BUDDHA SERIES

(Unit Wise Solved Question & Answers)

Course – B.Tech.

College – Buddha Institute of Technology

(AKTU CODE-525)

Department: Computer Science & Allied

PROGRAM: AIML-DS

Subject: Computer Networks

(BCS 603)

Faculty Name: Mr. Shailesh Kumar Patel

Unit - 5

Q1. What is the purpose of the Domain Name System? Discuss the three main divisions of the domain name space. **(AKTU 2018-19)**

Solution:

Domain names are a key part of the Internet infrastructure. They provide a human-readable address for any web server available on the Internet.

A domain name serves as a human-readable, memorable address for websites, replacing complex numerical IP addresses (e.g., 192.0.2.1) with recognizable names (e.g., google.com). Its primary purposes are to facilitate easy navigation to web resources, establish a unique online brand identity, improve credibility, and provide a permanent address for a website even if its underlying physical server changes.

A Domain Name System (DNS) turns domain names into IP addresses, which allow browsers to get to websites and other internet resources.

- **Generic Domains:** These define registered hosts based on their organizational type using three-character suffixes, such as .com (commercial), .org (organizations), .edu (educational institutions), and .gov (government).
- **Country Domains:** These utilize two-character country codes (following ISO 3166 standards) to identify the geographical location of the entity, such as .uk (United Kingdom), .in (India), or .jp (Japan).
- **Inverse Domain (Reverse Lookup):** This specialized domain is used to resolve a known IP address back into its corresponding domain name, which is vital for security and auditing services.

Q2. What is the difference between a user agent (UA) and a mail transfer agent (MTA)? **(AKTU 2018-19)**

Solution:

A User Agent (UA) is the client-side software used to compose, read, and manage emails (e.g., Outlook, Gmail).
A Mail Transfer Agent (MTA) is server-side software that transfers, routes, and delivers those emails across the internet using SMTP.
UAs focus on the user's interaction with emails, MTAs are responsible for the actual transfer of email messages between servers.

Q3. Explain how SMTP can handle transfer of videos and images? Also, explain the advantages of IMAP4 over POP3 mail access protocols. **(AKTU 2024-25)**

Solution:

SMTP cannot handle binary files (images, videos, documents) natively because it only understands 7-bit ASCII text. MIME extends SMTP to allow it to carry non-text data.

SMTP (Simple Mail Transfer Protocol) handles the transfer of images and videos by relying on MIME (Multipurpose Internet Mail Extensions) to convert binary data into 7-bit ASCII text.

Difference between POP3 and IMAP:

Post Office Protocol (POP3)	Internet Message Access Protocol (IMAP)
POP is a simple protocol that only allows downloading messages from your Inbox to your local computer.	IMAP (Internet Message Access Protocol) is much more advanced and allows the user to see all the folders on the mail server.
The POP server listens on port 110, and the POP with SSL secure(POP3DS) server listens on port 995	The IMAP server listens on port 143, and the IMAP with SSL secure(IMAPDS) server listens on port 993.
In POP3 the mail can only be accessed from a single device at a time.	Messages can be accessed across multiple devices
To read the mail it has to be downloaded on the local system.	The mail content can be read partially before downloading.

The user can not organize mail in the mailbox of the mail server.	On the mail server, the user can directly arrange the email.
The user can not create, delete,e or rename email on the mail server.	The user can create, delete,e or rename an email on the mail server.
It is unidirectional i.e. all the changes made on a device do not affect the content present on the server.	It is Bi-directional i.e. all the changes made on the server or device are made on the other side too.
It does not allow a user to sync emails.	It allows a user to sync their emails.
It is fast.	It is slower as compared to POP3.
A user can not search the content of mail before downloading it to the local system.	A user can search the content of mail for a specific string before downloading.
It has two modes: delete mode and keep mode. • In delete mode, the mail is deleted from the mailbox after retrieval. • In keep mode, the mail remains in the mailbox after retrieval.	Multiple redundant copies of the message are kept at the mail server, in case of loss of message on a local server, the mail can still be retrieved
Changes in the mail can be done using local email software.	Changes made to the web interface or email software stay in sync with the server.
All the messages are downloaded at once.	The Message header can be viewed before downloading.

Q4. Elaborate about TELNET and its working procedure. **(AKTU 2017-18)**

Solution:

TELNET (short for TErminal NETwork) is a veteran networking protocol used to establish a bidirectional, interactive text-oriented communication channel between two computers. It allows a user on a local "client" machine to log into and control a "server" machine remotely as if they were physically present at that system's console.

Working procedure of TELNET:

1. Client-Server Interaction

- The Telnet client initiates the connection by sending requests to the Telnet server.
- Once the connection is established, the client can send commands to the server.
- The server processes these commands and responds accordingly.

2. Character Flow

- When the user types on the local computer, the local operating system accepts the characters.
- The Telnet client transforms these characters into a universal character set called Network Virtual Terminal (NVT) characters.
- These NVT characters travel through the Internet to the remote computer via the local TCP/IP protocol stack.
- The remote Telnet server converts these characters into a format understandable by the remote computer.
- The remote operating system receives the characters from a pseudo-terminal driver and passes them to the appropriate application program

3. Network Virtual Terminal (NVT)

- NVT is a virtual terminal in Telnet that provides a common structure shared by different types of real terminals.
- It ensures communication compatibility between various terminals with different operating systems.

Q5. Explain public key cryptography. List its advantages and disadvantages. Explain the working of RSA algorithm with suitable example. **(AKTU 2024-25)**

Solution:

Public key cryptography, also known as asymmetric cryptography, is a secure communication method that uses a pair of mathematically linked keys: a public key for encryption and a private key for decryption.

Public key cryptography (asymmetric cryptography) is a cryptographic system that uses pairs of keys: a public key for encryption (shared) and a private key for decryption (kept secret). This system ensures secure communication over public networks by removing the need for parties to share secret keys, allowing for confidentiality, integrity, and digital authentication.

Advantages:

- **Secure Key Exchange:** Solves the key distribution problem of symmetric encryption, as the private key is never transmitted or revealed.
- **Digital Signatures & Authentication:** Enables verification of the sender's identity and confirms the message was not altered in transit.
- **Non-repudiation:** Ensures that the sender cannot deny sending the message, as only their private key could have created the signature.
- **Scalability:** Fewer keys are needed compared to symmetric encryption for secure communication between multiple parties.

Disadvantages:

- **Speed:** It is generally much slower than symmetric encryption, making it inefficient for encrypting large amounts of data.
- **Computational Overhead:** Requires significant processing power, which can impact performance on devices with limited resources.
- **Vulnerability to Key Mismanagement:** If the private key is stolen, all security is lost, and the system relies entirely on user protection of that key.
- **Certificate Reliance:** Usually requires a Public Key Infrastructure (PKI) and trusted certification authorities to verify public keys.

Common algorithms for this type of encryption include **RSA** (Rivest–Shamir–Adleman)

Working of RSA Algorithm

The RSA (Rivest-Shamir-Adleman) algorithm's security is based on the difficulty of factoring the product of two large prime numbers.

1. Key Generation

1. **Choose Primes:** Select two distinct large prime numbers, p and q.
2. **Compute Modulus (n):** $n = p \times q$.
3. **Compute Totient ($\phi(n)$):** $\phi(n) = (p-1) \times (q-1)$.
4. **Choose Public Exponent (e):** Select an integer e such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$.
5. **Compute Private Exponent (d):** Calculate d such that $(d \times e) \pmod{\phi(n)} = 1$.
    1. **Public Key:** (e, n)
    2. **Private Key:** (d, n)

2. Encryption and Decryption Formulas

- **Encryption:** $C = M^e \pmod{n}$, where M is the message and C is the ciphertext.
- **Decryption:** $M = C^d \pmod{n}$.

Using small numbers for demonstration:

1. **Step 1:** Choose $p = 3$ and $q = 11$.
2. **Step 2:** $n = 3 \times 11 = 33$.
3. **Step 3:** $\phi(n) = (3-1) \times (11-1) = 2 \times 10 = 20$.
4. **Step 4:** Choose $e = 7$ (since 7 and 20 are coprime).
5. **Step 5:** Find d such that $(d \times 7) \pmod{20} = 1$. Here, $d = 3$ because $21 \pmod{20} = 1$.
6. **Encryption:** To send message $M = 2$:
   1. $C = 2^7 \pmod{33} = 128 \pmod{33} = 29$.
7. **Decryption:** To recover the message:
   1. $M = 29^3 \pmod{33} = 24389 \pmod{33} = 2$.

Q6. Differentiate between FTP and HTTP. **(AKTU 2023-24)**

Solution:

Difference between FTP and HTTP

HTTP	FTP
It stands for HyperText Transfer Protocol.	It stands for File Transfer Protocol
It is the set of rules that how web pages are transferred on different computers over the internet.	It is the set of rules that permit the downloading and uploading the files on the computer over the internet.
It only supports the data connection.	It supports both data connection and control connection
It uses Transmission Control Protocol and runs on TCP port 80.	It uses Transmission Control Protocol and runs on TCP port 20 and TCP port 21.
The URL using the HTTP protocol will start with HTTP.	The URL using the FTP will start with FTP.
It does not require authentication.	It requires authentication.
It is efficient in transferring small files.	It is efficient in transferring large files.
The files transferred to the computer over the internet are not saved to the memory.	The files transferred to the computer over the internet are saved to the memory.
HTTP is used to provide the web pages to the web browser from the webserver	FTP is used to upload or download files between client and server.
It is a stateless protocol.	It is not a stateless protocol and it maintains states.
It supports an In-band type of band transfer.	It supports an Out-of-band type of band transfer.
It can use both types of Persistent and Non-persistent TCP connection.	It uses a Persistent TCP connection for the Control connection and a Non-persistent TCP Connection for Data Connection.

It uses one way communication system.	It uses two way communication systems.
HTTP is faster.	FTP is slower as compared to HTTP.

Q7. Explain Data compression. How is TFTP different from FTP? **(AKTU 2018-19)**

Solution:

Data compression is the process of reducing the size of digital data by re-encoding information using fewer bits, removing redundancies, or eliminating unnecessary information.

Compression techniques are useful for reducing file sizes for storage, minimizing bandwidth during transmission and enabling faster uploading/downloading of web content over the internet.

Data compression can be divided into two categories: lossless and lossy.

Lossless Data Compression:

Lossless data compression guarantees that the decompressed data is identical to the original data. It works best for text and data files where precision matters.

- **Huffman coding:** Uses a frequency-sorted binary tree to locate values efficiently.
- **Run-length encoding (RLE):** This compresses sequences of replicated data values.
- **Lempel-Ziv-Welch (LZW):** It creates a dictionary of data patterns and replaces them with shorter codes.

Lossy Data Compression:

Lossy data compression gives away the accuracy of some of its input data for a better compression ratio. It is usually applied to multimedia files, where some loss of detail can be tolerated. Some techniques include:

- **Transform Coding:** Uses mathematical transforms that shrink the data, usually in JPEG
- **Quantization:** Reducing the precision of data; it is common in image and video compression.

FTP (File Transfer Protocol) is a secure, complex, and reliable protocol for transferring files over TCP (port 21) with user authentication. TFTP (Trivial File Transfer Protocol) is a basic, lightweight protocol using UDP (port 69) without authentication, best suited for local network device configuration updates.

Feature	FTP	TFTP
Purpose	Transfer files between computers	Transfer files between computers
Connection	Establishes a connection between two computers, allowing for a more complex set of commands and options	Establishes a connection between two computers, but with a more limited set of commands and options
Authentication	Uses username and password for authentication	Does not support authentication
Security	Encrypts data transfer	Does not encrypt data transfer
Error handling	Can recover from errors during transfer	Does not have error recovery
File transfer mode	Supports both ASCII and binary transfer modes	Only supports binary transfer mode
Transfer options	Supports resuming interrupted transfers and setting transfer mode, transfer type, and other options	Does not support any transfer options

Q8. Explain SNMP protocols and working scenario. **(AKTU 2023-24)**

Solution:

Simple Network Management Protocol (SNMP) is an application-layer protocol used to monitor, manage, and configure network devices (routers, switches, servers). It operates on UDP, utilizing ports 161 and 162 for communication between a central manager and device agents, primarily for performance tracking and proactive alerts.

Components of SNMP

- **SNMP Manager (Network Management Station - NMS):** A centralized system that requests data from devices and monitors network health.
- **SNMP Agent:** Software on managed network devices (routers, switches) that maintains a database of device information and communicates with the manager.

- **Management Information Base (MIB):** A hierarchical database defining the managed objects (variables) on the device, such as CPU usage or interface status.
- **Object Identifier (OID):** A unique identifier for specific objects within the MIB, allowing the manager to request particular data points

SNMP Working Scenario:

- **Polling (Monitoring):** The SNMP Manager sends a Get request to the SNMP Agent on a router via port 161.
- **Data Retrieval:** The Agent queries its local MIB database to find the requested OID value.
- **Response:** The Agent sends a Response back to the Manager with the data.
- **Trap Notification:** If the router's interface goes down, the Agent immediately sends an unsolicited Trap message to the Manager to notify it of the incident, using port 162.
- **Configuration:** If necessary, the administrator uses the manager to send a Set request to change a setting on the device.

Q9. What is MIME? Explain. **(AKTU 2003-04)**

Solution:

MIME (Multipurpose Internet Mail Extensions) is a standard designed to extend the format of email messages, allowing them to include more than just plain text. It enables the transmission of multimedia content such as images, audio, video and attachments, as well as other types of content, across email systems that traditionally only supported plain ASCII text.

- MIME allows email messages to carry diverse types of data by encoding them into a format that can safely travel over protocols like SMTP (Simple Mail Transfer Protocol) without data loss or corruption.
- It also provides metadata to help the receiving client identify and process the content correctly

MIME Structure:

A typical MIME email contains several key components:

- **MIME-Version:** Specifies the MIME version used (commonly 1.0).
- **Content-Type:** Indicates the type of content, such as text/plain, text/html, image/jpeg or audio/mpeg.
- **Content-Transfer-Encoding:** Shows how content is encoded for safe transmission (e.g., base64, quoted-printable).
- **Content-ID:** Provides a unique identifier for referencing embedded objects like inline images.
- **Content-Description:** Offers a short description of the content (e.g., "PDF Document" or "Image File").

Q10. How does FTP work? Differentiate between passive and active FTP. **(AKTU 2016-17)**

Solution:

FTP (File Transfer Protocol) transfers files between a client and server using two separate channels: a command channel (Port 21) for commands and a data channel for file transfers.

FTP works by establishing two parallel connections:

- **Control Channel (Port 21):** Used for logging in, sending commands (e.g., LIST, GET), and receiving server responses.
- **Data Channel:** Used only for transferring file contents or directory listings.

Differences Between Active and Passive FTP:

Feature	Active FTP	Passive FTP (PASV)
Data Initiation	Server initiates data connection	Client initiates data connection
Firewall Status	Issues with client-side firewalls	Friendly to firewalls
Connection Flow	Client sends PORT command to server	Client sends PASV command to server
Common Use Case	Internal networks, trusted environments	Default mode for internet browsers & servers

Q11. Mention the use of HTTP. **(AKTU 2017-18)**

Solution:

HTTP (Hypertext Transfer Protocol) is the foundational application-layer protocol for the World Wide Web, designed to enable communication between web browsers (clients) and web servers. It uses a request-response model to transfer data, including HTML documents, images, videos, and scripts.

Uses of HTTP:

- **Web Browsing and Data Transfer:** When you enter a URL or click a link, your browser sends an HTTP request to a server to load web pages, images, and other multimedia content.
- **Submitting User Data:** HTTP is used to send data from a client to a server, such as filling out online forms, submitting login credentials, or uploading files, typically via the POST or PUT methods.
- **Web APIs (RESTful Services):** HTTP serves as the underlying protocol for modern application programming interfaces (APIs), enabling applications to communicate and exchange data, often in JSON or XML format.
- **Caching and Optimization:** HTTP headers control how web resources are stored (cached) in browsers or proxy servers to improve performance and reduce network traffic.
- **Session Management:** Through the use of cookies, HTTP enables stateful sessions (e.g., keeping a user logged in, managing online shopping carts) despite being fundamentally a stateless protocol.
- **Content Negotiation:** HTTP allows a client and server to negotiate the best format or language for content, ensuring the correct data is returned based on user preferences.
- **Resource Manipulation:** HTTP supports various methods like GET (retrieve), POST (create), PUT (update), and DELETE (remove) to manage resources on a server.