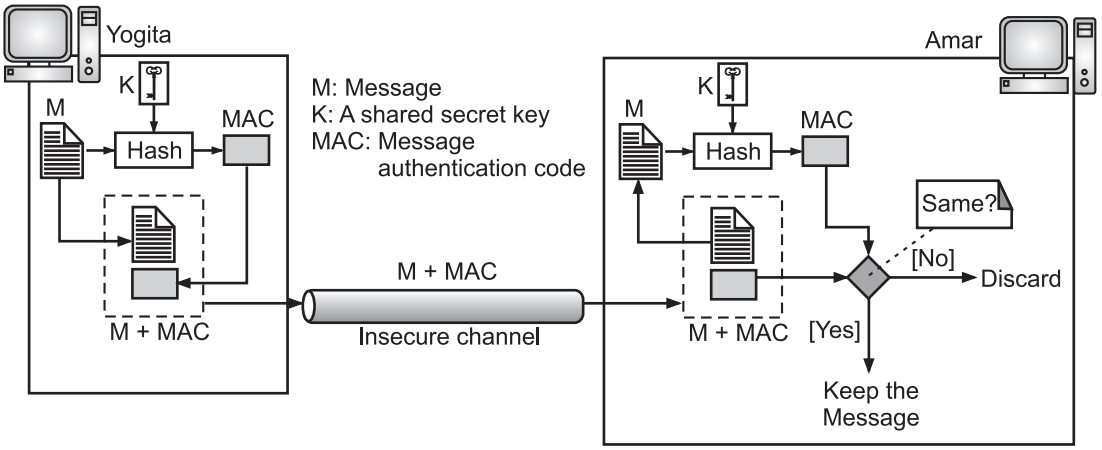


Fig. 3.47: Concept of MAC

Hashed Message Authentication Code (HMAC):

- NIST has issued a standard for a nested MAC that is often referred to as HMAC (hashed MAC). The implementation of HMAC is much more complex than the simplified MAC.
- As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message.
- HMAC can provide message authentication using a shared secret instead of using digital signatures with asymmetric cryptography.
- HMAC is a hash function created using a Shared Secret key. Since, HMAC is created using shared secret, a hacker cannot alter the data and create new HMAC hash in-between the transmission.
- The HMAC can be used to verify the integrity and authenticity of data transmissions.

3.4.4 Digital Signature

- The digital signature is a technique which is used to validate the authentication and integrity of the message.
- Digital signatures are used to identify the originator of network transactions and to ensure the integrity of the signed data against tampering or corruption.
- Digital signatures allow us to verify the author, date and time of signatures, authenticate the message contents.
- A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.
- A digital signature is an electronic version of a paper signature. Once, a document or transaction is digitally signed it means that it has legal stand.
- A digital signature uses a pair of private-public keys. Fig. 3.48 shows the digital signature process.
- The sender uses a signing algorithm to sign the message. The message and the signature are sent to the receiver.

- The receiver receives the message and the signature and applies the verifying algorithm to the combination. If the result is true, the message is accepted; otherwise, it is rejected.
- A conventional signature is like a private "key" belonging to the signer of the document. The signer uses it to sign documents; no one else has this signature.
- The copy of the signature on file is like a public key; anyone can use it to verify a document, to compare it to the original signature.
- In a digital signature, the signer uses her private key, applied to a signing algorithm, to sign the document. The verifier, on the other hand, uses the public key of the signer, applied to the verifying algorithm, to verify the document.

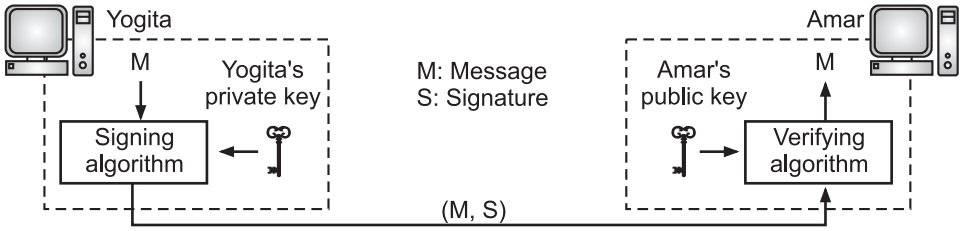


Fig. 3.48: Process of Digital Signature

- A digital signature needs a public-key system. The signer signs with her private key; the verifier verifies with the signer's public key.
- A cryptosystem uses the private and public keys of the receiver while a digital signature uses the private and public keys of the sender.
- The sender can sign the message digest and the receiver can verify the message digest. The effect is the same. Fig. 3.49 shows signing a digest in a digital signature system.
- A digest is made out of the message at Yogita's site. The digest then goes through the signing process using Yogita's private key. Yogita then sends the message and the signature to Amar.
- At Amar's site, using the same public hash function, a digest is first created out of the received message. The verifying process is applied. If authentic, the message is accepted; otherwise, it is rejected.

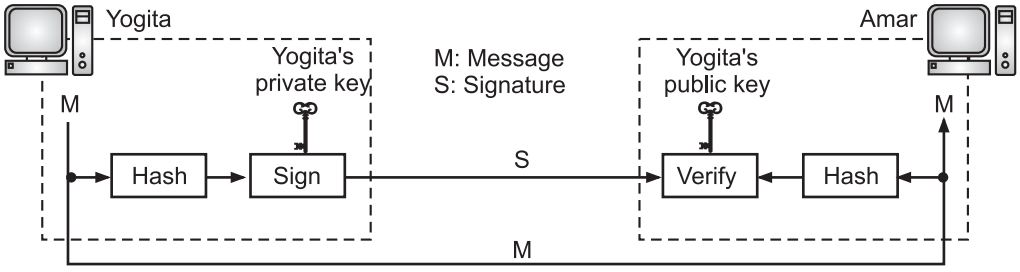


Fig. 3.49

Services of Digital Signature (DS):

- Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.
- A digital signature can directly provide services like message authentication, message integrity, and nonrepudiation, for message confidentiality we still need encryption/decryption.
  1. **Message Authentication:** A secure digital signature scheme, like a secure conventional signature (one that cannot be easily copied) can provide message authentication (also referred to as data-origin authentication). Amar can verify that the message is sent by Yogita because Yogita's public key is used in verification. Yogita's public key cannot verify the signature signed by Sagar's private key.
  2. **Message Integrity:** The integrity of the message is preserved even if we sign the whole message because we cannot get the same signature if the message is changed. The digital signature schemes today use a hash function in the signing and verifying algorithms that preserves the integrity of the message.
  3. **Nonrepudiation:** In this service DS uses trusted third party can prevent Yogita from denying that she sent the message.
  4. **Confidentiality:** A digital signature does not provide confidential communication. If confidentiality is required, the message and the signature must be encrypted using either a secret-key or public-key cryptosystem.

Working of Digital Signature (DS):

- It consist of following two processes:
  1. Digital signature creation, (performed by sender).
  2. Digital signature verification, (performed by receiver).
- Digital certificate is a data with digital signature from one trusted Certification Authority, (CA). This data contain:
  1. Who owns the certificate?
  2. Who signs this certificate?
  3. The expiry data.
  4. User name and e-mail address.
- CA (Certification Authority) is trusted agent who certifies public keys for general use. User has to decide which CAs can be trusted.
  1. **Creation of Digital Signature:** Signature is created by sender. Message Digest (MD) is extracted from message using hash function. MD is encrypted using private key of sender and we get the digital signature.
  2. **Digital Signature Verification:** It is the process of checking the digital signature by reference to the original message and a given public key. Hence, determining whether the digital signature was created for the same message using private key that corresponds to the referenced public key.

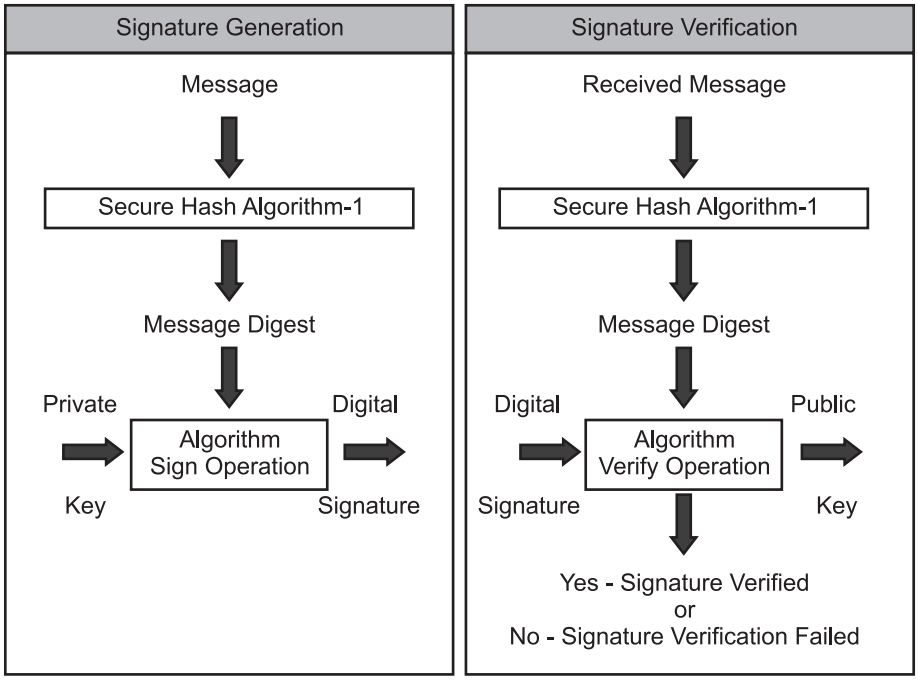


Fig. 3.50

RSA Digital Signature Scheme:

- The RSA idea can also be used for signing and verifying a message. In this case, it is called the RSA digital signature scheme.
- In the RSA scheme in which the signing and verifying is done on the digest of the message instead of the message itself.

Digital Signature Standards (DSS):

- DSS was developed for performing digital signature. DSS uses digital signature algorithm. DSS make use of SHA-1 algorithm for Calculating message digest. Hash function is used to generate MD.
- MD is given input to DSA to generate digital signature. Digital signature sent to the verifier along with the massage.
- Verifier then verifies signature by using sender's public key. Same hash function is used in the verification process.

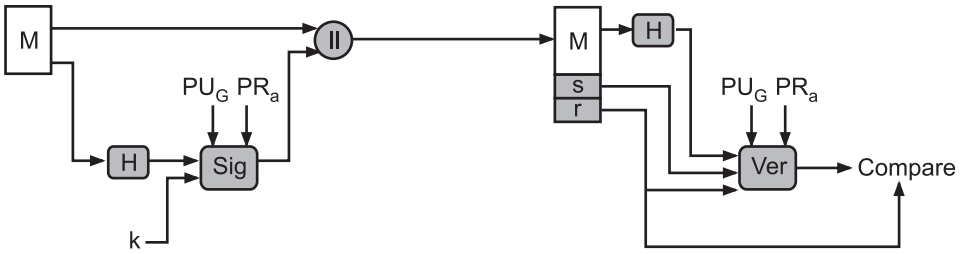


Fig. 3.51: DSS Approach

Where,

M	:	Message.	s	:	Signature.
H	:	Hash function.	r	:	$(g^k \bmod p) \bmod q$ (key pair).
Sig	:	Signature.	PU_a	:	Public key of sender.
PR_a	:	Private key of sender.	Ver	:	Verification function.
PU_G	:	Set of global public key.	Compare	:	Compare function.

- DSS is a standard and DSA is actual algorithm. DSA provide capability to generate and verify signature.
- Signature generation makes use of private key to generate digital signature. Signature verification makes use of public key which corresponds to, but is not the same as the private key.
- Each user possesses a private and public key pair. Anyone can verify the signature of user by employing that user's public key.

Advantages of DS:

1. **Speed:** In business no longer have to wait for paper document to be sent by couriers using DS contracts are easily written completed and signed by all concerned parties in less time.
2. **Cost:** Postal or courier service for paper document is much more expensive as compared using DS.
3. **Security:** Use of DS and electronic document reduces risk of document being intercepted read, destroyed.
4. **Authenticity:** An electronic document signed with DS can stand up in court just as well as any other signed paper document
5. **Non-Republication:** DS identifies us as the signatory and later that cannot be denied.
6. **Tracking:** Digitally signed document can be easily tracked and located in short amount of time.

Disadvantages of DS:

1. The private key must be kept in secure manner.
2. The process of generation and verification of digital signature requires considerable amount of time.
3. Although digital signature provides the authenticity, it does not ensure secrecy of the data.
4. For using the digital signature the user has to obtain private & public key, the receiver has to obtain the digital signature certificate also.

3.4.5 Entity Authentication

- Entity authentication is a technique designed to let one party prove the identity of another party. An entity can be a process, a client, or a server.
- The entity whose identity needs to be proved is called the claimant; the party that tries to prove the identity of the claimant is called the verifier.
- Entity authentication is the process by which one entity (the verifier) is assured of the identity of a second entity (the claimant).

Entity Authentication versus Message Authentication:

- Message authentication might not happen in real time; entity authentication does.
- Message authentication simply authenticates one message; the process needs to be repeated for each new message. Entity authentication authenticates the claimant for the entire duration of a session.
- Message authentication (or data origin authentication) is the assurance that a given entity was the original source of the received data.
- Entity authentication (or user authentication) is the assurance that a given entity is involved and currently active in a session.

Verification Categories:

- In entity authentication, the claimant must identify herself to the verifier. This can be done with one of the following three kinds of witnesses:
  1. **Something known** is a secret known only by the claimant that can be checked by the verifier. Examples are a password, a PIN, a secret key, and a private key.
  2. **Something possessed** is something that can prove the claimant's identity. Examples are a passport, a driver's license, an identification card, a credit card, and a smart card.
  3. **Something inherent** is an inherent characteristic of the claimant. Examples are conventional signatures, fingerprints, voice, facial characteristics, retinal pattern, and handwriting.

Passwords:

- Passwords are the most common method of authentication. Password consists of a string of characters to gain access to resources.
- The simplest and oldest method of entity authentication is the use of a password, which is something that the claimant knows.
- A password is used when a user needs to access a system for using the system's resources (login). Each user has a user identification that is public, and a password that is private.

- Passwords, however, are very prone to attack. A password can be stolen, intercepted, guessed, and so on.

Challenge-Response:

- In password authentication, the claimant proves her identity by demonstrating that he/she knows a secret, the password. However, because the claimant sends this secret, it is susceptible to interception by the adversary.
- In challenge-response authentication, the claimant proves that she knows a secret without sending it.
- In other words, the claimant does not send the secret to the verifier; the verifier either has it or finds it.
- The challenge is a time-varying value such as a random number or a timestamp that is sent by the verifier.
- The claimant applies a function to the challenge and sends the result, called a response, to the verifier. The response shows that the claimant knows the secret.

Using a Symmetric-Key Cipher:

- Number of approaches to challenge-response authentication use symmetric-key encryption.
- The secret here is the shared secret key, known by both the claimant and the verifier. The function is the encrypting algorithm applied on the challenge.
- Although there are several approaches to this method, we just show the simplest one to give an idea.
- Fig. 3.58 shows this first approach of challenge-response. The first message is not part of challenge-response, it only informs the verifier that the claimant wants to be challenged.
- The second message is the challenge. R_B is the nonce (abbreviation for number once) randomly chosen by the verifier (Amar) to challenge the claimant.
- The claimant encrypts the nonce using the shared secret key known only to the claimant and the verifier and sends the result to the verifier.
- The verifier decrypts the message. If the nonce obtained from decryption is the same as the one sent by the verifier, Yogita is authenticated.
- Note that in this process, the claimant and the verifier need to keep the symmetric key used in the process secret.
- The verifier must also keep the value of the nonce for claimant identification until the response is returned.

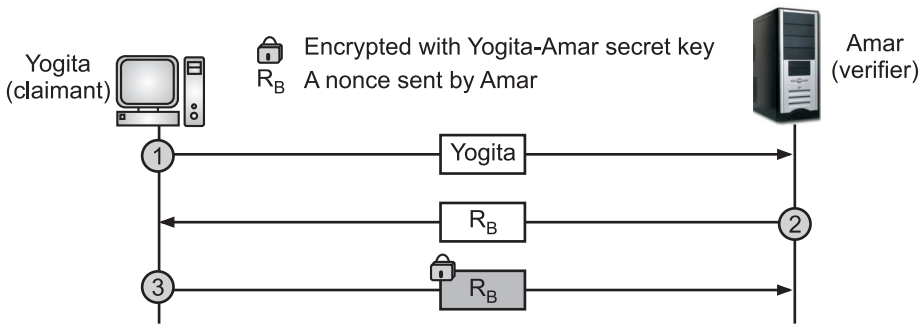


Fig. 3.52: Unidirectional, Symmetric-Key Authentication in Challenge-Response

Using an Asymmetric-Key Cipher:

- We can use an asymmetric-key cipher for entity authentication. Fig. 3.53 shows asymmetric-key authentication approach of challenge-response.
- In this approach, the secret must be the private key of the claimant. The claimant must show that she owns the private key related to the public key that is available to everyone.
- This means that the verifier must encrypt the challenge using the public key of the claimant; the claimant then decrypts the message using her private key.
- The response to the challenge is the decrypted challenge. If the R_B received in the third message is the same sent in the second message, Alice is authenticated.

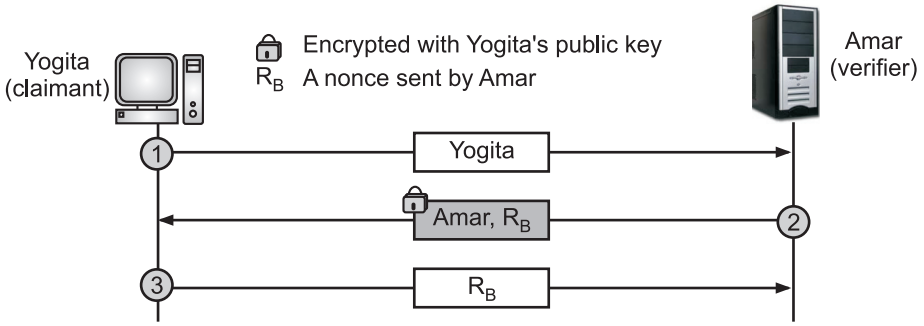


Fig. 3.53: Unidirectional, Asymmetric-Key Authentication in Challenge-Response

Using Digital Signature:

- Entity authentication can also be achieved using a digital signature. When a digital signature is used for entity authentication, the claimant uses her private key for signing.
- In Fig. 3.54, Amar uses a plaintext challenge and Yogita signs the response. If the R_B received in the third message is the same sent in the second message, Yogita is authenticated.

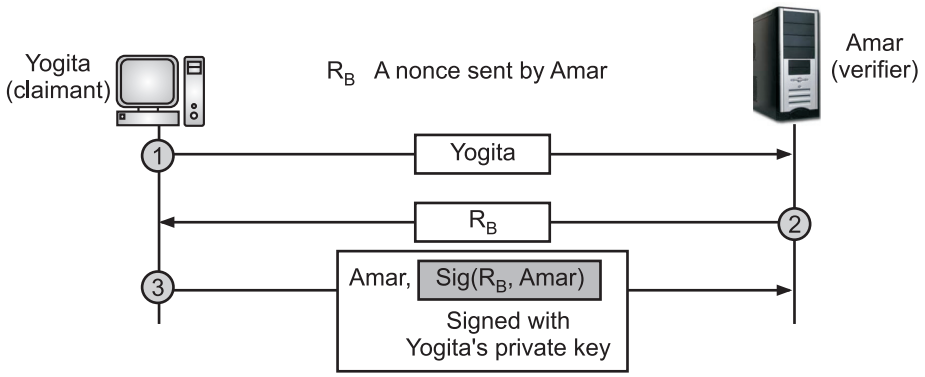


Fig. 3.54: Digital Signature, Unidirectional Authentication in Challenge-Response

PRACTICE QUESTIONS

Q.I Multiple Choice Questions:

1. An asymmetric-key (or public-key) cipher uses,
   (a) 1 key (b) 2 key
   (c) 3 key (d) 4 key
2. A straight permutation cipher or a straight P-box has the same number of inputs as,
   (a) cipher (b) frames
   (c) outputs (d) bits
3. We use Cryptography term to transforming messages to make them,
   (a) secure and immune to change
   (b) secure and immune to idle
   (c) secure and immune to attacks
   (d) secure and immune to defend
4. Which is the art and science of making a cryptosystem that is capable of providing information security?
   (a) Cryptography (b) Cryptanalysis
   (c) Cryptology (d) None of the mentioned
5. The shift cipher is sometimes referred to as the,
   (a) Caesar cipher (b) shift cipher
   (c) cipher (d) cipher text
6. The substitutional ciphers are,
   (a) monoalphabatic (b) semi alphabetic
   (c) polyalphabetic (d) bialphabetic

7. The heart of Data Encryption Standard (DES), is the
   (a) cipher (b) rounds
   (c) encryption (d) DES function
8. DES stands for,
   (a) Data Encryption Standard (b) Data Encryption Subscription
   (c) Data Encryption Solutions (d) Data Encryption Slots
9. The cryptography algorithms (ciphers) are divided into,
   (a) Two groups (b) Four groups
   (c) One single group (d) zero single group
10. Which security service that deals with identifying any alteration to the data?
   (a) Confidentiality (b) Authentication
   (c) integrity (d) Non-repudiation
11. Which of the following slows the cryptographic algorithm?
   (i) Increase in Number of rounds
   (ii) Decrease in Block size
   (iii) Decrease in Key Size
   (iv) Increase in Sub key Generation
   (a) (i) and (iii) (b) (ii) and (iii)
   (c) (iii) and (iv) (d) (ii) and (iv)
12. DES follows,
   (a) Hash Algorithm (b) Caesars Cipher
   (c) Feistel Cipher Structure (d) SP Networks
13. In Cryptography, the input bits are rotated to right or left in,
   (a) rotation cipher (b) xor cipher
   (c) cipher (d) cipher text Answer
14. An encryption algorithm transforms the plaintext into,
   (a) cipher text (b) simple text
   (c) plain text (d) empty text Answer
15. Examples of symmetric key encryption includes,
   (a) DES (b) IDEA
   (c) BLOWFISH (d) All of the mentioned
16. The original message, before being transformed, is
   (a) cipher text (b) plaintext
   (c) decryption (d) none

17. In asymmetric-key cryptography, although Rivest, Shamir, and Adelman (RSA) can be us to encrypt and decrypt actual messages, it is very slow if the message is,
    (a) short (b) long
    (c) flat (d) thin
18. In symmetric-key cryptography, the key used by the sender and the receiver is,
    (a) shared (b) different
    (c) Two keys are used (d) same keys are used
19. In Rotation Cipher, keyless rotation the number of rotations is,
    (a) jammed (b) idle
    (c) rotating (d) fixed
20. In symmetric-key cryptography both party used,
    (a) same keys (b) multi keys
    (c) different keys (d) Two keys
21. The process of converting plaintext to ciphertext using a cipher and a key is called as,
    (a) encryption (b) shared
    (c) private (d) public
22. Which is a string of bits used by a cryptographic algorithm to transform plaintext into ciphertext?
    (a) cipher (b) encryption algorithm
    (c) Decryption algorithm (d) key
23. Data Encryption Standard (DES) is an example of,
    (a) complex block cipher (b) cryptography
    (c) Electronic Cipher Book (d) Electronic Code Book
24. The relationship between a character in the plaintext to a character is,
    (a) many-to-one relationship (b) one-to-many relationship
    (c) many-to-many relationship (d) one-to-one relationship
25. Cryptography, a word with Greek origins, means
    (a) corrupting data (b) secret writing
    (c) open writing (d) closed writing
26. A transposition cipher reorders (permutes) symbols in a,
    (a) block of packets (b) block of slots
    (c) block of signals (d) block of symbols
27. The Cipher Feedback (CFB) mode was created for those situations in which we need to send or receive R bits of,
    (a) frames (b) pixels
    (c) data (d) encryption

28. In Cryptography, when text is treated at the bit level, each character is replaced by,
    (a) 4 bits (b) 6 bits
    (c) 8 bits (d) 10 bits
29. Which cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process?
    (a) Monoalphabetic (b) Polyalphabetic
    (c) Substitution (d) Transposition
30. ECB stands for,
    (a) Electronic Control Book (b) Electronic Code Book
    (c) Electronic Cipher Book (d) Electronic Cryptography Book
31. The cipher which uses the exclusive-or operation as defined in computer science is called as,
    (a) caesar cipher (b) xor cipher
    (c) cipher (d) cipher text
32. The cryptography can provide,
    (a) entity authentication (b) nonrepudiation of messages
    (c) confidentiality (d) authentication
33. The shift ciphers sometimes referred to as the,
    (a) Caesar cipher (b) Julia cipher
    (c) plain cipher (d) XOR cipher angle B
34. RSA stands for,
    (a) Rivest, Shamir, and Adleman (b) Roger, Shamir, and Adrian
    (c) Robert, Shamir, and Anthoney (d) Rivest, Shaw, and Adleman
35. The Data Encryption Standard (DES) was designed by,
    (a) Microsoft (b) Apple
    (c) IBM (d) HP
36. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.
    (a) True (b) False
37. In the DES algorithm, the round key is _____ bit and the Round Input is _____ bits.
    (a) 48, 32 (b) 64, 32
    (c) 56, 24 (d) 32, 32
38. The number of unique substitution boxes in DES after the 48 bit XOR operation are,
    (a) 8 (b) 4
    (c) 6 (d) 12

39. In stream ciphers the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of ciphertext.
    (a) True (b) False
40. View following answer for public key encryption method is a system,
    (a) Which uses a set of public keys one for each participant in e-Commerce
    (b) in which each person who wants to communicate has two keys; a private key known to him only and a public key, which is publicized to enable others to send message to him
    (c) Which uses the RSA coding system.
    (d) Which is a standard for use in e-Commerce.
41. In public key encryption if A wants to send an encrypted message,
    (a) A encrypts message using his private key
    (b) A encrypts message using B's private key
    (c) A encrypts message using B's public key
    (d) A encrypts message using his public key
42. Ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic
    (a) Substitution (b) Transposition
    (c) Either (a) or (b) (d) neither (a) nor (b)
43. The _____ cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26.
    (a) transposition (b) additive
    (c) shift (d) none of the above
44. A(n) _____ is a keyless transposition cipher with N inputs and M outputs that uses a table to define the relationship between the input stream and the output stream,
    (a) S-box (b) P-box
    (c) T-box (d) none of the above
45. _____ is a round cipher based on the Rijndael algorithm that uses a 128-bit block of data
    (a) AEE (b) AED
    (c) AER (d) AES
46. AES has _____ diff epsilon configurations
    (a) two (b) three
    (c) four (d) five
47. ECB and CBC are _____ ciphers
    (a) block (b) stream
    (c) field (d) none of the above

48. One commonly used public-key cryptography method is the _____ algorithm
    (a) RSS (b) RAS
    (c) RSA (d) RAA
49. The method provides a one-time session key for two parties,
    (a) Diffie-Hellman (b) RSA
    (c) DES (d) AES
50. A combination of an encryption algorithm and a decryption algorithm is called a _____.
    (a) cipher (b) secret
    (c) key (d) none of the above
51. Which provides message integrity and message authentication using a combination of a hash function and a secret key?
    (a) HMAC (b) MAC
    (c) Both (a) and (b) (d) All of these
52. Values returned by a hash function are called as,
    (a) (b) hash values
    (c) Both (a) and (b) (d) All of the mentioned
53. Which is a technique that binds a person/entity to the digital data?
    (a) hash function (b) digital signature
    (c) message digest (d) All of the mentioned

Answers

1. (b)	2. (b)	3. (c)	4. (a)	5. (a)	6. (d)	7. (d)	8. (a)	9. (a)	10. (c)
11. (b)	12. (c)	13. (a)	14. (a)	15. (d)	16. (b)	17. (b)	18. (a)	19. (d)	20. (a)
21. (a)	22. (d)	23. (a)	24. (b)	25. (b)	26. (d)	27. (c)	28. (c)	29. (a)	30. (b)
31. (b)	32. (d)	33. (a)	34. (a)	35. (c)	36. (b)	37. (a)	38. (a)	39. (a)	40. (b)
41. (c)	42. (a)	43. (c)	44. (b)	45. (d)	46. (b)	47. (a)	48. (c)	49. (d)	50. (a)
51. (b)	52. (c)	53. (b)							

Q.II Fill in the Blanks:

1. Cryptography involves the process of encryption and decryption of messages using _____.
2. The sender requires an encryption _____ and a _____ to transform the plaintext (original message) into a ciphertext (encrypted message).
3. The art and science of breaking the cipher text is known as _____.
4. Cryptography is simply the mathematical _____ of data.
5. In a _____ cipher, each letter or group of letters are replaced by another letter or group of letters to disguise it.

6. A _____ parallels the traditional transposition cipher for characters, but it transposes bits.
7. DES uses _____ rounds and each round of DES is an invertible transformation.
8. The text converted to readable format in a non-readable format using the encryption algorithm is called a _____.
9. The ECB mode is _____, that is, if plaintext block P1, P2, ..., Pm are encrypted twice under the same key, the output ciphertext blocks will be the same.
10. _____ is a security service that keeps the information from an unauthorized person and sometimes referred to as privacy or secrecy.
11. The encryption process where different keys are used for encrypting and decrypting the information is known as _____ Key Encryption.
12. _____ use a set of procedures known as cryptographic algorithms, or ciphers, to encrypt and decrypt messages to secure communications among computer systems, devices such as smartphones, and applications.
13. _____ provides the identification of the originator.
14. _____ authentication identifies the originator of the message without any regard router or system that has sent the message.
15. _____ cipher is a mono-alphabetic cipher wherein each letter of the plaintext is substituted by another letter to form the ciphertext.
16. Public-key or asymmetric-key encryption algorithms use a _____ of keys, a public key associated with the creator/sender for encrypting messages and a private key that only the originator knows for decrypting that information.
17. _____ Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process.
18. In _____ cipher the plain binary text is processed in blocks (groups) of bits at a time; i.e. a block of plaintext bits is selected, a series of operations is performed on this block to generate a block of ciphertext bits.
19. The block size of DES is _____.
20. _____ is the art and science of achieving security by encoding messages to make them non-readable.
21. The _____ operation, in which the output is 0 if the two inputs are the same, and the output is 1 if the two inputs are different.
22. The key which is not known to everyone, which is kept as a secret, is known as a _____ key.
23. The _____ signature is a technique which is used to validate the authentication and integrity of the message.
24. Symmetric encryption also called _____ Key Cryptography.

25. An _____ can be thought of as a miniature substitution cipher, but it substitutes bits.
26. Monoalphabetic cipher is a _____ cipher.
27. The Data Encryption Standard (DES) is a _____ block cipher.
28. In _____ mode, both the sender and receiver need to access to a reliable counter, which computes a new shared value each time a ciphertext block is exchanged.
29. The DES _____ applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.
30. _____ algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.
31. The hash function creates a compressed image of the message, called a _____.
32. _____ can provide message authentication using a shared secret instead of using digital signatures with asymmetric cryptography.

Answers

1. secret keys	2. algorithm, key	3. cryptanalysis	4. scrambling
5. substitution	6. P-box	7. 16	8. ciphertext
9. deterministic	10. Confidentiality	11. Asymmetric	12. Cryptosystems
13. Authentication	14. Message	15. Caesar	16. pair
17. Polyalphabetic	18. block	19. 64-bit	20. Cryptography
21. XOR	22. private	23. digital	24. Secret
25. S-box	26. substitution	27. symmetric-key	28. CTR
29. MAC	30. function	31. digest	32. HMAC

Q.III State True or False:

1. Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender.
2. Sharing the secret key in the beginning is not a problem in symmetric key encryption
3. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
4. CBC mode of operation provides message dependence for generating ciphertext and makes the system deterministic.
5. Message authentication does happen in real time; entity authentication might not.
6. Entity authentication can also be achieved using a digital signature.

7. Secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier.
8. The process of generation and verification of digital signature is very fast.
9. A MAC is a cryptographic checksum on data that uses a session key to detect both accidental and intentional modifications of the data.
10. The traditional symmetric key ciphers are bit oriented ciphers.
11. Entity authentication is assurance that data has been received from a specific entity, say a particular website.
12. Plaintext is the data to be protected during transmission.
13. The encryption process where same keys are used for encrypting and decrypting the information is known as asymmetric Key Encryption.
14. In cryptography a 'key' is a piece of information used in combination with an algorithm (a 'cipher') to transform plaintext into ciphertext (encryption) and vice versa (decryption).
15. A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size.
16. The algorithm which is used to convert cipher text to plain text is known as a decryption algorithm.
17. Key is the secret information in a cryptographic operation.
18. The process of converting ciphertext back into plaintext using a cipher and a key is called as encryption.
19. The key which is known to everyone is known as the public key.
20. A digital signature uses a pair of private-public keys.
21. Passwords are the most common method of authentication. Password consists of a string of characters to gain access to resources.
22. Symmetric key cryptography (or symmetric encryption) is a type of encryption technique in which the same key is used both to encrypt and decrypt messages.
23. Traditional ciphers are called symmetric key ciphers or secret key ciphers because the same key is used for encryption and decryption.
24. A cryptographic hash function takes a message of arbitrary length and creates a message digest of fixed length.
25. Monoalphabetic cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process.
26. A permutation box (P-box) parallels the traditional transposition cipher for characters, but it transposes bits.
27. DES is a symmetric key algorithm, which means that the same key is used for encrypting and decrypting data.

28. A block cipher processes the data blocks of variable size.
29. Message digest ensures the integrity of the document.
30. MAC algorithm is a symmetric key cryptographic technique.

Answers

1. (T)	2. (F)	3. (T)	4. (F)	5. (F)	6. (T)	7. (T)	8. (F)	9. (T)	10. (F)
11. (T)	12. (T)	13. (F)	14. (T)	15. (T)	16. (T)	17. (T)	18. (F)	19. (T)	20. (T)
21. (T)	22. (T)	23. (T)	24. (T)	25. (F)	26. (T)	27. (T)	28. (F)	29. (T)	30. (T)

Q.IV Answer the following Questions:

(A) Short Answer Questions:

1. What is cryptography?
2. Give the purpose of cryptography.
3. What is plaintext?
4. Define ciphertext.
5. What is encryption and decryption?
6. What is cryptographic key?
7. What is HMAC?
8. Define digital signature.
9. Give purpose of MAC?
10. What is message and message digest?
11. Define entity authentication.
12. List security services.
13. What is DES?
14. What is RSA?
15. Define block and stream ciphers.
16. What is s-box and p-box?
17. List traditional ciphers.
18. Give the purpose of ECB and OFB mode of block cipher.

(B) Long Answer Questions:

1. Define cryptography. Explain in detail.
2. With the help of diagram describe encryption and description process.
3. With the help of diagram describe encryption model.
4. What is symmetric key cryptography? How it works? State its advantages and disadvantages.
5. What is asymmetric key cryptography? How it works? State its advantages and disadvantages.
6. What is substitution cipher? Explain with example.

7. What is transposition cipher? Explain with example.
8. With the help of diagram describe various modes of block cipher?
10. Write short note on: Simple modern ciphers.
11. Describe block and stream ciphers diagrammatically. Also compare them.
12. Explain message confidentiality with Symmetric key cryptography and with asymmetric key cryptography.
13. Describe RSA with example.
14. Explain message integrity with document and fingerprint.
15. With the help of diagram describe operation of DES.
16. What is message authentication? Explain with MAC and HMAC.
17. Compare symmetric key cryptography and asymmetric key cryptography.
18. What is? State its advantages and disadvantages.
19. How the digital signature works? Explain in detail with diagram.
20. By using transposition cipher convert the following:

    Plaintext: "The reverse process of transforming ciphertext message back to plaintext message is called decryption".

    Key: ZQARXPM
21. By using substitution cipher transform the message “difference between random access protocol with controlled access protocol”. Key is ‘4’.
22. By using transposition cipher convert the following :

    Plain text : “ Please transfer one million dollar to my Swiss bank account six two two”.

    Key : MEGABUCK.
23. Encrypt the following plain text transposition cipher :

    Key : MAGNETIC

    Plain text : transmit this message.

UNIVERSITY QUESTIONS AND ANSWERS

April 2016

1. What is cipher? **[1 M]**

Ans. Refer to Section 3.1, Point (2).

2. What is encryption? **[1 M]**

Ans. Refer to Section 3.1.2, Point (6).

3. Using substitution cipher transform the message "HAPPY BIRTHDAY TO YOU" key I s 'S'. **[1 M]**

Ans. Refer to Section 3.2.1, Point (1).

4. What is steganography? **[1 M]**

Ans. Refer to Section 3.1.

5. Using transposition cipher convert the following plaintext
"The reverse process of transforming ciphertext message back to plaintext message is called decryption" key ZQARXMP. **[5 M]**

Ans. Refer to Section 3.2.1, Point (2).

April 2017

1. What is steganography? **[1 M]**

Ans. Refer to Section 3.1.

2. What is cipher? **[1 M]**

Ans. Refer to Section 3.1, Point (2).

3. Encrypt the following plain text transposition cipher:
Key: MAGNETIC
Plain text: transmit this message. **[5 M]**

Ans. Refer to Section 3.2.1, Point (2).

October 2017

1. By using substitution cipher transform the message "HONESTY IS THE BEST POLICY", KEY IS -5. **[1 M]**

Ans. Refer to Section 3.2.1, Point (1).

2. By using transposition cipher convert the following:
Plain text: "The application layer is the topmost layer in layered network model"
Key: MAGABUCK **[5 M]**

Ans. Refer to Section 3.2.1, Point (2).

3. Explain two fundamental cryptographic principles. **[4 M]**

Ans. Refer to Section 3.1.

April 2018

1. What is transposition cipher? **[1 M]**

Ans. Refer to Section 3.2.1, Point (2).

2. What is Cryptography? Explain two cryptographic principles. **[5 M]**

Ans. Refer to Section 3.1.

October 2018

1. By using transposition cipher convert the following plain text to cipher text. Using key ZQPBEXC.
"Digital signature is a mathematical method for implementing the authentication of a digital message or document". **[5 M]**

Ans. Refer to Section 3.2.1, Point (2).

April 2019

1. Define: (i) Plain Text (ii) Cipher Text (iii) Encryption (iv) Decryption. **[4 M]**

Ans. Refer to Section 3.1.2, Points, (1), (2), (6) and (7).

❖❖❖

CHAPTER 4

Security in the Internet

Objectives...

- To understand Basic Concept of Internet
- To learn Security in Internet
- To study IPSec with its Modes
- To learn PGP and SSL/TLS
- To learn Firewall with its Types

4.0 INTRODUCTION

- Internet is a world-wide global system of interconnected computer networks. The word 'Internet' is derived from two words namely, interconnection and networks. It is also referred to as 'Net'.
- Internet is a global network links thousands of computers at universities, research institutions, government agencies, business and houses throughout the world.
- An Internet is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.
- Internet is a worldwide system of computer networks, i.e. a network of networks, which allows the participants (users) to share information.
- In today's digital landscape, many of our daily activities rely on the Internet. Various forms of communication, entertainment, and financial and work-related tasks are accomplished online.
- This means that tons of data and sensitive information are constantly being shared over the Internet.
- The Internet is mostly private and secure, but it can also be an insecure channel for exchanging information.
- With a high risk of intrusion by hackers and cybercriminals, Internet security is a top priority for individuals and businesses.
- Internet security encompasses the Internet, browser security, web site security, and network security as it applies to other applications or operating systems as a whole.
- The objective of Internet security is to establish rules and measures to use against attacks over the Internet.

- Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the Internet.
- The most common Internet security threats are given below:
  1. **Malware:** Short for "malicious software," malware comes in several forms, including computer viruses, worms, Trojans, and dishonest spyware. Computer viruses are programs that can replicate their structures or effects by infecting other files or structures on a computer. The typical purpose of a virus is to take over a computer to steal data. Spyware refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent. A Trojan horse, commonly known as a Trojan, is a general term for malware that pretends to be harmless, so that a user will be convinced to download it onto the computer.
  2. **Computer worm:** A computer worm is a software program that copies itself from one computer to the next. It does not require human interaction to create these copies and can spread rapidly and in great volume.
  3. **Spam:** Spam refers to unwanted messages in your email inbox. In some cases, spam can simply include junk mail that advertises goods or services you aren't interested in. These are usually considered harmless, but some can include links that will install malicious software on your computer if they're clicked on.
  4. **Phishing:** Phishing scams are created by cybercriminals attempting to solicit private or sensitive information. They can pose as your bank or web service and lure you into clicking links to verify details like account information or passwords. Phishing targets online users in an attempt to extract sensitive information such as passwords and financial information.[
  5. **Botnet:** A botnet is a network of private computers that have been compromised. Infected with malicious software, these computers are controlled by a single user and are often prompted to engage in nefarious activities, such as sending spam messages or denial-of-service (DoS) attacks.
  6. **Brute-force Attack:** It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.
  7. **Denial of Service (DoS) Attack:** It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server.
  8. **Man In The Middle (MITM) Attack:** It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between

them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

9. **Backdoors:** It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

- So, Internet security is one of the most important aspect to consider when working with the Internet.

4.1 IPSec

- Internet Protocol Security (IPSec) is a set of protocols that provides security for Internet Protocol using advanced cryptography.
- IP Security (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.
- IPSec helps create authenticated and confidential packets for the IP layer. IPSec provides security and authentication at the IP layer by transforming data using encryption.
- IPSec is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network.
- IPSec uses cryptographic security services to protect communications over Internet Protocol (IP) networks.
- IPSec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).
- IPSec was developed for the newest version of Internet Protocol (IPv6) and retrospectively also for IPv4. It can be divided into the following three function groups:
  1. **Transfer protocols** (Authentication Header (AH), Encapsulating Security Payload (ESP)).
  2. **Key management** (Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange (IKE)).
  3. **Database** (Security Association Database (SAD), Security Policy Database (SPD)).

4.1.1 Two Modes

- IPSec operates on two modes of functioning namely, transport mode and tunnel mode. These modes can be used in combination or used individually depending upon the type of communication desired.

Transport Mode:

- In transport mode, IPSec protects what is delivered from the transport layer to the network layer.

- In other words, transport mode protects the payload to be encapsulated in the network layer, as shown in Fig. 4.1.
- Note that transport mode of IPSec does not protect the IP header. In other words, transport mode does not protect the whole IP packet; it protects only the packet from the transport layer (the IP layer payload).
- In transport mode, the IPSec header (and trailer) is added to the information coming from the transport layer. The IP header is added later.

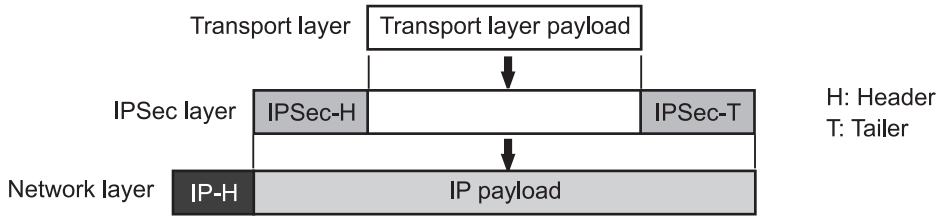


Fig. 4.1: IPSec in Transport Mode

- Transport mode of IPSec is normally used when we need host-to-host (end-to-end) protection of data.
- The sending host uses IPSec to authenticate and/or encrypt the payload delivered from the transport layer.
- The receiving host uses IPSec to check the authentication and/or decrypt the IP packet and deliver it to the transport layer.
- Fig. 4.2 shows the concept of transport mode in action.

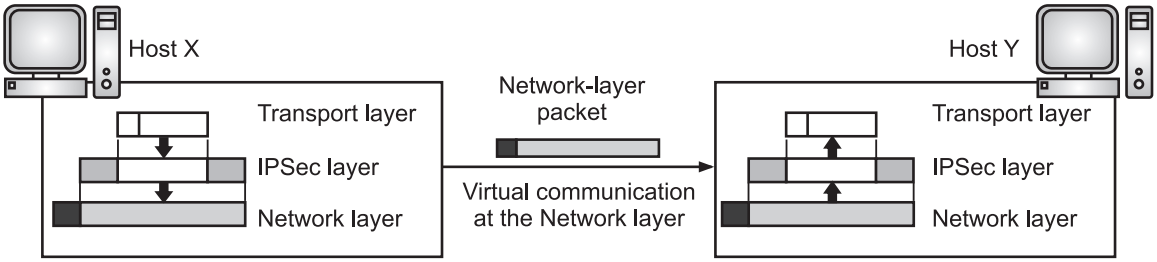


Fig. 4.2

Tunnel Mode:

- In tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header, as shown in Fig. 4.3.
- Tunnel mode is used to create virtual private networks for network-to-network communication (e.g. between routers to link sites), host-to-network communications (e.g. remote user access) and host-to-host communications (e.g. private chat).
- The new IP header, as we will see shortly, has different information than the original IP header.

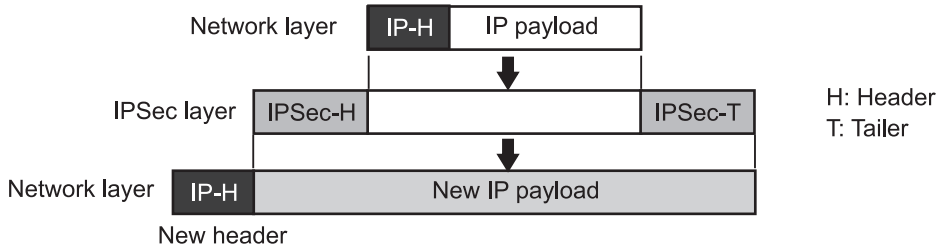


Fig. 4.3: IPSec in Tunnel Mode

- Tunnel mode is normally used between two routers, between a host and a router, or between a router and a host, as shown in Fig. 4.4.
- The entire original packet is protected from intrusion between the sender and the receiver, as if the whole packet goes through an imaginary tunnel.
- Fig. 4.4 shows the concept of tunnel mode in action.

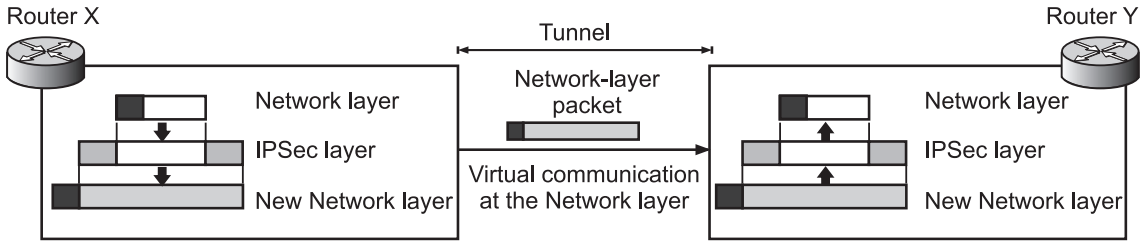


Fig. 4.4

Comparison between Transport Mode and Tunnel Mode:

- In transport mode, the IPSec layer comes between the transport layer and the network layer.
- In tunnel mode, the flow is from the network layer to the IPSec layer and then back to the network layer again.
- In transport mode, only the payload of the IP packet is usually encrypted or authenticated.
- In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header.
- Fig. 4.5 compares the transport and tunnel modes in IPSec.

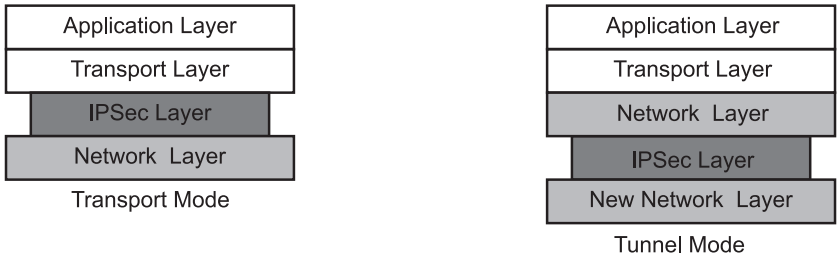


Fig. 4.5

4.1.2 Two Security Protocols

- IPSec uses the security protocols to provide desired security services. These protocols are the heart of IPSec operations and everything else is designed to support these protocols in IPSec.
- IPSec defines two protocols namely, Authentication Header (AH) Protocol and the Encapsulating Security Payload (ESP) Protocol to provide authentication and/or encryption for packets at the IP level.
- The AH and ESP protocols provide data integrity, data origin authentication, and anti-replay services. These protocols can be used alone or in combination.

Authentication Header (AH) Protocol:

- The AH protocol is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet.
- The AH protocol uses a hash function and a symmetric (secret) key to create a message digest; the digest is inserted in the authentication header.
- The AH protocol is then placed in the appropriate location, based on the mode (transport or tunnel).
- When an IP datagram carries an authentication header, the original value in the protocol field of the IP header is replaced by the value 51.
- A field inside the authentication header (the next header field) holds the original value of the protocol field (the type of payload being carried by the IP datagram).
- Fig. 4.6 shows the fields and the position of the authentication header in IPSec transport mode.

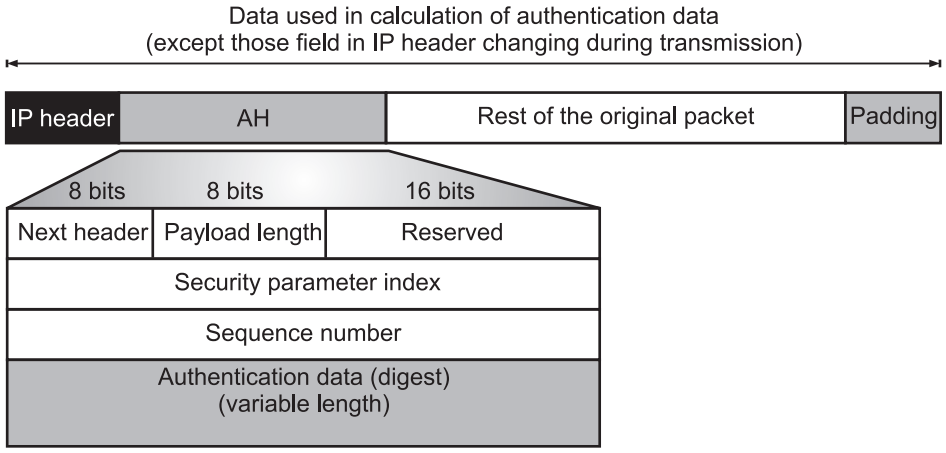


Fig. 4.6: AH Protocol

- Description of each field of AH protocol as follows:
  1. **Next Header:** The 8-bit next header field defines the type of payload carried by the IP datagram like TCP, UDP, ICMP, or OSPF.

2. **Payload Length:** The name of this 8-bit field is misleading. It does not define the length of the payload; it defines the length of the authentication header in 4-byte multiples, but it does not include the first 8 bytes.
3. **Reserved:** This is 16 bits field reserved for future use (all zeroes until then).
4. **Security Parameter Index:** The 32-bit Security Parameter Index (SPI) field plays the role of a virtual circuit identifier and is the same for all packets sent during a connection called a Security Association (SA).
5. **Sequence Number:** A 32-bit sequence number provides ordering information for a sequence of datagrams. The sequence numbers prevent a playback. Note that the sequence number is not repeated even if a packet is retransmitted. A sequence number does not wrap around after it reaches 232; a new connection must be established.
6. **Authentication Data:** Finally, the authentication data field is the result of applying a hash function to the entire IP datagram except for the fields that are changed during transit (e.g., time-to-live).

Encapsulating Security Payload (ESP) Protocol:

- The IPSec, AH protocol does not provide confidentiality, only source authentication and data integrity. IPSec later defined an alternative protocol, Encapsulating Security Payload (ESP), which provides source authentication, integrity, and confidentiality.
- In ESP the set of services provided depends on options selected at the time of Security Association (SA) establishment.
- In ESP, algorithms used for encryption and generating authenticator are determined by the attributes used to create the SA.
- ESP adds a header and trailer. Note that ESP's authentication data are added at the end of the packet, which makes its calculation easier.
- Fig. 4.7 shows the location of the ESP header and trailer. When an IP datagram carries an ESP header and trailer, the value of the protocol field in the IP header is 50.
- A field inside the ESP trailer (the next-header field) holds the original value of the protocol field (the type of payload being carried by the IP datagram, like TCP or UDP).

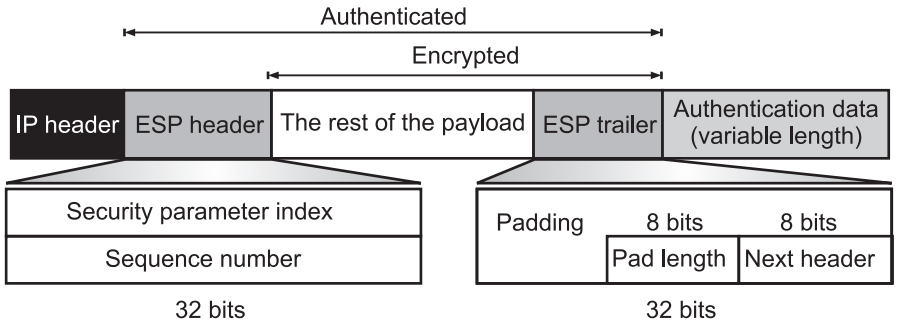


Fig. 4.7: ESP Protocol

- The fields for the header and trailer in ESP protocol are as follows:
  1. **Security Parameter Index:** The 32-bit security parameter index field is similar to the one defined for the AH protocol.
  2. **Sequence Number:** The 32-bit sequence number field is similar to the one defined for the AH protocol.
  3. **Padding:** This variable-length field (0 to 255 bytes) of 0s serves as padding.
  4. **Pad Length:** The 8-bit pad-length field defines the number of padding bytes. The value is between 0 and 255; the maximum value is rare.
  5. **Next Header:** The 8-bit next-header field is similar to that defined in the AH protocol. It serves the same purpose as the protocol field in the IP header before encapsulation.
  6. **Authentication Data:** Finally, the authentication data field is the result of applying an authentication scheme to parts of the datagram.

4.1.3 Services Provided by IPSec

- IPSec is suite of protocols to provide security services during communications between networks.
- It supports network level peer authentication, data origin authentication, data integrity, data encryption and data decryption. It is often used to create a VPN.
- The two IPSec protocols (AH and ESP) can provide several security services for packets at the network layer.
- Following are the list of services provided by AH and ESP protocols:
  1. **Access Control:** IPSec provides access control indirectly using a Security Association Database (SAD). When a packet arrives at a destination, and there is no Security Association already established for this packet, the packet is discarded.
  2. **Message Integrity:** Message integrity is preserved in both AH and ESP. A digest of data is created and sent by the sender to be checked by the receiver.
  3. **Entity Authentication:** The Security Association and the keyed-hash digest of the data sent by the sender authenticate the sender of the data in both AH and ESP.
  4. **Confidentiality:** The encryption of the message in ESP provides confidentiality. AH, however, does not provide confidentiality. If confidentiality is needed, one should use ESP instead of AH.
  5. **Replay Attack Protection:** In both protocols, the replay attack is prevented by using sequence numbers and a sliding receiver window. Each IPSec header contains a unique sequence number when the Security Association is established.

4.1.4 Security Association

- Security Association (SA) is a very important aspect of IPSec. IPSec requires a logical relationship between two hosts called as SA.

- The IPSec protocols use a Security Association (SA), where the communicating parties establish shared security attributes such as algorithms and keys.
- As such IPSec provides a range of options once it has been determined whether IPSec AH or IPSec ESP is used.
- Before exchanging data the two hosts agree on which algorithm is used to encrypt the IP packet, for example DES or IDEA, and which hash function is used to ensure the integrity of the data, such as MD5 or SHA.
- SA is the foundation of an IPsec communication. A SA is a contract between two parties; it creates a secure channel between them.
- Let us assume that Alice needs to unidirectionally communicate with Amar. If Yogita and Amar are interested only in the confidentiality aspect of security, they can create a shared secret key between themselves.
- We can say that there are two SAs between Yogita and Amar; one outbound SA and one inbound SA. Each of them stores the value of the key in a variable and the name of the encryption/ decryption algorithm in another.
- Yogita uses the algorithm and the key to encrypt a message to Amar; Amar uses the algorithm and the key when he needs to decrypt the message received from Yogita.
- Fig. 4.8 shows a simple SA in IPSec.

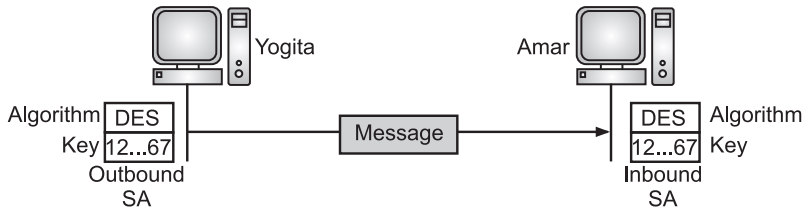


Fig. 4.8

- The SA can be more involved if the two parties need message integrity and authentication. Each association needs other data such as the algorithm for message integrity, the key, and other parameters.
- It can be much more complex if the parties need to use specific algorithms and specific parameters for different protocols like AH or ESP.

Security Association Database (SAD):

- We need a set of SAs that can be collected into a database called as Security Association Database (SAD).
- The database can be thought of as a two-dimensional table with each row defining a single SA.
- Normally, there are two SADs, one inbound and one outbound. Fig. shows the concept of outbound or inbound SADs for one entity.
- When a host needs to send a packet that must carry an IPSec header, the host needs to find the corresponding entry in the outbound SAD to find the information for applying security to the packet.

- Similarly, when a host receives a packet that carries an IPSec header, the host needs to find the corresponding entry in the inbound SAD to find the information for checking the security of the packet.

Index	SN	OF	ARW	AH/ESP	LT	Mode	MTU
< SPI, DA, P >							
< SPI, DA, P >							
< SPI, DA, P >							
< SPI, DA, P >							

Security Association Database

Note:

SPI: Security Parameter Index
SN: Sequence Number
DA: Destination Address
OF: Overflow Flag
AH/ESP: Information for either one
ARW: Anti-Replay Window
P: Protocol
LT: LifeTime
Mode: IPSec Mode Flag
MTU: Path MTU

Fig. 4.9

- This searching must be specific in the sense that the receiving host needs to be sure that correct information is used for processing the packet.
- Each entry in an inbound SAD is selected using a triple index (security parameter index (a 32-bit number that defines the SA at the destination), destination address, and protocol (AH or ESP)).

Security Policy (SP):

- The Security Policy (SP) is important aspect of IPSec. SP defines the type of security applied to a packet when it is to be sent or when it has arrived.
- Before using the SAD, a host must determine the predefined policy for the packet.

Security Policy Database (SPD):

- Each host that is using the IPSec protocol needs to keep a SPD. Again, there is a need for an inbound SPD and an outbound SPD.
- Each entry in the SPD can be accessed using a sextuple index: source address, destination address, name, protocol, source port, and destination port, as shown in Fig. 4.10.
- Source and destination addresses can be unicast, multicast, or wildcard addresses. The name usually defines a DNS entity. The protocol is either AH or ESP.
- The source and destination ports are the port addresses for the process running at the source and destination hosts.

Index	Policy
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	

Note:

SA: Source Address **SPort:** Source Port

DA: Destination Address **DPort:** Destination Port

P: Protocol

Fig. 4.10: SPD

Inbound SPD:

- When a packet arrives, the inbound SPD is consulted. Each entry in the inbound SPD is also accessed using the same sextuple index.
- Fig. 4.11 shows the processing of a packet by a receiver.
- The input to the inbound SPD is the sextuple index; the output is one of the three cases namely, discard (drop the packet), bypass (bypass the security and deliver the packet to the transport layer), and apply (apply the policy using the SAD).

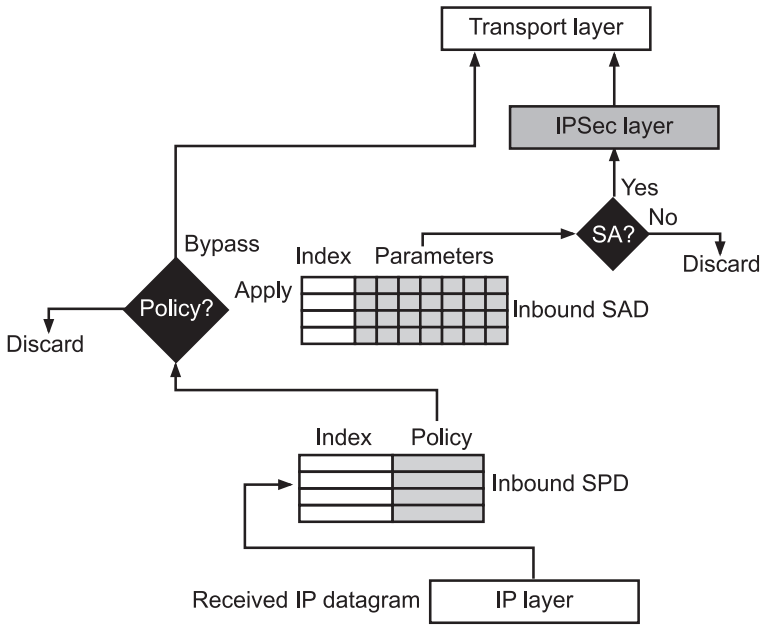


Fig. 4.11: Inbound Processing in SPD

Outbound SPD:

- When a packet is to be sent out, the outbound SPD is consulted. Fig. shows the processing of a packet by a sender.

- The input to the outbound SPD is the sextuple index; the output is one of the three cases namely, drop (packet cannot be sent), bypass (bypassing security header), and apply (apply the security according to the SAD; if no SAD, create one).

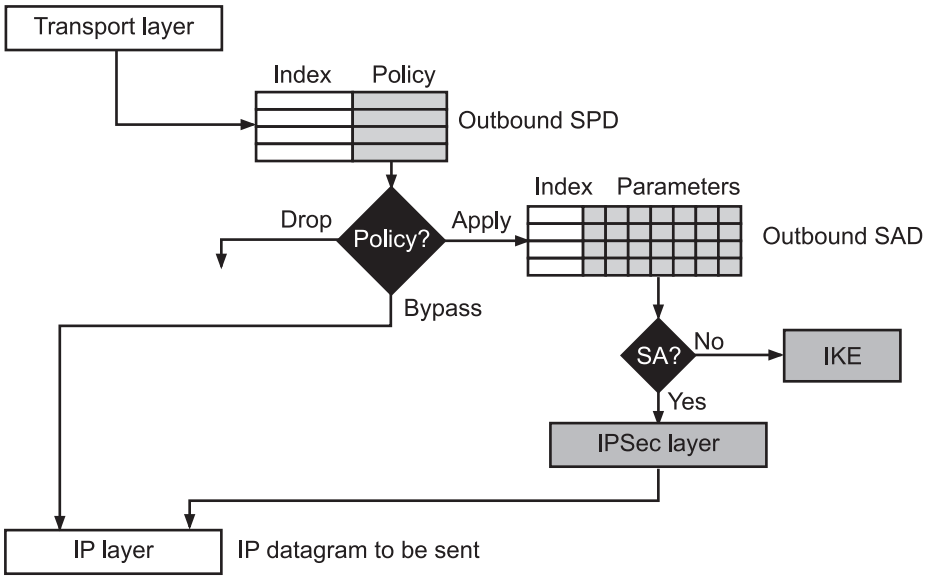


Fig. 4.12: Outbound Processing in SPD

4.1.5 Internet Key Exchange

- The Internet Key Exchange (IKE) is a protocol used for the key management procedures in IPSec. The IKE is the protocol used to set up a Security Association (SA) in the IPSec protocol.
- The IKE is a protocol designed to create both inbound and outbound Security Associations (SAs).
- When a peer needs to send an IP packet, it consults the Security Policy Database (SPD) to see if there is an SA for that type of traffic. If there is no SA, IKE is called to establish one.
- IKE is a complex protocol based on three other protocols namely, Oakley, SKEME and ISAKMP.
- The Oakley protocol was proposed by Hilarie K. Orman in 1998. Oakley is a key creation protocol.
- The Oakley protocol allows authenticated parties to exchange keying material across an insecure connection using the Diffie–Hellman (DH) key exchange algorithm.
- SKEME protocol is designed by Hugo Krawcyzk, for key exchange. SKEME protocol uses public key encryption for entity authentication in a key exchange protocol.
- Internet Security Association and Key Management Protocol (ISAKMP) is a protocol designed by National Security Agency (NSA) that actually implements the exchanges defined in IKE.

- ISAKMP protocol defines several packets, protocols, and parameters that allow the IKE exchanges to take place in standardized, formatted messages to create SAs.
- ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent; protocols such as Internet Key Exchange (IKE).
- ISAKMP defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques and threat mitigation (e.g. denial of service and replay attacks).

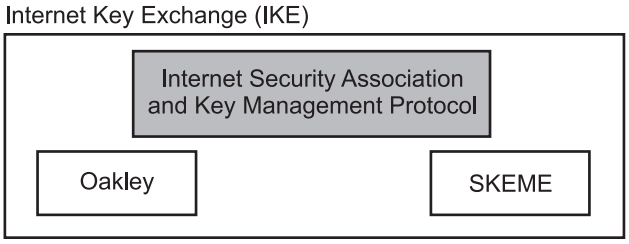


Fig. 4.13: IKE Components

4.1.6 Virtual Private Network

- A Virtual Private Network (VPN) is a technology that is gaining popularity among large organizations that use the global Internet for both intra- and inter-organization communication, but require privacy in their intra-organization communication.
- A VPN is a private computer network that uses a public telecommunication network (usually the Internet) to connect remote sites or users together.
- VPN is a network that is private but virtual. It is private because it guarantees privacy inside the organization.
- VPN is virtual, because it does not use real private WANs; the network is physically public but virtually private.
- A VPN is a private network that uses a public network (usually the Internet) to connect remote sites.
- The VPN uses "virtual" connections routed through the Internet from the business's private network to the remote sites.
- Fig. 4.14 shows the idea of a virtual private network. Routers R1 and R2 use VPN technology to guarantee privacy for the organization.
- VPN technology uses ESP protocol of IPSec in the tunnel mode. A private datagram, including the header, is encapsulated in an ESP packet.
- The router at the border of the sending site uses its own IP address and the address of the router at the destination site in the new datagram.

- The public network (Internet) is responsible for carrying the packet from R1 to R2. Outsiders cannot decipher the contents of the packet or the source and destination addresses.
- Deciphering takes place at R2, this finds the destination address of the packet and delivers it.

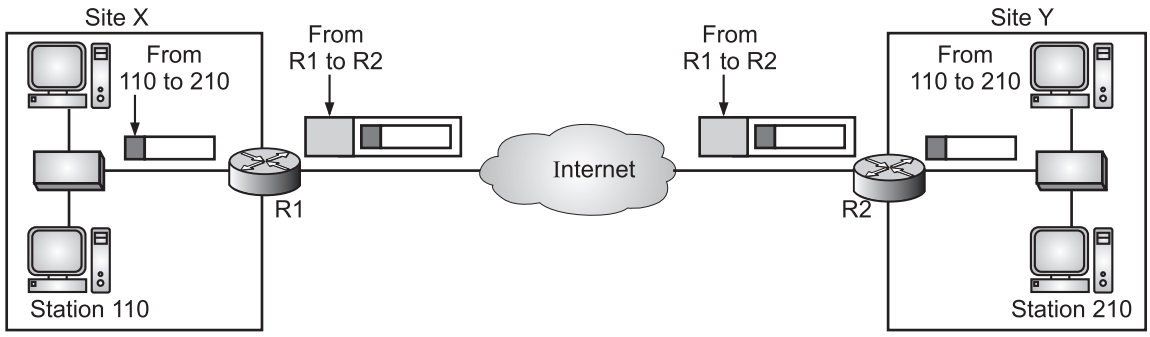


Fig. 4.14: VPN

Benefits of VPN:

1. **Security:** The VPN should protect data while it's travelling on the public network. If intruders attempt to capture data, they should be unable to read or use it.
2. **Reliability:** Employees and remote offices should be able to connect to VPN. The virtual network should provide the same quality of connection for each user even when it is handling the maximum number of simultaneous connections.
3. **Cost Savings:** Its operational cost is less as it transfers the support burden to the service providers.
4. **Scalability:** Growth is the flexible, i.e., we can easily add new locations to the VPN.

Disadvantages of VPN:

1. For VPN network to establish, we require an in-depth understanding of the public network security issues.
2. VPNs need to accommodate complicated protocols other than IP.

4.2 SSL/TLS

- The Secure Sockets Layer (SSL) protocol and the Transport Layer Security (TLS) protocol are the two protocols are dominant today for providing security at the transport layer.
- The SSL protocol addresses the security issues like privacy, integrity, and authentication. The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications.
- Fig. 4.15 shows the location of SSL and TLS in the Internet model.

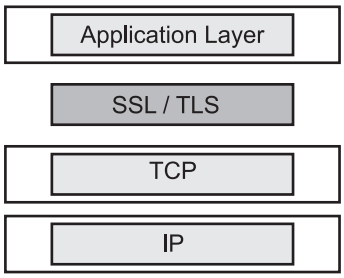


Fig. 4.15: Position of SSL and TLS in the Internet Model

- One of the goals of SSL and TLS protocols is to provide server and client authentication, data confidentiality, and data integrity.
- Application-layer client/server programs, such as HTTP, that use the services of TCP can encapsulate their data in SSL packets.
- If the server and client are capable of running SSL (or TLS) programs, then the client can use the URL https://... instead of http://... to allow HTTP messages to be encapsulated in SSL (or TLS) packets.
- For example, credit card numbers can be safely transferred via the Internet for online shoppers.
- The 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.
- TLS was derived from a security protocol called Secure Service Layer (SSL). TLS (Transport Layer Security) is just an updated, more secure, version of SSL. TLS ensures that no third party may eavesdrops or tampers with any message.
- TLS, the successor of the now-deprecated Secure Sockets Layer (SSL), is a cryptographic protocol designed to provide communications security over a computer network.
- Secure Sockets Layer/Transport Layer Security (SSL/TLS) is a widely supported protocol both on corporate networks and on the Internet for secures to transmit sensitive information.
- SSL/TLS is a must whenever sensitive information such as usernames and passwords or payment processing information is being transferred.

SSL Features:

- The salient features of SSL protocol are as follows:
  1. SSL supported by almost all web browsers.
  2. SSL provides network connection security through confidentiality (information is exchanged in an encrypted form), authentication (entities identify each other through the use of digital certificates) and reliability (maintains message integrity checks).

3. SSL is available for all TCP applications.
4. Provides ease in doing business with new online entities.
5. SSL developed primarily for Web e-commerce.

SSL Architecture:

- The SSL protocol was developed by Netscape Corporation in 1994 to provide exchange of information between a Web browser and a Web server in a secure manner.
- SSL is designed to provide security and compression services to data generated from the application layer.
- Typically, SSL can receive data from any application layer protocol, but usually the protocol is HTTP. The data received from the application is compressed (optional), signed, and encrypted.
- The data is then passed to a reliable transport layer protocol such as TCP. Netscape developed SSL in 1994. Versions 2 and 3 were released in 1995. In this section, we discuss the current version of SSL i.e., SSLv3.

4.2.1 SSL Services

- SSL provides several services on data received from the application layer. Some of them are explained below:
  1. **Fragmentation:** First, SSL divides the data into blocks of 2^{14} bytes or less.
  2. **Compression**: Each fragment of data is compressed using one of the lossless compression methods negotiated between the client and server. This service is optional.
  3. **Message Integrity:** To preserve the integrity of data, SSL uses a keyed-hash function to create a MAC.
  4. **Confidentiality:** To provide confidentiality, the original data and the MAC are encrypted using symmetric-key cryptography.
  5. **Framing**: A header is added to the encrypted payload. The payload is then passed to a reliable transport layer protocol.

4.2.2 Security Parameters

- SSL is a standard security protocol which is used for establishing encrypted links between a web server and a browser in a client server communication (online communication).
- SSL security parameters are given below:
  1. **Key Exchange Algorithms:** To exchange an authenticated and confidential message, the client and the server each need a set of cryptographic secrets. However, to create these secrets, one pre-master secret must be established

between the two parties. SSL defines several key-exchange methods to establish this pre-master secret.

2. **Encryption/Decryption Algorithms:** The client and server also need to agree to a set of encryption and decryption algorithms.
3. **Hash Algorithms:** SSL uses hash algorithms to provide message integrity (message authentication). Several hash algorithms have also been defined for this purpose.
4. **Cipher Suite:** The combination of key exchange, hash, and encryption algorithms defines a cipher suite for each SSL session.
5. **Compression Algorithms:** Compression is optional in SSL. No specific compression algorithm is defined. Therefore a system can use whatever compression algorithm it desires.

SSL Cryptographic Parameter Generation:

- To achieve message integrity and confidentiality, SSL needs six cryptographic secrets, four keys and two IVs (Initialization Vectors).
- The client needs one key for message authentication, one key for encryption, and one IV as original block in calculation and the server needs the same.
- SSL requires that the keys for one direction be different from those for the other direction. If there is an attack in one direction, the other direction is not affected.
- The parameters are generated using the following process :
  1. The client and server exchange two random numbers; one is created by the client and the other by the server.
  2. The client and server exchange one pre-master secret using one of the predefined key- exchange algorithms.
  3. A 48-byte master secret is created from the pre-master secret by applying two hash functions (SHA-1 and MD5), as shown in Fig. 4.16.

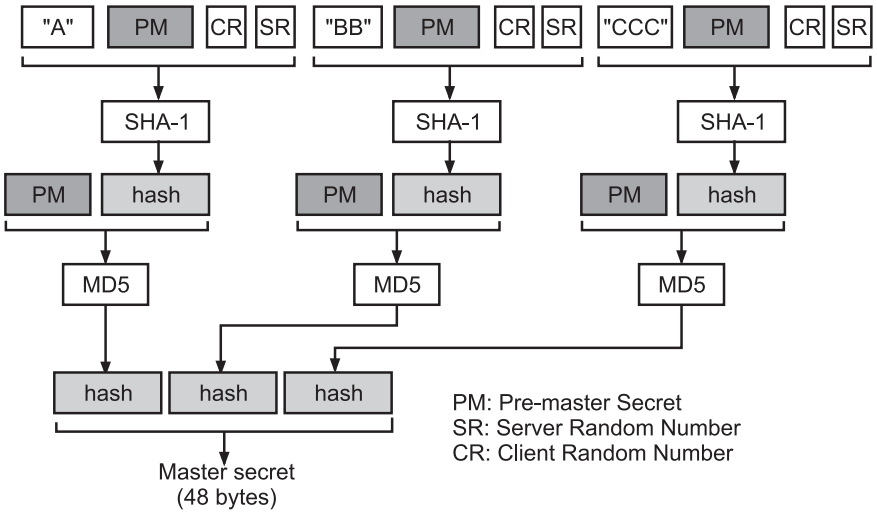


Fig. 4.16: Calculation of Master Secret from Pre-master Secret

4. The master secret is used to create variable-length key material by applying the same set of hash functions and pre-pending with different constants, as shown in Fig. 4.17. The module is repeated until key material of adequate size is created.

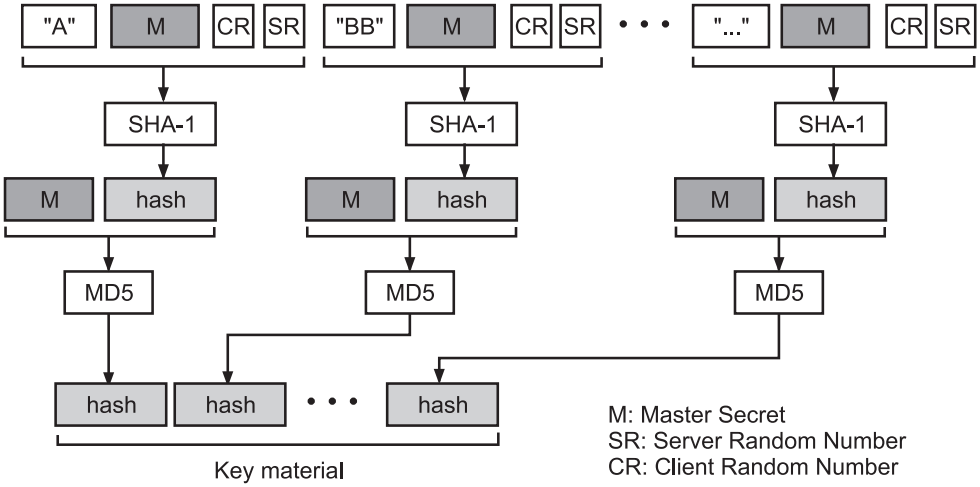


Fig. 4.17: Calculation of Key Material from Master Secret

5. Six different secrets are extracted from the key material, as shown in Fig. 4.18.

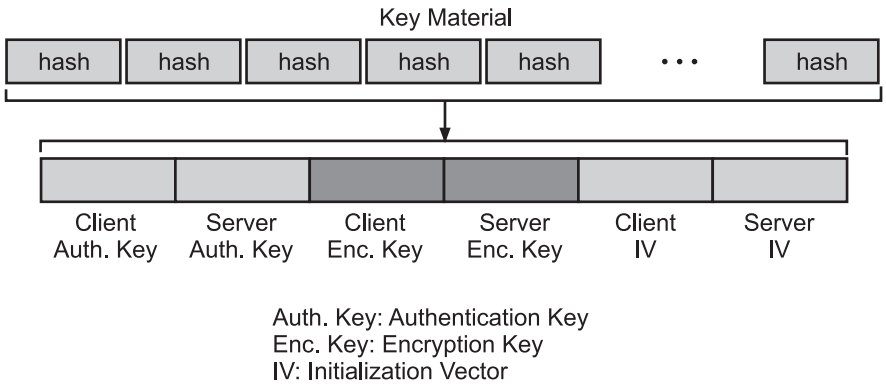


Fig. 4.18: Extractions of Cryptographic Secrets from Key Material

4.2.3 Sessions and Connections

- A session in SSL is an association between a client and a server. After a session is established, the two parties have common information such as the session identifier, the certificate authenticating each of them (if necessary), the compression method (if needed), the cipher suite, and a master secret that is used to create keys for message authentication encryption.
- For two entities to exchange data the establishment of a session is necessary, but not sufficient; they need to create a connection between themselves.

- The two entities exchange two random numbers and create, using the master secret, the keys and parameters needed for exchanging messages involving authentication and privacy.
- A session can consist of number of connections. A connection between two parties can be terminated and reestablished within the same session.
- When a connection is terminated, the two parties can also terminate the session, but it is not mandatory. A session can be suspended and resumed again.

4.2.4 Four Protocols

- In previous sections we studied the idea of SSL without showing how SSL accomplishes its tasks.
- SSL defines four protocols (Record Protocol, Handshake Protocol, ChangeCipherSpec Protocol and Alert Protocol) in two layers namely, application layer and transport layer as shown in Fig. 4.19.
- The **Record Protocol** of SSL is the carrier. The Record Protocol carries messages from three other protocols as well as the data coming from the application layer.
- Messages from the Record Protocol are payloads to the transport layer, normally TCP (Transmission Control Protocol).
- The **Handshake Protocol** of SSL provides security parameters for the Record Protocol. It establishes a cipher set and provides keys and security parameters.
- The Handshake Protocol also authenticates the server to the client and the client to the server if needed.
- The **ChangeCipherSpec Protocol** of SSL is used for signaling the readiness of cryptographic secrets. The **Alert Protocol** of SSL is used to report abnormal conditions.

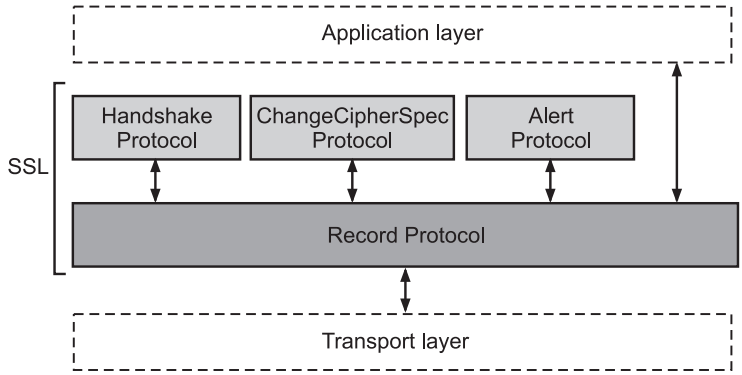


Fig. 4.19: Four Protocols in SSL

- Let us explain the four protocols of SSL in Fig. 4.19 in detail:

1. Handshake Protocol:

- This Protocol uses messages to negotiate the cipher suite, to authenticate the server to the client and the client to the server if needed and to exchange information for building the cryptographic secrets.

- The handshaking is done in four phases, as shown in Fig. 4.20.
  - **Phase I (Establishing Security Capability):** In Phase I, the client and the server announce their security capabilities and choose those that are convenient for both. In Phase I, a session ID is established and the cipher suite is chosen. The parties agree upon a particular compression method. Finally, two random numbers are selected, one by the client and one by the server, to be used for creating a master secret as we saw before.
  - **Phase II (Server Key Exchange and Authentication):** In Phase II, the server authenticates itself if needed. The sender may send its certificate, its public key, and may also request certificates from the client.
  - **Phase III (Client Key Exchange and Authentication):** Phase III is designed to authenticate the client.
  - **Phase IV (Finalizing and Finishing):** In Phase IV, the client and server send messages to change cipher specification and to finish the handshaking protocol.

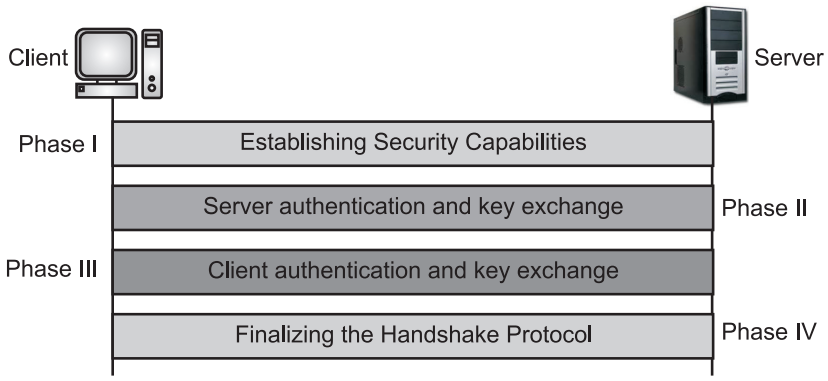


Fig. 4.20: Phases in Handshake Protocol

2. ChangeCipherSpec Protocol:

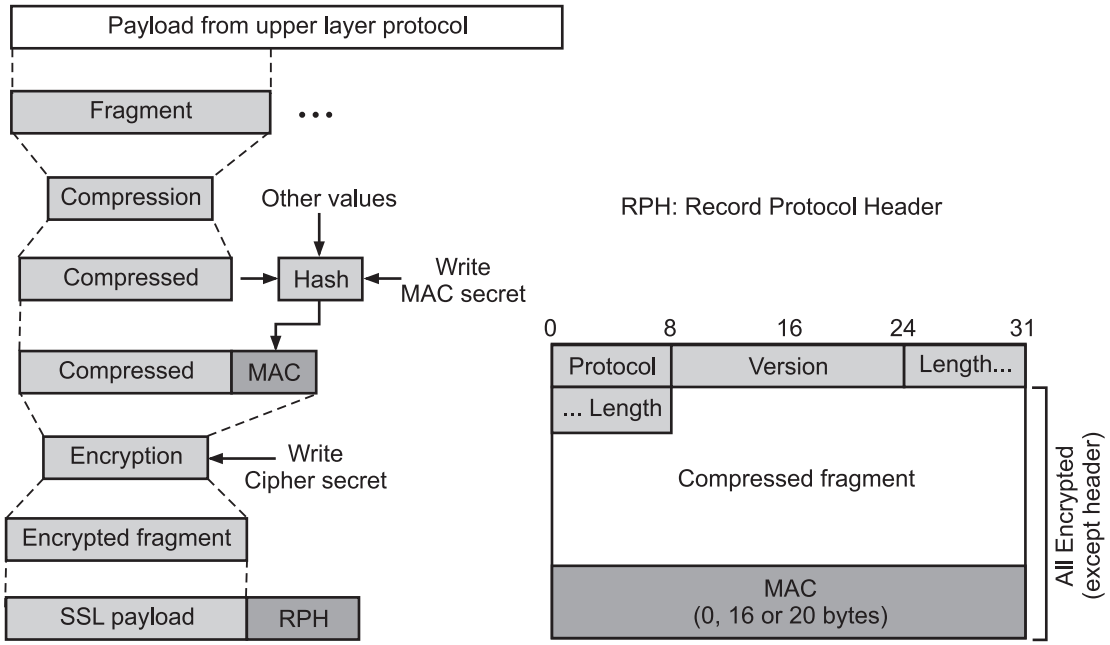
- In previous point, have seen that the negotiation of the cipher suite and the generation of cryptographic secrets are formed gradually during the Handshake Protocol. The question now is 'when can the two parties use these parameter secrets?.
- SSL mandates that the parties cannot use these parameters or secrets until they have sent or received a special message, the Change-CipherSpec message, which is exchanged during the Handshake protocol and defined in the ChangeCipherSpec Protocol.
- The reason is that the issue is not just sending or receiving a message. The sender and the receiver need two states, not one. One state, the pending state, keeps track of the parameters and secrets.
- The other state, the active state, holds parameters and secrets used by the Record Protocol to sign/verify or encrypt/decrypt messages. In addition, each state holds two sets of values namely, read (inbound) and write (outbound).

3. Alert Protocol:

- The Alert Protocol in SSL used for reporting errors and abnormal conditions. It uses only one message that describes the problem and its level (warning or fatal).

4. Record Protocol:

- The Record Protocol of SSL carries messages from the upper layer (Handshake Protocol, ChangeCipherSpec Protocol, Alert Protocol, or application layer).
- The message is fragmented and optionally compressed; a MAC is added to the compressed message using the negotiated hash algorithm.
- The compressed fragment and the MAC are encrypted using the negotiated encryption algorithm. Finally, the SSL header is added to the encrypted message.
- Fig. 4.21 shows this process at the sender. The process at the receiver is reversed.



(a) Process **(b) Encapsulation**

Fig. 4.21: Processing done by the Record Protocol

4.2.5 Transport Layer Security

- Two protocols are dominant today for providing security at the transport layer namely, Secure Sockets Layer (SSL) protocol and the Transport Layer Security (TLS) protocol.
- When the SSL protocol was standardized by the IETF (Internet Engineering Task Force), it was renamed to Transport Layer Security (TLS). Many use the TLS and SSL names interchangeably (SSL/TLS).

- TLS evolved from Secure Socket Layers (SSL) which was originally developed by Netscape Communications Corporation in 1994 to secure web sessions.
- SSL 1.0 was never publicly released, whilst SSL 2.0 was quickly replaced by SSL 3.0 on which TLS is based.
- TLS was first specified in RFC 2246 in 1999 as an applications independent protocol, and whilst was not directly interoperable with SSL 3.0, offered a fallback mode if necessary.
- However, SSL 3.0 is now considered insecure and was deprecated by RFC 7568 in June 2015, with the recommendation that TLS 1.2 should be used. TLS 1.3 is also currently (as of December 2015) under development and will drop support for less secure algorithms.
- TLS was designed to operate on top of a reliable transport protocol such as TCP. However, it has also been adapted to run over datagram protocols such as UDP.
- TLS encrypts data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what user transmit which is particularly useful for private and sensitive information such as passwords, credit card numbers, and personal correspondence.
- The TLS protocol is designed to provide three essential services amely, encryption, authentication and data integrity.
- TLS uses a combination of symmetric and asymmetric cryptography, as this provides a good compromise between performance and security when transmitting data securely.
- With symmetric cryptography, data is encrypted and decrypted with a secret key known to both sender and receiver.
- Symmetric cryptography is efficient in terms of computation, but having a common secret key means it needs to be shared in a secure manner.
- Asymmetric cryptography uses key pairs – a public key, and a private key. The public key is mathematically related to the private key, but given sufficient key length, it is computationally impractical to derive the private key from the public key.
- This allows the public key of the recipient to be used by the sender to encrypt the data they wish to send to them, but that data can only be decrypted with the private key of the recipient.
- For example, for performing secure web browsing we use of SSL/TLS protocol. HyperText Transfer Protocol (HTTP) protocol is used for web browsing.
- The function of https is similar to HTTP. The only difference is that https provides “secure” web browsing. The https stands for HTTP over SSL.
- This protocol is used to provide the encrypted and authenticated connection between the client Web browser and the Web server.

4.3 PGP

- PGP stands for Pretty Good Privacy. PGP was invented by Phil Zimmerman in 1991.
- PGP provide e-mail with privacy, integrity, and authentication. PGP can be used to create secure e-mail messages.
- PGP is a popular encryption and decryption program used to encrypt and decrypt e-mail over the Internet.
- Encryption program uses cryptography to prevent unauthorized access to digital information. Cryptography is used to protect digital information on computers as well as the digital information that is sent to other computers over the Internet.
- PGP is a hybrid cryptosystem that combines the advantages of both symmetric and public key cryptography. PGP is used to protect the privacy of e-mail communication and files stored on disk.
- The key features of PGP include generating message digests, digital signatures, management of personal key rings and distributable public key certificates.

4.3.1 Security Parameters

- PGP was designed to provide main three parameters of security, i.e., privacy, integrity, authentication in the sending of e-mail.
- PGP uses a combination of secret key encryption and public key encryption to provide privacy.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity and authentication.
- PGP provides confidentiality through the use of symmetric block encryption. PGP provides compression by using the ZIP algorithm.

4.3.2 Services

- Let us discuss the general idea of PGP, moving from a simple scenario to a complex one. We use the term “Data” to show the message prior to processing.
- The simplest scenario is to send the e-mail message in plaintext as shown in Fig. 4.22. There is no message integrity or confidentiality in this scenario.

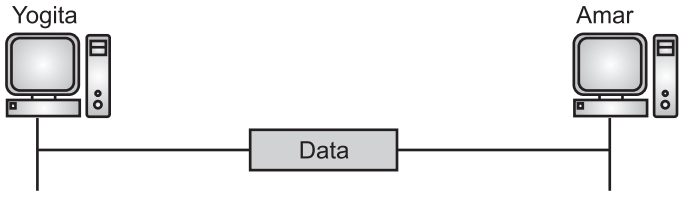


Fig. 4.22: A Plaintext Message

1. Message Integrity:

- Probably the next improvement is to let Yogita sign the message. Yogita creates a digest of the message and signs it with her private key (See Fig. 4.23).
- When Amar receives the message, he verifies the message by using Yogita's public key. Two keys are needed for this scenario. Yogita needs to know her private key; Amar needs to know Yogita's public key.

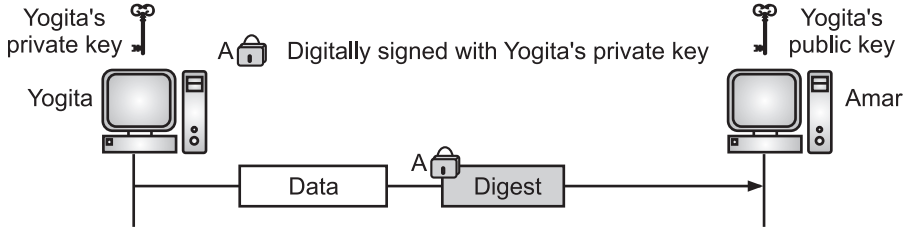


Fig. 4.23: An Authenticated Message

- Authentication means to verify that the message comes from the intended sender. Integrity means to ensure that the message has not been altered/modified in transit.

2. Compression:

- A further improvement is to compress the message to make the packet more compact. This improvement has no security benefit, but it eases the traffic.
- Fig. 4.24 shows the new scenario using compression.

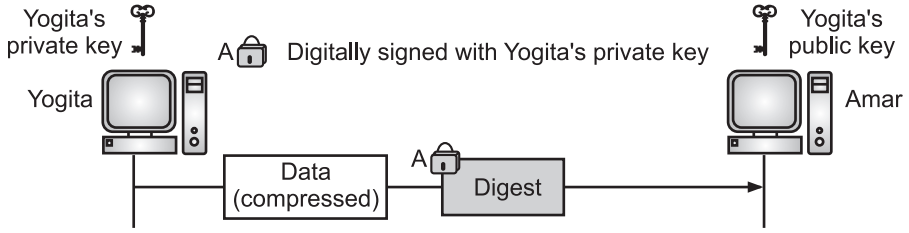


Fig. 4.24: A Compressed Message

3. Confidentiality:

- Confidentiality means to protect the message so that it can be read-only by the intended recipient.
- Confidentiality in an e-mail system can be achieved using conventional encryption with a one-time session key.
- Yogita can create a session key, use the session key to encrypt the message and the digest, and send the key itself with the message.
- However, to protect the session key, Yogita encrypts it with Amar's public key. When Amar receives the packet, he first decrypts the key, using his private key to remove the key.
- He then uses the session key to decrypt the rest of the message. After decompressing the rest of the message, Amar creates a digest of the message and checks to see if it is equal to the digest sent by Yogita. If it is, then the message is authentic.

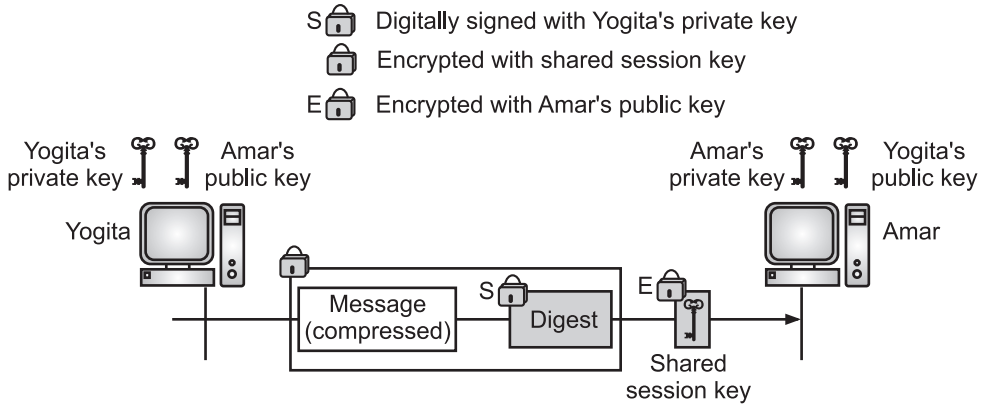


Fig. 4.25: A Confidential Message

4. Segmentation:

- PGP allows segmentation of the message after it has been converted to Radix-64 to make each transmitted unit the uniform size allowed by the underlying e-mail protocol.

5. Code Conversion:

- Code conversion is service provided by PGP. Most e-mail systems allow the message to consist of only ASCII characters.
- To translate other characters not in the ASCII set, PGP uses Radix-64 conversion.

4.3.3 Key Rings

- In all previous scenarios, we assumed that Yogita needs to send a message only to Amar. That is not always the case.
- Yogita may need to send messages to many people; she needs key rings. In this case, Yogita needs a ring of public keys, with a key belonging to each person with whom Yogita needs to correspond (send or receive messages).
- In addition, the PGP designers specified a ring of private/public keys. One reason is that Yogita may wish to change her pair of keys from time to time.
- Another reason is that Yogita may need to correspond with different groups of people (friends, colleagues, relatives and so on).
- Yogita may wish to use a different key pair for each group. Therefore, each user needs to have two sets of rings namely, a ring of private/public keys and a ring of public keys of other people.
- Fig. 4.26 shows a community of people, each having a ring of pairs of private/public keys and, at the same time, a ring of public keys belonging to other people in the community.

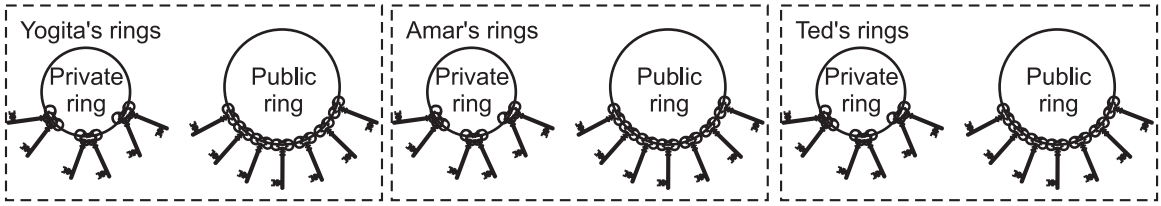


Fig. 4.26: PGP Key Rings

- Yogita, for example, has several pairs of private/public keys belonging to her and public keys belonging to other people.
- Note that everyone can have more than one public key. Following two cases may arise:

  Case 1: Yogita needs to send a message to another person in the community.

  (i) She uses her private key to sign the digest.

  (ii) She uses the receiver's public key to encrypt a newly created session key.

  (iii) She encrypts the message and signed digest with the session key created.

  Case 2: Yogita receives a message from another person in the community.

  (i) She uses her private key to decrypt the session key.

  (ii) She uses the session key to decrypt the message and digest.

  (iii) She uses her public key to verify the digest.

4.3.4 PGP Algorithms

- PGP defines a set of asymmetric-key and symmetric-key algorithms, cryptography hash functions and compression methods.
- When Yogita sends an e-mail to Amar, she defines the algorithm she has used for each purpose.

4.3.5 PGP Certificates

- PGP uses certificates to authenticate public keys. In PGP, there is no need for CAs; anyone in the ring can sign a certificate for anyone else in the ring.
- Amar can sign a certificate for Ted, John, Anne and so on. There is no hierarchy of trust in PGP; there is no tree.
- The lack of hierarchical structure may result in the fact that Ted may have one certificate from Amar and another certificate from Liz.
- If Yogita wants to follow the line of certificates for Ted, there are two paths, one starts from Amar and one starts from Liz.
- An interesting point is that Yogita may fully trust Amar, but only partially trust Liz. There can be multiple paths in the line of trust from a fully or partially trusted authority to a certificate.
- In PGP, the issuer of a certificate is usually called an introducer. In short, In PGP, there can be multiple paths from fully or partially trusted authorities to any subject.

Trusts and Legitimacy:

- The term trust refers to the ability of an application to perform actions with integrity, to keep confidential information private,
- The entire operation of PGP is based on introducer trust, the certificate trust, and the legitimacy of the public keys.

1. Introducer Trust Levels:

- With the lack of a Central Authority (CA), it is obvious that the ring cannot be very large if every user in the PGP ring of users has to fully trust everyone else, (even in real life we cannot fully trust everyone that we know).
- To solve this problem, PGP allows different levels of trust. The number of levels is mostly implementation dependent, but for simplicity, let us assigns three levels of trust to any introducer: none, partial and full.
- The introducer trust level specifies the trust levels issued by the introducer for other people in the ring.
- For example, Yogita may fully trust Amar, partially trust Anne, and not trust John at all. There is no mechanism in PGP to determine how to make a decision about the trustworthiness of the introducer; it is up to the user to make this decision.

2. Certificate Trust Levels:

- When Yogita receives a certificate from an introducer, she stores the certificate under the name of the subject (certified entity). She assigns a level of trust to this certificate.
- The certificate trust level is normally the same as the introducer trust level that issued the certificate. Assume that Yogita fully trusts Amar, partially trusts Anne and Janette, and has no trust in John. The following scenarios can happen:
  - (i) Amar issues two certificates, one for Linda (with public key K1) and one for Lesley (with public key K2). Yogita stores the public key and certificate for Linda under Linda's name and assigns a full level of trust to this certificate. Yogita also stores the certificate and public key for Lesley under Lesley's name and assigns a full level of trust to this certificate.
  - (ii) Anuja issues a certificate for John (with public key K3). Yogita stores this certificate and public key under John's name, but assigns a partial level for this certificate.
  - (iii) Anne issues two certificates, one for John (with public key K3) and one for Lee (with public key K4). Yogita stores Chetan's certificate under his name and Amol's certificate under his name, each with a partial level of trust. Note that John now has two certificates, one from Anne and one from Janette, each with a partial level of trust.
  - (iv) John issues a certificate for Liz. Yogita can discard or keep this certificate with a signature trust of none.

3. Key Legitimacy:

- The purpose of using introducer and certificate trusts is to determine the legitimacy of a public key.
- Yogita needs to know how legitimate the public keys of Amar, John, Liz, Anne and so on are. PGP defines a very clear procedure for determining key legitimacy.
- The level of the key legitimacy for a user is the weighted trust levels of that user. For example, suppose we assign the following weights to certificate trust levels:
  - o A weight of 0 to a non-trusted certificate.
  - o A weight of 1/2 to a certificate with partial trust.
  - o A weight of 1 to a certificate with full trust.
- Then to fully trust an entity, Yogita needs one fully trusted certificate or two partially trusted certificates for that entity.
- For example, Yogita can use John's public key in the previous scenario because both Anne and Janette have issued a certificate for John, each with a certificate trust level of 1/2.
- Note that the legitimacy of a public key belonging to an entity does not have anything to do with the trust level of that person.
- Although Amar can use John's public key to send a message to him, Yogita cannot accept any certificate issued by John because, for Yogita, John has a trust level of none.

Trust Model in PGP:

- As Phil Zimmermann has proposed, we can create a trust model for any user in a ring with the user as the center of activity.
- A trust model can look like the one shown in Fig. 4.27 which shows the trust model for Yogita at some moment.

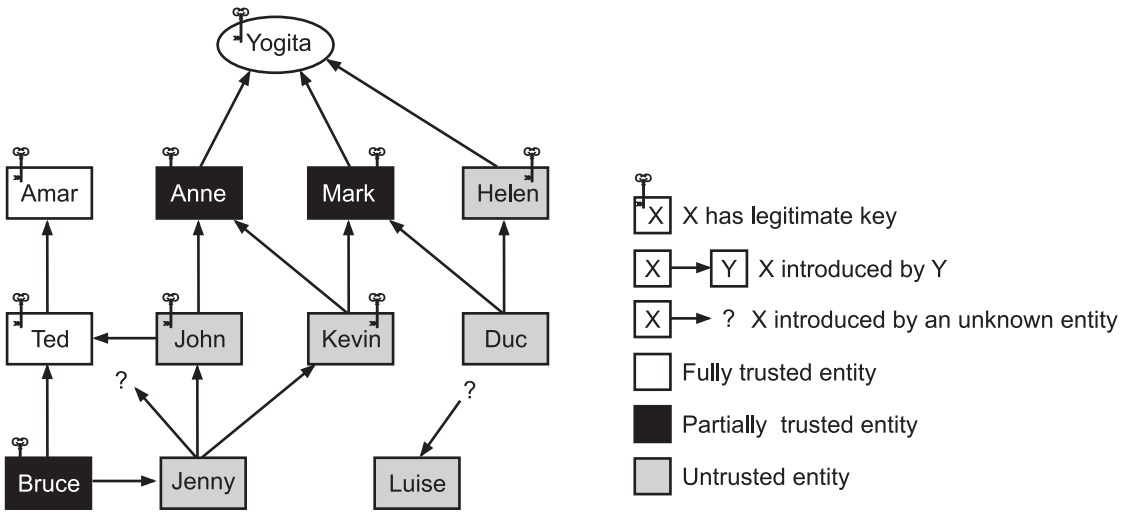


Fig. 4.27: Trust Model in PGP

- Fig. 4.27 shows that there are three entities in Yogita's ring with full trust (Yogita herself, Amar, and Ted).
- The Fig. 4.27 also shows three entities with partial trust (Anne, Mark, and Bruce). There are also six entities with no trust. Nine entities have a legitimate key.
- Yogita can encrypt a message to any one of these entities or verify a signature received from one of these entities (Yogita's key is never used in this model).
- There are also three entities that do not have any legitimate keys with Yogita. Amar, Anne, and Mark have made their keys legitimate by sending their keys by e-mail and verifying their fingerprints by phone.
- On the other hand, Helen has sent a certificate from a CA because she is not trusted by Yogita and verification on the phone is not possible.
- Although Ted is fully trusted, he has given Yogita a certificate signed by Amar. John has sent Yogita two certificates, one signed by Ted and one by Anne.
- Kevin has sent two certificates to Yogita, one signed by Anne and one by Mark. Each of these certificates gives Kevin half a point of legitimacy; therefore, Kevin's key is legitimate.
- Duc has sent two certificates to Yogita one signed by Mark and the other by Helen. Since Mark is half-trusted and Helen is not trusted, Duc does not have a legitimate key.
- Jenny has sent four certificates, one signed by a half-trusted entity, two by untrusted entities, and one by an unknown entity. Jenny does not have enough points to make her key legitimate.
- Luise has sent one certificate signed by an unknown entity. Note that Yogita may keep Luise's name in the table in case future certificates for Luise arrive.

Web of Trust:

- PGP contains the concept of Web of Trust where the certification can be done by end users thereby avoiding the need for a single certification authority.
- PGP can eventually make a web of trust between a group of people.
- If each entity introduces more entities to other entities, the public key ring for each entity gets larger and larger and entities in the ring can send secure e-mail to each other.

Key Revocation:

- In PGP it may become necessary for an entity to revoke his or her public key from the ring. This may happen if the owner of the key feels that the key is compromised (stolen, for example) or just too old to be safe.
- To revoke a key, the owner can send a revocation certificate signed by herself. The revocation certificate must be signed by the old key and disseminated to all the people in the ring that use that public key.

4.4 FIREWALLS (April 16, 18)

- A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. To control access to a system we need firewalls.
- The purpose of firewall is to establish a barrier between the internal network and incoming traffic from external sources (such as the Internet) in order to block malicious traffic like viruses, attackers and hackers.
- A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet.
- Firewall is designed to forward some packets and filter (not forward) others. Fig. 4.28 shows concept of firewall.
- For example, 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.

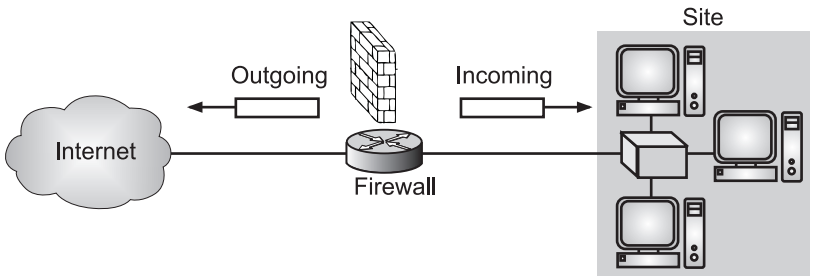


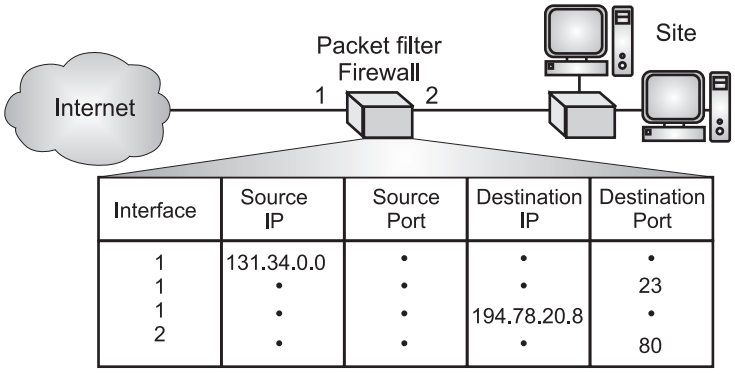
Fig. 4.28: Firewall

- Firewall is a network device that isolates organization's internal network from larger outside network/Internet.
- Firewall can be hardware, software or combined system that prevents unauthorized access to or from internal network.
- A firewall is usually classified as a packet-filter firewall and a proxy-based firewall. Let us see them in detail.

1. Packet-Filter Firewall: (Oct. 17, April 18, 19)

- A firewall can be used as a packet filter. Packet-filter firewall is a network security technique that is used to control data flow to and from a network.
- It is a security mechanism that allows the movement of packets across the network and controls their flow on the basis of a set of rules, protocols, IP addresses, and ports.
- Packet filter can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses and type of protocol (TCP or UDP).

- A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded).
- Fig. 4.29 shows an example of a filtering table for packet filter firewall. According to the Fig. 4.29, the following packets are filtered:
  - Incoming packets from network 131.34.0.0 are blocked (security precaution). Note that the * (asterisk) means "any."
  - Incoming packets destined for any internal TELNET server (port 23) are blocked.
  - Incoming packets destined for internal host 194.78.20.8 are blocked. The organization wants this host for internal use only.
  - Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the Internet.



Interface	Source IP	Source Port	Destination IP	Destination Port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	*	*	80

Fig. 4.29: Packet-Filter Firewall

Advantages of Packet Filter Firewalls:

(i) One packet-filter firewall can help protect an entire network.

(ii) Packet filter firewall provides efficient at processing packets.

(iii) Packet filter firewall enables complex security policies through filtering on protocol headers.

Disadvantages of Packet Filter Firewalls:

(i) Incapable of filtering at application layer.

(ii) Can be difficult to securely configure.

2. Proxy Firewall:

- The packet-filter firewall is based on the information available in the two layers namely, network layer and transport layer headers such as IP and TCP/UDP.
- However, sometimes we need to filter a message based on the information available in the message itself (at the application layer).
- For example, assume that an organization wants to implement the policies regarding its Web pages: only those Internet users who have previously established business relations with the company can have access; access to other users must be blocked.

- In this case, a packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP). Testing must be done at the application level (using URLs).
- One solution of above problem is to install a proxy computer (sometimes called an application gateway), which stands between the customer computer and the corporation computer.
- When the user client process sends a message, the application gateway runs a server process to receive the request. The server opens the packet at the application level and finds out if the request is legitimate.
- If it is, the server acts as a client process and sends the message to the real server in the corporation. If it is not, the message is dropped and an error message is sent to the external user.
- In this way, the requests of the external users are filtered based on the contents at the application layer.
- Fig. 4.30 shows an application gateway implementation for HTTP.

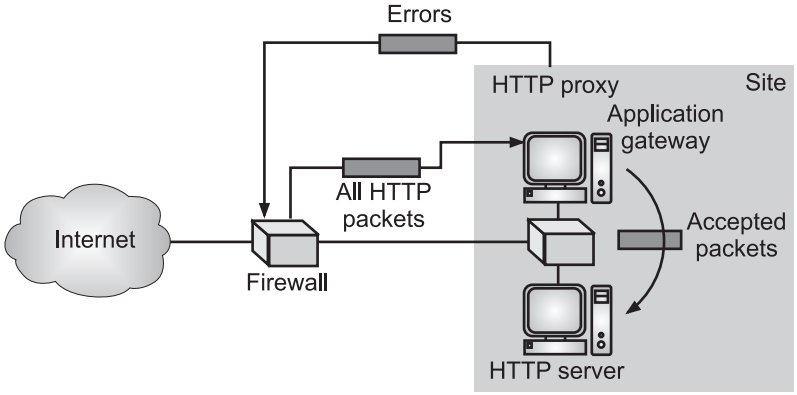


Fig. 4.30: Proxy Firewall

Advantages:

(i) Robust, protocol-aware logging is possible in proxy firewalls. This can make it significantly easier to identify the methods of an attack.

(ii) Proxy firewall provides high level of security than packet filter firewalls.

Disadvantages:

(i) Complex setup of application firewall needs more and detailed attentions to the applications that use the gateway.

(ii) Proxy firewalls are not compatible with all network protocols.

(iii) A reduction of performance occurs due to the additional processing requests required for application services.

PRACTICE QUESTIONS

Q.I Multiple Choice Questions:

1. IPSec is designed to provide security at the,
   (a) transport layer (b) network layer
   (c) application layer (d) session layer
2. In tunnel mode, IPSec protects the,
   (a) Entire IP packet (b) IP header
   (c) IP payload (d) IP trailer
3. Network layer firewall works as a,
   (a) frame filter (b) packet filter
   (c) signal filter (d) content filter
4. Network layer firewall has two sub-categories called as,
   (a) Stateful firewall and stateless firewall
   (b) Bit oriented firewall and byte oriented firewall
   (c) Frame firewall and packet firewall
   (d) Network firewall and data firewall
5. Extensible authentication protocol is authentication framework frequently used in,
   (a) wired personal area network
   (b) wireless networks
   (c) wired local area network
   (d) wired metropolitan area network
6. Pretty good privacy (PGP) is used in,
   (a) Browser security (b) email security
   (c) FTP security (d) WiFi security
7. PGP encrypts data by using a block cipher called as,
   (a) international data encryption algorithm
   (b) private data encryption algorithm
   (c) internet data encryption algorithm
   (d) local data encryption algorithm
8. Firewall is a type of,
   (a) Virus (b) Security threat
   (c) Worm (d) None of the mentioned

9. Unsolicited commercial email is known as,
   (a) Spam (b) Malware
   (c) Virus (d) Spyware
10. Which of the following is a class of computer threat,
   (a) Phishing (b) Soliciting
   (c) DoS attacks (d) Stalking
11. Which is a worldwide system of computer networks, i.e. a network of networks, which allows the participants (users) to share information?
   (a) Intranet (b) Extranet
   (c) WWW (d) Internet
12. IKE creates SAs for,
   (a) SSL (b) PGP
   (c) IPSec (d) VP
13. Which network is used inside an organization?
   (a) private (b) public
   (c) semi-private (d) semi-public
14. Which is a private network that uses the Internet model?
   (a) intranet
   (b) internet
   (c) extranet
   (d) None of the mentioned
15. Which is a network that allows authorized access from outside users?
   (a) intranet (b) internet
   (c) extranet (d) None of the mentioned
16. Following which provides privacy for LANs that must communicate through the global Internet.
   (a) VPP (b) VNP
   (c) VNN (d) VPN
17. A _____ layer security protocol provides end-to-end security services for applications.
   (a) data link (b) network
   (c) transport (d) None of the mentioned
18. SSL provides,
   (a) message integrity (b) confidentiality
   (c) compression (d) All of the mentioned

19. IPSec can be divided into the following three function groups,
    (a) Transfer protocols (AH and ESP)
    (b) Key management (ISAKMP and IKE)
    (c) Database (SAD and SPD)
    (d) All of the mentioned
20. In _____, the cryptographic algorithms and secrets are sent with the message.
    (a) IPSec (b) SSL
    (c) TLS (d) PGP
21. One security protocol for the e-mail system is,
    (a) IPsec (b) SSL
    (c) PGP (d) None of the mentioned
22. _____ was invented by Phil Zimmerman.
    (a) IPSec (b) SSL
    (c) PGP (d) None of the above
23. Which provides privacy, integrity, and authentication in e-mail?
    (a) PGP (b) SSL
    (c) IPSec (d) None of the mentioned
24. Which is a collection of protocols designed by the IETF (Internet Engineering Task Force) to provide security for a packet at the network level?
    (a) IPSec (b) SSL
    (c) PGP (d) None of the mentioned
25. Which operates in the transport mode or the tunnel mode?
    (a) PGP (b) SSL
    (c) IPSec (d) None of the mentioned
26. In which mode IPSec protects information delivered from the transport layer to the network layer.
    (a) transport (b) tunnel
    (c) Either (a) or (b) (d) neither (a) nor (b)
27. IPSec in the _____ mode does not protect the IP header.
    (a) tunnel (b) transport
    (c) Either (a) or (b) (d) neither (a) nor (b)
28. The _____ mode is normally used when we need host-to-host (end-to-end) protection of data.
    (a) transport (b) tunnel
    (c) Either (a) or (b) (d) neither (a) nor (b)

29. In the _____ mode, IPsec protects the whole IP packet, including the original IP header.
    (a) transport (b) tunnel
    (c) either (a) or (b) (d) neither (a) nor (b)
30. IPSec defines two protocols: namely, _____ and _____.
    (a) AH; SSL (b) PGP; ESP
    (c) AH; ESP (d) none of the above
31. _____ provides authentication at the IP level.
    (a) AH (b) ESP
    (c) PGP (d) SSL
32. _____ provides either authentication or encryption, or both, for packets at the IP level.
    (a) AH (b) ESP
    (c) PGP (d) SSL
33. IPSec uses a set of SAs called them,
    (a) SAD (b) SAB
    (c) SADB (d) None of the mentioned
34. Collecting personal information and effectively posting as another individual is termed,
    (a) Spooling
    (b) Identity theft
    (c) Spoofing
    (d) Hacking
35. Which of the following forms the basis for the classification of cryptographic algorithms?
    (a) Plaintext alphabets, Number of keys, Key size, Symmetry of process
    (b) Secrecy of algorithms, Number of keys, Key size, Symmetry of process
    (c) Secrecy of algorithms, Cipher text alphabets, Key size, Usage statistics
    (d) Usage statistical, Number of keys, Key size, OS Specification Incorrect
36. Network security consists of:
    (a) Protection (b) Detection
    (c) Reaction (d) All of the mentioned
37. Which of the following we should configure the systems and networks as correctly as possible?
    (a) Protection (b) Detection
    (c) Reaction (d) None of the mentioned

38. Which protocol is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet?
    (a) AH (b) ESP
    (c) PGP (d) SSL
39. What is true about VPN in Network security methods?
    (a) A tool that authenticates the communication between a device and a secure network
    (b) VPN creating a secure, encrypted "tunnel" across the open internet
    (c) VPN typically based on IPSec or SSL
    (d) All of the mentioned
40. The IPSec protocols use a _____, where the communicating parties establish shared security attributes such as algorithms and keys.
    (a) Security Binding (SB)
    (b) Protection Association (PA)
    (c) Security Association (SA)
    (d) All of the mentioned
41. Which of these is a part of network identification?
    (a) User ID (b) Password
    (c) OTP (d) Fingerprint
42. Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?
    (a) Malware
    (b) Spyware
    (c) Adware
    (d) All of the mentioned
43. _____ is a type of software designed to help the user's computer detect viruses and avoid them
    (a) Malware (b) Adware
    (c) Antivirus (d) Both (b) and (c)
44. Read the following statement carefully and find out whether it is correct about the hacking or not?
    (a) It can be possible that in some cases, hacking a computer or network can be legal.
    (b) No, in any situation, hacking cannot be legal
    (c) It may be possible that in some cases, it can be referred to as a legal task
    (d) None of the mentioned

45. Which of the following refers to the violation of the principle if a computer is no more accessible?
    (a) Access control (b) Confidentiality
    (c) Availability (d) All of the mentioned
46. Which one of the following refers to the technique used for verifying the integrity of the message?
    (a) Digital signature (b) Decryption algorithm
    (c) Protocol (d) Message Digest
47. Which defines the type of security applied to a packet when it is to be sent or when it has arrived?
    (a) Security Report (SR)
    (b) Security Association (SA)
    (c) Security Policy (SP)
    (d) All of the mentioned
48. Which protocol used for the key management procedures in IPSec?
    (a) IKE (b) ISAKMP
    (c) SKEME (d) Oakley
49. Message authentication is a service beyond,
    (a) message confidentiality
    (b) message integrity
    (c) message splashing
    (d) message sending
50. In message confidentiality, the transmitted message must make sense to only intended,
    (a) receiver (b) sender
    (c) modular (d) translator
51. Which a private computer network that uses a public telecommunication network (usually the Internet) to connect remote sites or users together.
    (a) Intranet (b) Internet
    (c) Extranet (d) VPN
52. Which protocols providing security at the transport layer?
    (a) SSL (b) TLS
    (c) Both (a) and (b) (d) None of the mentioned
53. Which a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules?
    (a) router (b) firewall
    (c) switch (d) modem

54. Which firewall is a network security technique that is used to control data flow to and from a network?
    (a) packet-filter (b) proxy
    (c) Both (a) and (b) (d) None of the mentioned

Answers

1. (b)	2. (a)	3. (b)	4. (a)	5. (b)	6. (b)	7. (a)	8. (d)	9. (a)	10. (c)
11. (d)	12. (c)	13. (a)	14. (a)	15. (d)	16. (d)	17. (c)	18. (d)	19. (d)	20. (d)
21. (c)	22. (c)	23. (a)	24. (a)	25. (c)	26. (a)	27. (b)	28. (a)	29. (b)	30. (c)
31. (a)	32. (b)	33. (c)	34. (b)	35. (b)	36. (d)	37. (a)	38. (a)	39. (d)	40. (c)
41. (a)	42. (b)	43. (c)	44. (c)	45. (c)	46. (d)	47. (c)	48. (a)	49. (b)	50. (a)
51. (d)	52. (c)	53. (b)	54. (a)						

Q.II Fill in the Blanks:

1. An Internet is a network of _____.
2. A computer _____ is a software program that copies itself from one computer to the next.
3. In transport mode, the _____layer comes between the transport layer and the network layer.
4. _____ mode is used to create virtual private networks for network-to-network communications, host-to-network communications and host-to-host communications.
5. PGP uses _____ to authenticate public keys.
6. _____ defines the type of security applied to a packet when it is to be sent or when it has arrived.
7. The _____ should protect data while it's travelling on the public network.
8. _____ is a network device that isolates organization's internal network from larger outside network/Internet.
9. The _____ protocol is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet.
10. The _____ firewall is based on the information available in the two layers namely, network layer and transport layer headers such as IP and TCP/UDP.
11. _____ means to protect the message so that it can be read-only by the intended recipient.
12. The objective of _____ security is to establish rules and measures to use against attacks over the Internet.
13. IPsec uses _____ security services to protect communications over Internet Protocol (IP) networks.

14. The AH protocol uses a hash function and a _____ (secret) key to create a message digest.
15. _____ is the foundation of an IPsec communication which is a contract between two parties; it creates a secure channel between them.
16. A _____ firewall is also be called an application firewall or gateway firewall.
17. _____, which provides source authentication, integrity, and confidentiality.
18. A set of SAs that can be collected into a database called as _____.
19. _____ uses a combination of secret key encryption and public key encryption to provide privacy.
20. The _____ is a protocol designed to create both inbound and outbound Security Associations (SAs).
21. VPN is a network that is private but _____.
22. A _____ is a security device — computer hardware or software — that can help protect the network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on the computer.
23. The _____ protocol addresses the security issues like privacy, integrity, and authentication.
24. PGP uses certificates to authenticate _____ keys.
25. A _____ in SSL is an association between a client and a server.
26. The _____ protocol in SSL used for reporting errors and abnormal conditions.
27. _____ was derived from a security protocol called Secure Service Layer (SSL).
28. PGP can be used to create secure _____ messages.
29. TLS _____ data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what user transmit which is particularly useful for private and sensitive information such as passwords.
30. A firewall is a network security system that _____ and controls incoming and outgoing network traffic based on predetermined security rules.
31. Asymmetric cryptography uses key _____ - a public key, and a private key.

Answers

1. networks	2. worm	3. IPSec	4. Tunnel
5. certificates	6. SP	7. VPN	8. Firewall
9. AH	10. packet-filter	11. Confidentiality	12. Internet
13. cryptographic	14. symmetric	15. SA	16. proxy
17. ESP	18. SAD	19. PGP	20. IKE
21. virtual	22. firewall	23. SSL	24. public
25. session	26. Alert	27. TLS	28. e-mail
29. encrypts	30. monitors	31. pairs	

Q.III State True or False:

1. Internet Protocol Security (IPSec) is a set of protocols that provides security for Internet Protocol using advanced cryptography.
2. The IPSec, AH protocol provides confidentiality.
3. Payload Length define the length of the payload.
4. Tunnel mode is normally used between two routers, between a host and a router, or between a router and a host,
5. Message integrity is preserved in AH and not in ESP.
6. When a packet is to be sent out, the outbound SPD is consulted.
7. In transport mode, IPSec protects the entire IP packet.
8. Tunnel mode protects the payload to be encapsulated in the network layer
9. The Security Association and the keyed-hash digest of the data sent by the sender authenticate the sender of the data in both AH and ESP.
10. The entire operation of PGP is based on introducer trust, the certificate trust, and the legitimacy of the public keys.
11. IPSec can be a hardware, software or combined system that prevents unauthorized access to or from internal network.
12. Internet is a global network links thousands of computers at universities, research institutions, government agencies, business and houses throughout the world.
13. Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the Internet.
14. IPSec stands for IP Security.
15. A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
16. Authentication Header (AH) authenticates the origin of IP packets (datagrams) and guarantees the integrity of the data (means confirms the originating source of a packet and ensures that its contents have not been changed since transmission).
17. The tunnel mode of IPSec protects the payload to be encapsulated in the network layer.
18. The collection of parameters that the two devices will use is called a SA (Security Association).
19. Packet-filtering firewalls checks the packet's source and destination IP addresses. If packets match those of an "allowed" rule on the firewall, then it is trusted to enter the network.
20. IKE (Internet Key Exchange) is one of the primary protocols for IPsec since it establishes the security association between two peers.

21. A proxy firewall is a network security system that protects network resources by filtering messages at the application layer.
22. In tunnel mode, IPSec protects the entire IP packet.
23. IPSec provides access control indirectly using a Security Association Database (SAD).
24. The ESP protocol is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet.
25. The encryption of the message in ESP provides confidentiality.
26. IPSec requires a logical relationship between two hosts called a SA.
27. Each host that is using the IPSec protocol needs to keep a SPD.
28. The IKE is the protocol used to set up a security association (SA) in the IPSec protocol.
29. The ISAKMP protocol defines several packets, protocols, and parameters that allow the IKE exchanges to take place in standardized, formatted messages to create SAs.
30. PGP is a popular encryption and decryption program used to encrypt and decrypt e-mail over the Internet.
31 The VPN uses "virtual" connections routed through the Internet from the business's private network to the remote sites.
32. The SSL provide security to the data that is transferred between web browser and server.
33. The Handshake Protocol of SSL establishes a cipher set and provides keys and security parameters.
34. SSL encrypts data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what user transmit which is particularly useful for private and sensitive information such as passwords, credit card numbers etc.
35. PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity and authentication.
36. The purpose of using introducer and certificate trusts is to determine the legitimacy of a public key.

Answers

1. (T)	2. (F)	3. (F)	4. (T)	5. (T)	6. (F)	7. (F)	8. (F)	9. (T)	10. ()
11. (F)	12. (T)	13. (T)	14. (T)	15. (T)	16. (T)	17. (F)	18. (T)	19. (T)	20. (T)
21. (T)	22. (T)	23. (T)	24. (F)	25. (T)	26. (T)	27. (T)	28. (T)	29. (T)	30. (T)
31. (T)	32. (T)	33. (F)	34. (T)	35. (T)	36. (T)				

Q.IV Answer the following Questions:

(A) Short Answer Questions:

1. What is Internet?
2. Give importance of Internet security.
3. What is IPSec?
4. What is the purpose of firewall.
5. What is VPN?
6. List modes of IPSec.
7. What are key rings in PGP?
8. Define SA.
9. Give purpose of IKE?
10. Which services provided by IPSec?
11. List types of firewalls.
12. What is PGP certificate?
13. List services of PGP.
14. What is SSL/TLS?
15. List four protocols for SSL.

(B) Long Answer Questions:

1. Define Internet. List Internet security threats in detail.
2. What is tunnel mode? How it works? Explain diagrammatically.
3. With the help of diagram describe transport mode of IPSec.
4. Describe AH and ESP protocols. Also compare them.
5. What is Security Association (SA)? Explain with diagram.
6. What are SAD, SP and SPD? Give their purposes.
7. Explain the Oakley, SKEME and ISAKMP in detail.
8. Define VPN. How it works? State its advantages and disadvantages.
10. Write short note on: PGP security parameters.
11. With the help of diagram describe sessions and connections in SSL/TLS.
12. Explain protocols of SSL in detail.
13. Describe packet-filter and proxy firewalls diagrammatically. Also compare them.
14. Explain key rings in PGP with diagram.

UNIVERSITY QUESTIONS AND ANSWERS

April 2016

1. Explain firewalls? **[4 M]**

Ans. Refer to Section 4.4.

October 2017

1. What is packet filter? **[1 M]**

Ans. Refer to Section 4.4, Point (1).

April 2018

1. What is role of packet filter? **[1 M]**

Ans. Refer to Section 4.4, Point (1).

April 2019

1. What is firewall? Explain packet firewall. **[4 M]**

Ans. Refer to Section 4.4 and Section 4.4, Point (1).

❖❖❖