

UNIT – V

APPLICATION LAYER

1. What is the purpose of Domain Name System?

Domain Name System can map a name to an address and conversely an address to name.

2. Discuss the three main division of the domain name space.

Domain name space is divided into three different sections: generic domains, country domains & inverse domain.

Generic domain: Define registered hosts according to their generic behavior, uses generic suffixes.

Country domain: Uses two characters to identify a country as the last suffix. Inverse

domain: Finds the domain name given the IP address.

3. Discuss the TCP connections needed in FTP.

FTP establishes two connections between the hosts. One connection is used for data transfer, the other for control information. The control connection uses very simple rules of communication. The data connection needs more complex rules due to the variety of data types transferred.

4. Discuss the basic model of FTP.

The client has three components: the user interface, the client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.

5. What is the function of SMTP?

The TCP/IP protocol supports electronic mail on the Internet is called Simple Mail Transfer (SMTP). It is a system for sending messages to other computer users based on e-mail addresses. SMTP provides mail exchange between users on the same or different computers.

6. What is the difference between a user agent (UA) and a mail transfer agent (MTA)?

The UA prepares the message, creates the envelope, and puts the message in the envelope. The MTA transfers the mail across the Internet.

7. How does MIME enhance SMTP?

MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers it to the client SMTP to be sent through the Internet. The server SMTP at the receiving side

receives the NVT ASCII data and delivers it to MIME to be transform feed back to the original data.

8. Why is an application such as POP needed for electronic messaging

Workstations interact with the SMTP host, which receives the mail on behalf of every host in the organization, to retrieve messages by using a client-server protocol such as Post Office Protocol, version 3(POP3). Although POP3 is used to download messages from the server, the SMTP client still needed on the desktop to forward messages from the workstation user to its SMTP mail server.

9. Write down the three types of WWW documents.

The documents in the WWW can be grouped into three broad categories: static, dynamic and active.

Static: Fixed-content documents that are created and stored in a server. Dynamic: Created by web server whenever a browser requests the document. Active: A program to be run at the client side.

10. What is the purpose of HTML?

HTML is a computer language for specifying the contents and format of a web document. It allows additional text to include codes that define fonts, layouts, embedded graphics and hypertext links.

11. Define CGI.

CGI is a standard for communication between HTTP servers and executable programs. It is used in crating dynamic documents.

12. Name four factors needed for a secure network.

Privacy: The sender and the receiver expect confidentiality.

Authentication: The receiver is sure of the sender's identity and that an imposter has not sent the message.

Integrity: The data must arrive at the receiver exactly as it was sent. Non-Reputation: The receiver must able to prove that a received message came from a specific sender.

13. How is a secret key different from public key?

In secret key, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

In public key, there are two keys: a private key and a public key. The private key is kept

by the receiver. The public key is announced to the public.

14. What is a digital signature?

Digital signature is a method to authenticate the sender of a message. It is similar to that of signing transactions documents when you do business with a bank. In network transactions, you can create an equivalent of an electronic or digital signature by the way you send data.

15. What are the advantages & disadvantages of public key encryption?

Advantages:

- a) Remove the restriction of a shared secret key between two entities. Here each entity can create a pair of keys, keep the private one, and publicly distribute the other one.
- b) The no. of keys needed is reduced tremendously. For one million users to communicate, only two million keys are needed.

Disadvantages:

If you use large numbers the method to be effective. Calculating the cipher text using the long keys takes a lot of time. So it is not recommended for large amounts of text.

16. What are the advantages & disadvantages of secret key encryption?

Advantages:

Secret Key algorithms are efficient: it takes less time to encrypt a message. The reason is that the key is usually smaller. So it is used to encrypt or decrypt long messages.

Disadvantages:

- a) Each pair of users must have a secret key. If N people in world want to use this method, there needs to be $N(N-1)/2$ secret keys. For one million people to communicate, a half-billion secret keys are needed.
- b) The distribution of the keys between two parties can be difficult.

17. Define permutation.

Permutation is transposition in bit level.

Straight permutation: The no. of bits in the input and output are preserved. Compressed

permutation: The no. of bits is reduced (some of the bits are dropped). Expanded

permutation: The no. of bits is increased (some bits are repeated).

18. Define substitutional & transpositional encryption.

Substitutional: A character level encryption in which each character is replaced by another character in the set.

Transpositional: A Character level encryption in which the characters retain their plaintext but the position of the character changes.

16 Marks

1. Explain how security is provided in interact operations in detail.
2. What is HTTP protocol used for? What is the default port number of HTTP protocol?
3. Discuss the features of HTTP and also discuss how HTTP works.
4. List and discuss the types of DNS records.
5. Explain WWW.
6. What are the duties of FTP protocol?
7. Explain the type of encryption/decryption method.
8. Explain about RSA algorithm