APPLICATION LAYER

Multiple Choice Type Questions

1. Which one is not an application layer protocol? [WBUT 2014]
   a) SMTP b) telnet c) TCP d) DNS

Answer: (c)

2. If user *A* want to send a message to user *B* confidentially, the plain text is encrypted with the public key of [WBUT 2015]
   a) *A* b) *B* c) the network d) either (a) or (b)

Answer: (b)

3. File transfer is done by [WBUT 2016]
   a) Physical layer b) DLL
   c) Application layer d) Network layer

Answer: (c)

4. Encryption can be done in [WBUT 2016]
   a) presentation layer b) data link layer
   c) network layer d) none of these

Answer: (a)

5. An interconnected collection of piconet is called _____. [WBUT 2018]
   a) Scatternet b) Micronet c) Mininet d) None of these

Answer: (a)

6. E-mail cannot be sent [MODEL QUESTION]
   a) if the sending site does not use TCP/IP
   b) if the receiving site does not use TCP/IP
   c) through private networks
   d) none of these

Answer: (d)

Short Answer Type Questions

1. What is firewall? How does firewall rule chain work? [WBUT 2013]

Answer:

1st Part:

Firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages

entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

2nd Part:

The firewall operates by means of firewall rules. Each rule consists of two parts - the matcher which matches traffic flow against given conditions and the action which defines what to do with the matched packet.

Firewall filtering rules are grouped together in chains. It allows a packet to be matched against one common criterion in one chain, and then passed over for processing against some other common criteria to another chain. For example a packet should be matched against the IP address: port pair. Of course, it could be achieved by adding as many rules with IP address: port match as required to the forward chain, but a better way could be to add one rule that matches traffic from a particular IP address, e.g.:/ip firewall filter add src-address=1.1.1.2/32 jump-target="mychain" and in case of successful match passes control over the IP packet to some other chain, id est mychain in this example. Then rules that perform matching against separate ports can be added to mychain chain without specifying the IP addresses.

There are three predefined chains, which cannot be deleted:

- **input** - used to process packets entering the router through one of the interfaces with the destination IP address which is one of the router's addresses. Packets passing through the router are not processed against the rules of the input chain
- **forward** - used to process packets passing through the router
- **output** - used to process packets originated from the router and leaving it through one of the interfaces. Packets passing through the router are not processed against the rules of the output chain

2. What is packet filter firewall? Why is it needed? **[WBUT 2013]**

Answer:

In the Internet, packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. The process is used in conjunction with packet mangling and Network Address Translation (NAT).

Packet filtering is often part of a firewall program for protecting a local network from unwanted intrusion. In a software firewall, packet filtering is done by a program called a packet filter.

3. What is SMTP? **[WBUT 2014, 2015]**

Answer:

SMTP is part of the application layer of the TCP/IP protocol. Using a process called "store and forward," SMTP moves our email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox.

4. Why DNS is required? **[WBUT 2014]**

OR,

Explain Domain Name System. **[WBUT 2018]**

Answer:

Without a Name Service there would simply not be a viable Internet. To understand why we need to look at what DNS does and how and why it evolved.

A DNS translates (or maps) the name of a resource to its physical IP address - typically referred to as forward mapping.

A DNS can also translate the physical IP address to the name of a resource - typically called reverse mapping.

Remember that the Internet (or any network for that matter) works by allocating every point (host, server, router, interface etc.) a physical IP address (which may be locally unique or globally unique).

Without DNS every host (PC) which wanted to access a resource on the network (Internet), say a simple web page e.g. www.thing.com, would need to know its physical IP address. With 100 of millions of hosts and billions of web pages it is an impossible task - it's also pretty impossible with just a handful of hosts and resources.

5. What do you mean by Cryptography? Explain it briefly. **[WBUT 2017]**

Answer:

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.

Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1) Confidentiality (the information cannot be understood by anyone for whom it was unintended)
2) Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4) Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

6. What do you mean by Private key and Public key Cryptography? Why is it used? **[MODEL QUESTION]**

Answer:

Public key encryption is considered very secure because it does not require a secret shared key between the sender and receiver. Other encryption technologies that use a single shared key to both encrypt and decrypt data rely on both parties deciding on a key ahead of time without other parties finding out what that key is. However, the fact that it must be shared between both parties opens the door to third parties intercepting the key. This type of encryption technology is called symmetric encryption, while public key encryption is known as asymmetric encryption.

Symmetric encryption (also called private-key encryption or secret-key encryption) involves using the same key for encryption and decryption.

Encryption involves applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible. The slightest algorithm (such as an exclusive OR) can make the system nearly tamper proof (there being so such thing as absolute security).

The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. Symmetric encryption is based on the exchange of a secret (keys). The problem of key distribution therefore arises:

Moreover, a user wanting to communicate with several people while ensuring separate confidentiality levels has to use as many private keys as there are people. For a group of N people using a secret-key cryptosystem, it is necessary to distribute a number of keys equal to N * (N-1) / 2.

Long Answer Type Questions

1. a) What is advantage of asymmetric key algorithm over symmetric key algorithm? **[WBUT 2014]**

Answer:

Advantages of asymmetric key algorithm

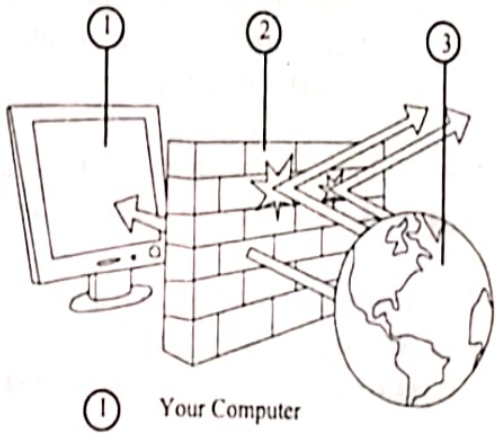
- In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.
- The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.
- Can provide digital signatures that can be repudiated

b) What is firewall? How does a firewall resolve the security issues? **[WBUT 2014]**

Answer:

1st Part: ***Refer to Question No. 1(1st Part) of Short Answer Type Questions.***

2nd Part:



① Your Computer

② Your firewall

③ Your Internet

At their most basic, firewalls work like a filter between our computer/network and the Internet. We can program what we want to get out and what we want to get in. Everything else is not allowed. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several different methods firewalls use to filter out information, and some are used in combination. These methods work at different layers of a network, which determines how specific the filtering options can be.

2. a) What is cryptography? Explain Public and Private Key cryptography with example. **[WBUT 2015]**

Answer:

1st Part:

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.

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit.

2nd Part:

Public key encryption is considered very secure because it does not require a secret shared key between the sender and receiver. Other encryption technologies that use a single shared key to both encrypt and decrypt data rely on both parties deciding on a key ahead of time without other parties finding out what that key is. However, the fact that it must be shared between both parties opens the door to third parties intercepting the key. This type of encryption technology is called symmetric encryption, while public key encryption is known as asymmetric encryption.

Symmetric encryption (also called private-key encryption or secret-key encryption) involves using the same key for encryption and decryption.

Encryption involves applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible. The slightest algorithm (such as an exclusive OR) can make the system nearly tamper proof (there being no such thing as absolute security).

The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. Symmetric encryption is based on the exchange of a secret (keys). The problem of key distribution therefore arises:

Moreover, a user wanting to communicate with several people while ensuring separate confidentiality levels has to use as many private keys as there are people. For a group of N people using a secret-key cryptosystem, it is necessary to distribute a number of keys equal to N * (N-1) / 2.

For example, if Bob wants to send sensitive data to Alice, and wants to be sure that only Alice may be able to read it, he will encrypt the data with Alice's Public Key. Only Alice has access to her corresponding Private Key and as a result is the only person with the capability of decrypting the encrypted data back into its original form.

As only Alice has access to her Private Key, it is possible that only Alice can decrypt the encrypted data. Even if someone else gains access to the encrypted data, it will remain confidential as they should not have access to Alice's Private Key.

Public Key Cryptography can therefore achieve Confidentiality. However another important aspect of Public Key Cryptography is its ability to create a Digital Signature.

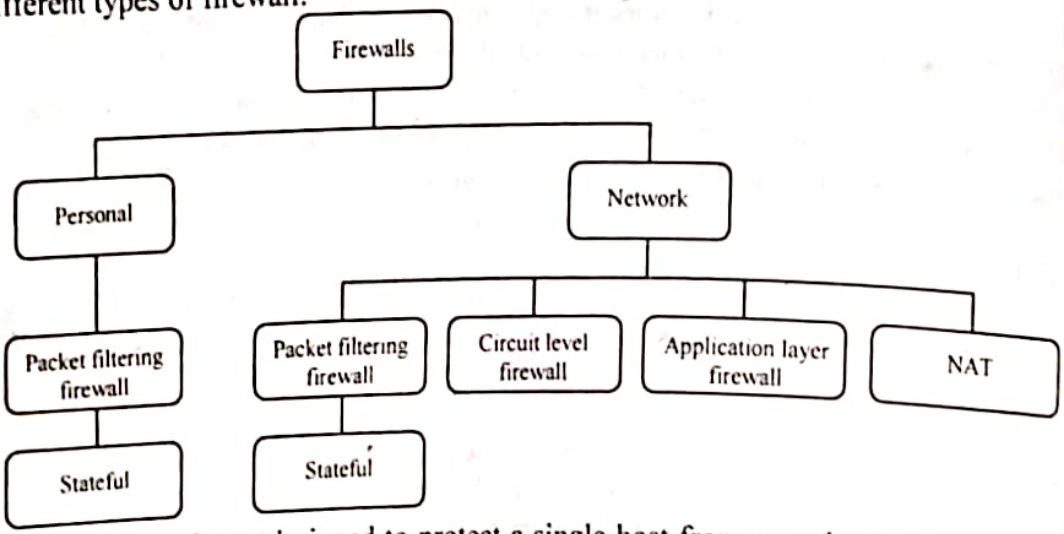
b) What is Firewall? Describe with examples different types of firewalls. Explain digital signature. **[WBUT 2015]**

Answer:

1st Part: ***Refer to Question No. 1(1st Part) of Short Answer Type Questions.***

2nd Part:

Different types of firewall:



Personal firewalls are designed to protect a single host from unauthorised access. They can take the form of software or hardware.

Network firewalls protect the whole network from unauthorised access. They can be a dedicated appliance (hardware) which is installed on the system or a software application or an integration of the two.

Software firewall applications are installed on top of the operating system and can be configured for more than one purpose including spam filter and DNS server. Examples of personal software firewalls include ZoneAlarm and Comodo; network capable software firewalls include Linus IPTables and Checkpoint NG.

Hardware Firewalls are dedicated appliances that physically sit between two networks; for example, the internet and the organisation's network. An example of a dedicated appliance could be the CISCO PIX or a Netgear router (for SO/HO).

Packet Filtering Firewall analyse network traffic at the transport layer. It will look at each packet entering or leaving the network and accepts or rejects it based on user defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Packet filters typically enable us to permit or deny the data flow based on the following controls:

- Source of the packet (IP address)
- Destination of the packet (IP address)
- Type of transport layer (TCP, UDP)
- Transport layer source port
- Transport layer destination port

Circuit Level Gateway operate at the session layer of the OSI model examining each connection to ensure that it follows a legitimate 'handshake' for the transport layer protocol being used (usually TCP). This is depends on TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Application Level Firewalls or Proxy Firewalls work at the application layer of the OSI model by forcing both sides of communication through the proxy. It applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation. The proxy servers are effectively hides the true network addresses.

Network Address Translation is a functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defence against network reconnaissance.

3rd Part:

A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be

imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

Digital signatures are created and verified by cryptography. A fundamental process known as the hash function is used to both create and verify the digital signatures. A hash function is an algorithm which creates a digital representation or "fingerprint" in the form of a hash value or hash result which is of standard length. This finger print is also known as the message digest. This fingerprint is smaller than the message but is substantially unique to the message. As a result, any change to this message, produces a different result, even when the same hash function is used. So hash functions are used to create digital signatures.

3. a) Explain RSA Algorithm in detail with numeric. Give example. **[WBUT 2018]**
b) What is firewall?
c) How does firewall resolves the security issue?
d) What is digital signature?

Answer:

a) RSA Algorithm:

In cryptography, RSA is an algorithm for public-key encryption. The algorithm was described in 1977 by Ron Rivest, Adi Shamir and Len Adleman at MIT; the letters RSA are the initials of their surnames. RSA involves two keys: public key and private key. The public key is known to everyone and is used to encrypt messages.

The following are steps to generate a public key and a private key:

Choose two large prime numbers p and q such that $p \neq q$, randomly and independently of each other.

Compute $n = pq$.

Compute $\phi(n) = (p-1)(q-1)$.

Choose an integer e such that $1 < e < \phi(n)$ which is coprime to $\phi(n)$

Compute d such that $de \equiv 1 \pmod{\phi(n)}$.

Encrypting messages

Suppose Bob wishes to send a message M to Alice. He turns M into a number $m < n$, using some previously agreed-upon reversible protocol. Bob now has m, and knows n and e, which Alice has announced. He then computes the ciphertext c corresponding to m:

$c = m^e \mod n$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

Decrypting messages

Alice receives c from Bob, and knows her private key d. She can recover m from c by the following procedure: $m = c^d \pmod{n}$

Given m, she can recover the original message M. The decryption procedure works because $c^d \equiv \left(m^e\right)^d \equiv m^{ed} \pmod{n}$.

Now, since $ed \equiv 1 \pmod{p\text{-}1}$ and $ed \equiv 1 \pmod{q\text{-}1}$, Fermat's little theorem yields

$m^{ed} \equiv m \pmod{p}$ and $m^{ed} \equiv m \pmod{q}$

Since p and q are distinct prime numbers, applying the Chinese remainder theorem to these two congruences yields

$m^{ed} \equiv m \pmod{pq}$

Thus, $c^d \equiv m \pmod{n}$.

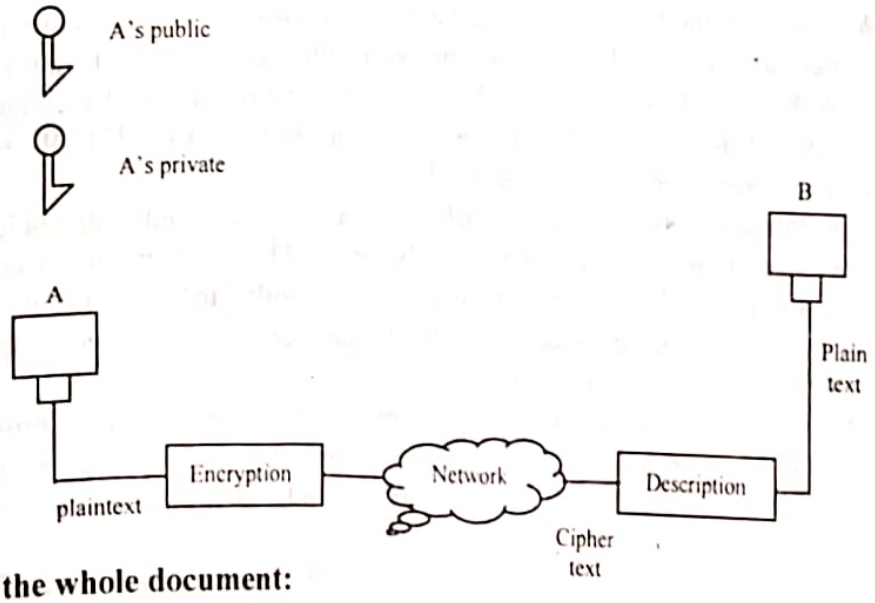
b) & c) ***Refer to Question No. 1(b) of Long Answer Type Questions.***

d) Digital signature:

A digital signature is a mathematical technique used to validate the authenticity and integrity of a massage, software or digital document. In Networking, there are four aspect of massage security:

i) Privacy
ii) Authentication
iii) Integrity
iv) Non-repudiation

The basic idea in digital signature is to sign a document. When we send a document electronically, we can also sign it. We can sign a document in two ways – to sign a document or to sign a digest.



Signing the whole document:

In digital signature, a public key encryption technique is used to sign a document. The sender uses a private key to encrypt the massage while the receiver uses the public key of the sender to decrypt the massage. Digital signature cannot be archived by using secret key encryption.

4. Write short notes on the following:

a) CHAP [WBUT 2014]
b) HTTP [WBUT 2014]
c) FTP [WBUT 2015]
d) DNS [WBUT 2015]

Answer:

a) CHAP:

CHAP (Challenge-Handshake Authentication Protocol) is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP). Here's how CHAP works:

1. After the link is made, the server sends a challenge message to the connection requestor. The requestor responds with a value obtained by using a one-way hash function.
2. The server checks the response by comparing it its own calculation of the expected hash value.
3. If the values match, the authentication is acknowledged; otherwise the connection is usually terminated.

At any time, the server can request the connected party to send a new challenge message. Because CHAP identifiers are changed frequently and because authentication can be requested by the server at any time, CHAP provides more security than PAP. RFC1334 defines both CHAP and PAP.

b) HTTP:

Short for HyperText Transfer Protocol, HTTP is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when we enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript and cookies.

Errors on the Internet can be quite frustrating — especially if we do not know the difference between a 404 error and a 502 error. These error messages, also called HTTP status codes are response codes given by Web servers and help identify the cause of the problem.

For example, "404 File Not Found" is a common HTTP status code. It means the Web server cannot find the file you requested. The file -- the webpage or other document we try to load in our Web browser -- has either been moved or deleted, or you entered the wrong URL or document name.

e) FTP:

FTP or **File Transfer Protocol** is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. There are two computers involved in an FTP transfer — a server and a client. The **FTP server**, running FTP server software, listens on the network for connection requests from other computers. The client computer, running FTP client software, initiates a connection to the server. Once connected, the client can do a number of file manipulation operations such as uploading files to the server, download files from the server, rename or delete files on the server and so on. Any computer connected to a TCP/IP based network can manipulate files on another computer on that network regardless of which operating systems are involved (if the computers permit FTP access). There are many existing FTP client and server programs, and many of these are free.

FTP is commonly run on two ports, 20 and 21, and runs exclusively over TCP. The FTP server listens on port 21 for incoming connection from FTP clients. A connection on this port forms the control stream, on which commands are passed to the FTP server. For the actual file transfer to take place, a different connection is required. Depending on the transfer mode, the client (active mode) or the server (passive mode) can listen for the incoming data connection. Before file transfer begins, the client and server also negotiate the port of the data connection. In case of active connections (where the server connects to the client to transfer data), the server binds on port 20 before connecting to the client. For passive connections, there is no such restriction.

While data is being transferred via the data stream, the control stream sits idle. This can cause problems with large data transfers through firewalls which time out sessions after lengthy periods of idleness. While the file may well be successfully transferred, the control session can be disconnected by the firewall, causing an error to be generated.

Many sites that run FTP servers enable so-called "anonymous ftp". Under this arrangement, users do not need an account on the server. The user name for anonymous access is typically 'anonymous' or 'ftp'. This account does not need a password. Although users are commonly asked to send their email addresses as their passwords for authentication, usually there is trivial or no verification.

While transferring data over the network, two modes can be used

- ASCII mode
- Binary mode

The two types differ in the way they send the data. When a file is sent using an ASCII-type transfer, the individual letters, numbers and characters are sent using their ASCII character codes. The receiving machine saves these in a text file in the appropriate format (for example, a Unix machine saves it in a Unix format, a Macintosh saves it in a Mac format). Hence if an ASCII transfer is used it can be assumed plain text is sent, which is stored by the receiving computer in its own format.

Sending a file in binary mode is different. The sending machine sends each file bit for bit and as such the recipient stores the bitstream as it receives it.

By default, most FTP clients use ASCII mode. Some clients try to determine the required transfer-mode by inspecting the file's name or contents.

d) DNS:

The **Domain Name System** or **Domain Name Server (DNS)** is a system that stores information associated with **domain names** in a distributed database on networks, such as the Internet. DNS associates many types of information with domain names, but most importantly, it provides the IP address associated with the domain name. DNS is an essential component of contemporary Internet use.

DNS is useful for several reasons. Most well known, the DNS makes it possible to attach hard-to-remember IP addresses (such as 207.142.131.206) to easy-to-remember domain names (such as "microsoft.com") Humans take advantage of this when they recite URLs and e-mail addresses. Less recognized, the domain name system makes it possible for people to assign authoritative names, without needing to communicate with a central registrar each time.

Domain names are arranged in a tree, and cut into zones, which are served by **nameservers**.

The domain name space is a tree of domain names. Each node or leaf in the tree is associated with **resource records**, which hold the information associated with the domain name. The tree is divided into **zones**. A zone is a collection of connected nodes that are authoritatively served by an **authoritative DNS nameserver**. A single nameserver can host several zones.

A domain name usually consists of two or more parts (technically *labels*), separated by dots. For example *microsoft.com*.

The rightmost label conveys the **top-level domain** (for example, the address *mail.yahoo.com* has the top-level domain *com*).

Each label to the left specifies a subdivision or **subdomain** of the domain above it. Note that "subdomain" expresses relative dependence, not absolute dependence. For example, *yahoo.com* comprises a subdomain of the domain, *com* and *mail.yahoo.com* is a subdomain of the domain *yahoo.com*. In theory, this subdivision can go down to 127 levels deep, and each label can contain up to 63 characters, as long as the whole domain name does not exceed a total length of 255 characters. But in practice some domain registries have shorter limits than that.

A domain name that has one or more associated IP addresses is called a **hostname**. For example, the *yahoo.com* and *mail.yahoo.com* domains are both hostnames, but the *com* domain is not.

5. a) Explain the SMTP in brief. **[MODEL QUESTION]**

b) What do you understand by data security? Explain the various aspects of security with the help of public and private key.

Answer:

a) *SMTP*

SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred. SMTP uses TCP port 25. SMTP started becoming widely used in the early 1980s and gradually replaced UUCP which was better suited to handle e-mail transfers

between Unix machines that were intermittently connected. SMTP works best when both the sending and receiving machines are connected to the network all the time.
Sendmail was one of the first (if not the first) mail transfer agents to implement SMTP. Today, there are several programs that implement SMTP as a client or a server, for example, *exim, Postfix, qmail*, and *Microsoft Exchange Server*.
This protocol started out as purely ASCII and did not deal well with binary files. Later, standards such as MIME were developed to encode binary files for transfer through SMTP.
SMTP is a "**push**" protocol that does not allow one to "**pull**" messages from a remote server on demand. To do this a mail client must use **POP3** or **IMAP**.

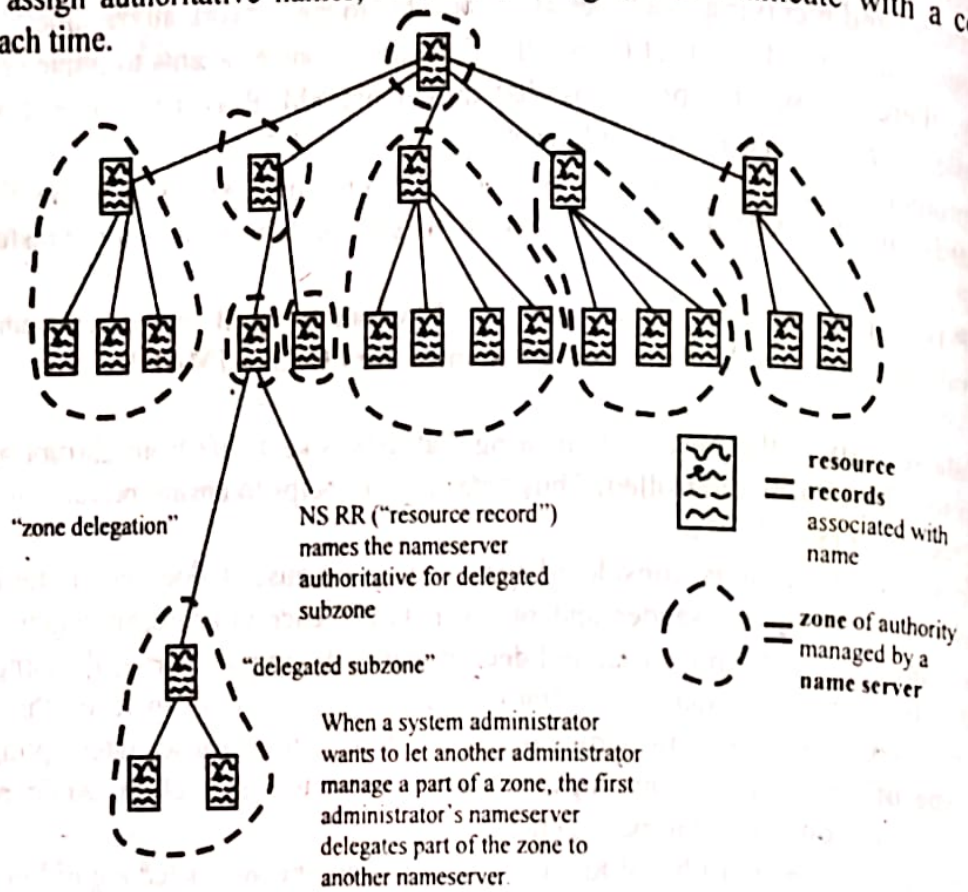
b) Data security is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data.
Public key encryption is considered very secure because it does not require a secret shared key between the sender and receiver. Other encryption technologies that use a single shared key to both encrypt and decrypt data rely on both parties deciding on a key ahead of time without other parties finding out what that key is. However, the fact that it must be shared between both parties opens the door to third parties intercepting the key. This type of encryption technology is called symmetric encryption, while public key encryption is known as asymmetric encryption.
A "key" is simply a small bit of text code that triggers the associated algorithm to encode or decode text. In public key encryption, a key pair is generated using an encryption program and the pair is associated with a name or email address. The public key can then be made public by posting it to a key server, a computer that hosts a database of public keys. Alternately, the public key can be discriminately shared by emailing it to friends and associates. Those that possess your public key can use it to encrypt messages to you. Upon receiving the encrypted message, your private key will decrypt it.
Secret-key encryption uses one key, the secret key, that is used to both encrypt and decrypt messages. This is also called symmetric encryption. The term "private key" is often used inappropriately to refer to the secret key.

6. What is DNS? How is it implemented? **[MODEL QUESTION]**

Answer:

The Domain Name System or Domain Name Server (DNS) is a system that stores information associated with domain names in a distributed database on networks, such as the Internet. DNS associates many types of information with domain names, but most importantly, it provides the IP address associated with the domain name. DNS is an essential component of contemporary Internet use.
DNS is useful for several reasons. Most well known, the DNS makes it possible to attach hard-to-remember IP addresses (such as 207.142.131.206) to easy-to-remember domain names (such as "microsoft.com") Humans take advantage of this when they recite URLs and e-mail addresses. Less recognized, the domain name system makes it possible for

people to assign authoritative names, without needing to communicate with a central registrar each time.



Domain names are arranged in a tree, and cut into zones, which are served by **nameservers.**

The domain name space is a tree of domain names. Each node or leaf in the tree is associated with **resource records**, which hold the information associated with the domain name. The tree is divided into **zones**. A zone is a collection of connected nodes that are authoritatively served by an **authoritative DNS nameserver**. A single nameserver can host several zones.

The information associated with nodes is looked up by a **resolver**. A resolver knows how to communicate with name servers by sending DNS requests, and heeding DNS responses. Resolving usually entails **recursing** through several name servers to find the needed information.

Some resolvers are simple, and can only communicate with a single name server. These simple resolvers rely on a **recursing name server** to perform the work of finding information for it.

A domain name usually consists of two or more parts (technically *labels*), separated by dots. For example *microsoft.com*.

The rightmost label conveys the **top-level domain** (for example, the address mail.yahoo.com has the top-level domain *.org*).

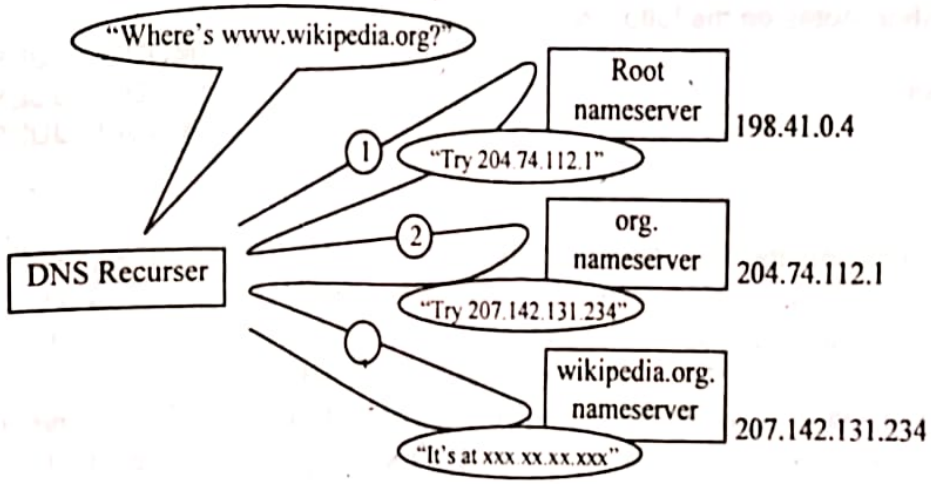
Each label to the left specifies a subdivision or **subdomain** of the domain above it. Note that "subdomain" expresses relative dependence, not absolute dependence. For example, yahoo.com comprises a subdomain of the domain, *com* and *mail.yahoo.com* is a subdomain of the domain *yahoo.com*. In theory, this subdivision can go down to 127

levels deep, and each label can contain up to 63 characters, as long as the whole domain name does not exceed a total length of 255 characters. But in practice some domain registries have shorter limits than that.

A domain name that has one or more associated IP addresses is called a **hostname**. For example, the *yahoo.com* and *mail.yahoo.com* domains are both hostnames, but the com domain is not.

The DNS consists of a hierarchical set of **DNS servers**. Each domain or subdomain has one or more **authoritative DNS servers** that publish information about that domain and the name servers of any domains "beneath" it. The hierarchy of authoritative DNS servers matches the hierarchy of domains. At the top of the hierarchy stand the **root servers**: the servers to query when looking up (**resolving**) a top-level domain name.

An example of theoretical DNS recursion



Here, the DNS recurser consults three nameservers to resolve *www.wikipedia.org*.

7. a) State the threats that can arise in a data network. Also, explain the security requirements to be met due to the stated threats.

b) Explain 'public key encryption' system as a means of secure transfer of information over a network. **[MODEL QUESTION]**

Answer:

a) Unauthorized entry into any compartmented computer system.

Unauthorized searching/browsing through classified computer libraries.

Unauthorized modification, destruction, manipulation, or denial of access to information residing on a computer system.

Storing or processing classified information on any system not explicitly approved for classified processing.

Attempting to circumvent or defeat security or auditing systems, without prior authorization from the system administrator, other than as part of a legitimate system testing or security research.

Any other willful violation of rules for the secure operation of your computer network.

b) A cryptographic system that uses two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. For this reason, it is sometime called Diffie-Hellman encryption. It is also called asymmetric encryption because it uses two keys instead of one key (symmetric encryption).

8. Write short notes on the following:

a) POP **[MODEL QUESTION]**

b) Firewall **[MODEL QUESTION]**

c) VLAN **[MODEL QUESTION]**

Answer:

a) POP:

E-mail clients use the Post Office Protocol version 3 (POP3), an application-layer Internet standard protocol, to retrieve e-mail from a remote server over a TCP/IP connection. Nearly all subscribers to individual Internet service provider e-mail accounts access their e-mail with client software that uses POP3. POP3 has obsoleted the earlier versions of the POP protocol, POP (informally called POP1) and POP2. In contemporary usage, the less precise term POP almost always means POP3 in the context of e-mail protocols.

The design of POP3 and its predecessors supports end users with intermittent connections (such as dial-up connections), allowing these users to retrieve e-mail when connected and then to view and manipulate the retrieved messages without needing to stay connected. Although most clients have an option to leave mail on server, e-mail clients using POP3 generally connect, retrieve all messages, store them on the user's PC as new messages, delete them from the server, and then disconnect. Most e-mail clients support either POP3 or IMAP to retrieve messages. The fundamental difference between POP3 and IMAP is that POP3 offers access to a mail drop; the mail exists on the server until it is collected by the client. Even if the client leaves some or all messages on the server, the client's message store is considered authoritative. In contrast, IMAP4 offers access to the mail store; the client may store local copies of the messages, but these are considered to be a temporary cache; the server's store is authoritative.

Whether using POP3 or IMAP to retrieve messages, e-mail clients typically use the SMTP_Submit profile of the SMTP protocol to send messages. E-mail clients are commonly categorized as either POP or IMAP clients, but in both cases the clients also use SMTP.

MIME serves as the standard for attachments and non-ASCII text in e-mail. Although neither POP3 nor SMTP require MIME-formatted e-mail, essentially all Internet e-mail

comes MIME-formatted, so POP clients must also understand and use MIME. IMAP, by design, assumes MIME-formatted e-mail.

POP3 works over a TCP/IP connection using TCP on network port 110. E-mail clients can encrypt POP3 traffic using TLS or SSL. A TLS or SSL connection is negotiated using the STLS command. Some clients and servers instead use the deprecated alternate-port method, which uses TCP port 995.

b) Firewall:

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

c) VLAN:

Virtual LAN (VLAN) refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization.

There are the following types of Virtual LANs:

Port-Based VLAN: each physical switch port is configured with an access list specifying membership in a set of VLANs.

MAC-based VLAN: a switch is configured with an access list mapping individual MAC addresses to VLAN membership.

Protocol-based VLAN: a switch is configured with a list of mapping layer 3 protocol types to VLAN membership - thereby filtering IP traffic from nearby end-stations using a particular protocol such as IPX.

ATM VLAN - using LAN Emulation (LANE) protocol to map Ethernet packets into ATM cells and deliver them to their destination by converting an Ethernet MAC address into an ATM address.