14EE506

1. Answer all questions (1X12=12 Marks)

a) Advantages of computer networks.

Ans: 1. People can share information freely. 2. It allows for frequent collaboration.

3. The cost of joining a computer network is going down.

b) Optimality principle.

Ans: The **optimality principle** states that if router J is on the **optimal** path from router I to router K, then the **optimal** path from J to K also falls along the same route.

c) Subnet.

Ans: A **subnet** is a logical partition of an IP network into multiple, smaller network segments. It is typically used to subdivide large networks into smaller, more efficient subnetworks.

d) List types of services provided by the transport entity.

Ans: 1. Connection oriented 2. Connection Less

e) Port

Ans: A **network port** is a process-specific or an application-specific software construct serving as a communication endpoint, which is used by the Transport Layer protocols of Internet Protocol suite

f) Socket

Ans: A network socket is an internal endpoint for sending or receiving data within a node on a computer network

g) Cookie

Ans: **Cookies** are a message given to a Web browser by a Web server.

h) SMTP

Ans: **SMTP** provides the ability to send and receive email messages. **SMTP** is an application-layer protocol that enables the transmission and delivery of email over the Internet.

i) Use of HTML

Ans: **Hypertext Markup Language** (HTML) is the standard **markup language** for creating web pages and web applications

j) Difference between System security and network security.

Ans: Network security is protecting your **network** infrastructure.

Computer **security** is protecting your **systems** infrastructure.

k) Cryptology

Ans: Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis

l) Use of PGP

Ans: Pretty Good Privacy (PGP) is an encryption program that provides **cryptographic** privacy and authentication for data communication. PGP is used for signing, encrypting, **decrypting** texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

UNIT I

2. a) Outline the Design issues of Network Layer. 6M

Ans:

- Store-and-Forward Packet Switching.
- Services Provided to the **Transport Layer**
- Implementation of Connectionless Service.
- Implementation of Connection-Oriented Service
- Comparison of Virtual-Circuit and Datagram Subnets. ---------→2M

----------→Explanation 4M

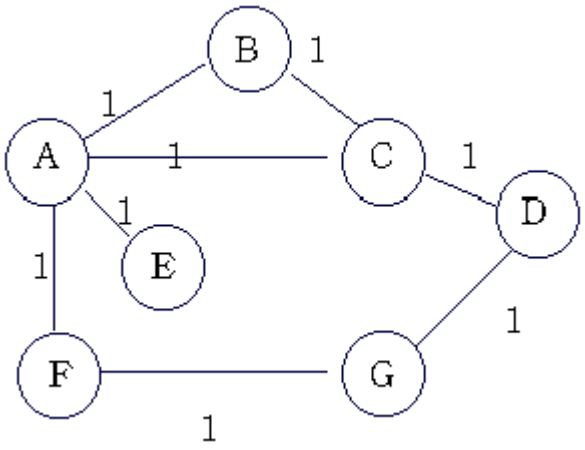
b) Illustrate distance vector routing algorithm with example.

Ans: Distance-Vector Routing

Each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbors.

1. The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors.
2. A link that is down is assigned an infinite cost. ----------→2M

Example.



Information Stored at Node	Distance to Reach Node A	B	C	D	E	F	G
A	0	1	1	□	1	1	?
B	1	0	1	□	□	□	□
C	1	1	0	1	□	□	□
D	□	□	1	0	□	□	1
E	1	□	?	□	0	□	□
F	1	□	□	□	□	0	1
G	□	□	□	1	□	1	0

Table 1. Initial distances stored at each node(global view).

We can represent each node's knowledge about the distances to all other nodes as a table like the one given in Table 1.

Note that each node only knows the information in one row of the table.

1. Every node sends a message to its directly connected neighbors containing its personal list of distance. (for example, **A** sends its information to its neighbors **B,C,E**, and **F**.)
2. If any of the recipients of the information from **A** find that **A** is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through **A**. (node **B** learns from **A** that node **E** can be reached at a cost of 1; **B** also knows it can reach **A** at a cost of 1, so it adds these to get the cost of reaching **E** by means of **A**. **B**records that it can reach **E** at a cost of 2 by going through **A**.)

3. After every node has exchanged a few updates with its directly connected neighbors, all nodes will know the least-cost path to all the other nodes.
4. In addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding table. (for example, **B** knows that it was **A** who said " I can reach **E** in one hop" and so **B** puts an entry in its table that says " To reach **E**, use the link to **A**.)

Information	**Distance to Reach Node**						
Stored at Node	**A**	**B**	**C**	**D**	**E**	**F**	**G**
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	0	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	0	3	2	1	3	1	0

Table 2. Final distances stored at each node

In practice, each node's forwarding table consists of a set of triples of the form:(Destination, Cost, NextHop).For example, Table 3 shows the complete routing table maintained at node B for the network in figure1.

Destination	**Cost**	**NextHop**
A	1	A
C	1	C
D	2	C
E	2	A
F	2	A
G	3	A

Table 3. Routing table maintained at node B. **--------→4M**

(OR)

3 a) What is meant by congestion control? Explain load shedding in brief.

Ans:

A state occurring in network layer when the message traffic is so heavy that it slows down network response time is called congestion control.
Effects of Congestion

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

Congestion control techniques:

- The leaky bucket algorithm
- The token bucket algorithm
- Admission Control
- Choke packets
- Weighted fair queuing
- Load shedding
- Resource reservation

------→3M

Load Shedding is a technique used in information systems, especially web services, to avoid overloading the system and making it unavailable for all users. The idea is to ignore *some requests* rather than crashing a system and making it fail to serve *any request*.

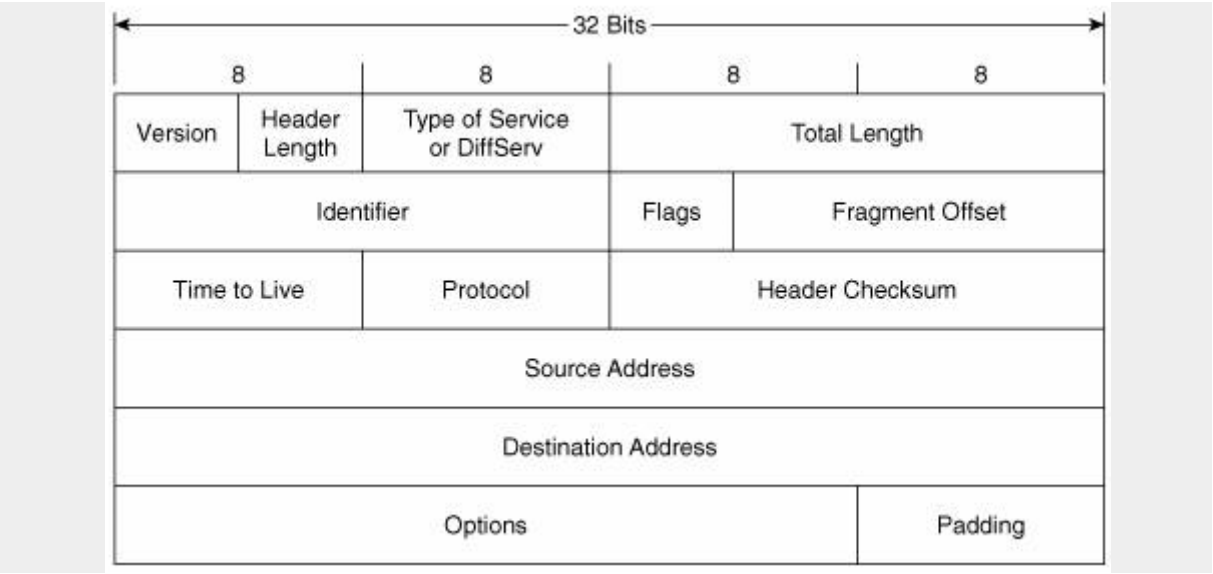
Considerations shaping the design of load shedding algorithms include:

- when one of several load balanced servers becomes unavailable due to overload, all other servers will receive a higher load, potentially leading to more overload and a snow-ball effect which takes down the entire system.
- when one part in a system of micro services starts becoming slower due to high load, other services will have waiting requests queuing up, potentially more than fits in their memory, which could again take down the entire system. -------→3M

3b) Outline IPV4 uses and its header format.

Ans: Diagram---3M Explanation ----3M

Internet Protocol version 4 (**IPv4**) is the fourth revision in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet IPv4 is a connectionless protocol for use on packet-switched Link Layer networks (e.g., Ethernet). It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol , such as the Transmission Control Protocol (TCP).



- Version: Version no. of Internet Protocol used (e.g. IPv4).
- IHL: Internet Header Length; Length of entire IP header.
- DSCP: Differentiated Services Code Point; this is Type of Service.
- ECN: Explicit Congestion Notification; It carries information about the congestion seen in the route.
- Total Length: Length of entire IP Packet (including IP header and IP Payload).
- Identification: If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
- Flags: As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- Fragment Offset: This offset tells the exact position of the fragment in the original IP Packet.
- Time to Live: To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- Protocol: Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- Header Checksum: This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- Source Address: 32-bit address of the Sender (or source) of the packet.
- Destination Address: 32-bit address of the Receiver (or destination) of the packet.

Unit-II

4 a) Write the elements that are involved in transport protocols to provide transport between 2 transport entities? Explain. 6M

Ans:

Elements of Transport Protocols:

- Addressing
- Connection Establishment
- Connection Release
- Flow Control and Buffering
- Multiplexing
- Crash Recovery ----------→2M

----------→Explanation 4M

b) Explain the procedure of connection establishment in TCP. 6M

Ans: TCP is a connection oriented protocol and every connection oriented protocol needs to establish connection in order to reserve resources at both the communicating ends.

Connection Establishment –

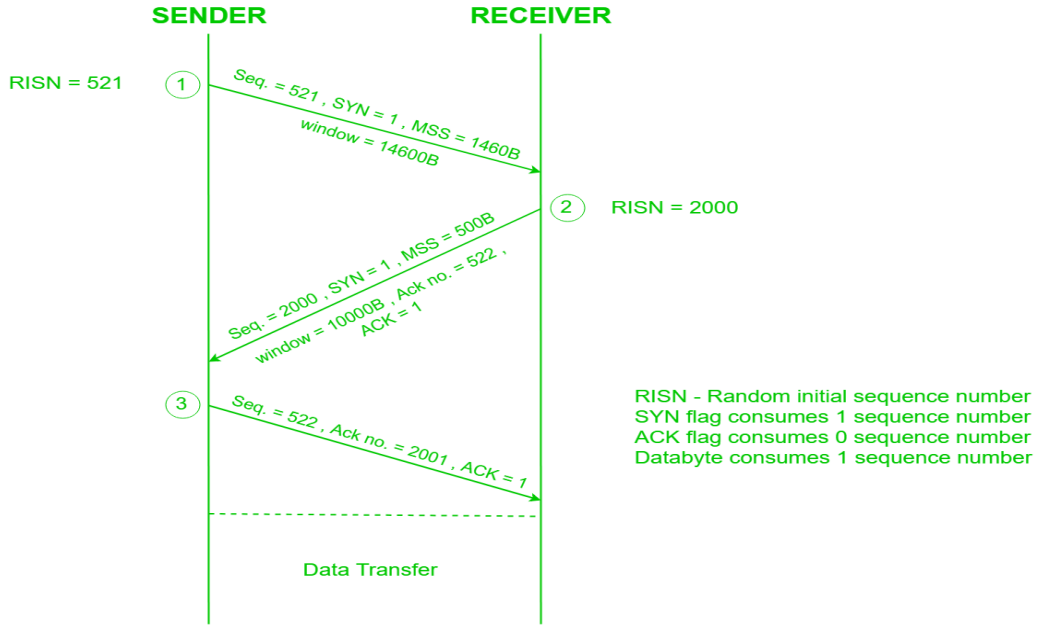
1. Sender starts the process with following:
    - **Sequence number (Seq=521):** contains the random initial sequence number which generated at sender side.
    - **Syn flag (Syn=1):** request receiver to synchronize its sequence number with the above provided sequence number.
    - **Maximum segment size (MSS=1460 B):** sender tells its maximum segment size, so that receiver sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header.
    - **Window size (window=14600 B):** sender tells about his buffer capacity in which he has to store messages from receiver.

2. TCP is a full duplex protocol so both sender and receiver require a window for receiving messages from one another.

- **Sequence number (Seq=2000):** contains the random initial sequence number which generated at receiver side.
- **Syn flag (Syn=1):** request sender to synchronize its sequence number with the above provided sequence number.
- **Maximum segment size (MSS=500 B):** sender tells its maximum segment size, so that receiver sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header.

3. Sender makes the final reply for connection establishment in following way:

- **Sequence number (Seq=522):** since sequence number = 521 in 1st step and SYN flag consumes one sequence number hence, next sequence number will be 522.
- **Acknowledgement Number (Ack no.=2001):** since sender is acknowledging SYN=1 packet from the receiver with sequence number 2000 so, the next sequence number expected is 2001.
- **ACK flag (ACK=1):** tells that acknowledgement number field contains the next sequence expected by sender.



----------→**Diagram 3M**

---------→**3 points -3M**

5. a) Illustrate different transport protocols at transport layer. Explain briefly. 6M

Ans: 1. TCP

- Connection oriented Point-to-point communication:
- Two end-points Reliable transfer:
- Data is delivered in order Full duplex communication Stream interface:
- Continuous sequence of octets Reliable connection startup:
- Data on old connection does not confuse new connections Graceful connection shutdown:
- Data sent before closing a connection is not lost.

Key Services: Send: Please send when convenient Data stream push: Please send it all now, if possible. Urgent data signalling: Destination TCP! please give this urgent data to the user (Urgent data is delivered in sequence. Push at the should be explicit if needed.) Note: Push has no effect on delivery. Urgent requests quick delivery. ----------→3M

2.UDP

- Connectionless end-to-end service
- No flow control.
- No error recovery (no acks)
- Provides port addressing
- Error detection (Checksum) optional.Applies to pseudo-header (same as TCP) and UDP segment. If not used, it is set to zero.
- Used by network management -------→3M

b) Draw the TCP header format and explain its fields briefly. 6M

Diagram---→3M Explanation----→3M

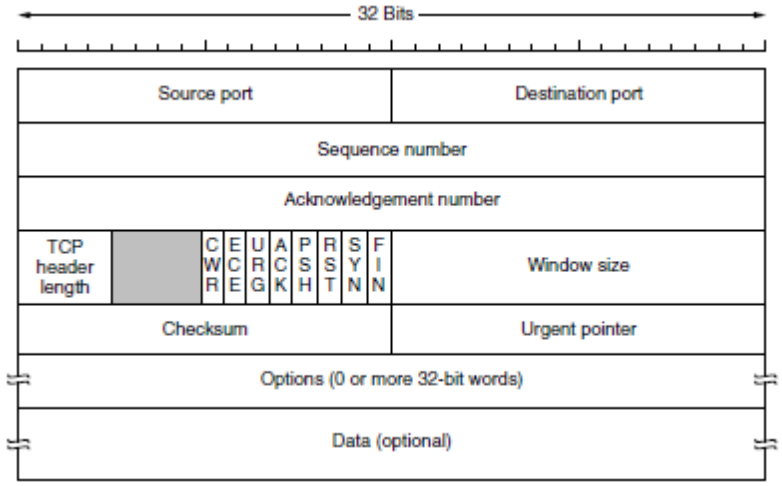
Ans: Figure below shows the layout of a TCP segment. Every segment begins with a fixed-format, 20-byte header. The fixed header may be followed by header options. After the options, if any, up to 65,535 − 20 − 20 = 65,495 data bytes may follow, where the first 20 refer to the IP header and the second to the TCP header. Segments without any data are legal and are commonly used for acknowledgements and control messages.

The Source port and Destination port fields identify the local end points of the connection.

The Sequence number and Acknowledgement number fields perform their usual functions. Note that the latter specifies the next in-order byte expected, not the last byte correctly received. It is a cumulative acknowledgement because it summarizes the received data with a single number.

The TCP header length tells how many 32-bit words are contained in the TCP header. This information is needed because the Options field is of variable length, so the header is, too. Technically, this field really indicates the start of the data within the segment, measured in 32-bit words, but that number is just the header length in words, so the effect is the same.

Now come eight 1-bit flags. CWR and ECE are used to signal congestion when ECN (Explicit Congestion Notification) is used, as specified in RFC 3168. ECE is set to signal an ECN-Echo to a TCP sender to tell it to slow down when the TCP receiver gets a congestion indication from the network. CWR is set to signal Congestion Window Reduced from the TCP sender to the TCP receiver so that it knows the sender has slowed down and can stop sending the ECN-Echo.



URG is set to 1 if the Urgent pointer is in use. The Urgent pointer is used to indicate a byte offset from the current sequence number at which urgent data are to be found.The ACK bit is set to 1 to indicate that the Acknowledgement number is valid. This is the case for nearly all packets. If ACK is 0, the segment does not contain an acknowledgement, so the Acknowledgement number field is ignored. The PSH bit indicates PUSHed data. The RST bit is used to abruptly reset a connection that has become confused due to a host crash or some other reason. The SYN bit is used to establish connections. The connection request has SYN = 1 and ACK = 0 to indicate that the piggyback acknowledgement field is not in use.

Unit-III

6 a) What is meant by DNS? Explain DNS resource record. 6M

Ans: Domain Name System is an Internet service that translates domain names into IP addresses. The DNS has a distributed database that resides on multiple machines on the Internet. DNS has some protocols that allow the client and servers to communicate with each other. **-------→2M**

Every domain, whether it is a single host or a top-level domain, can have a set of resource records associated with it. These records are the DNS database. For a single host, the most common resource record is just its IP address, but many other kinds of resource records also exist. When a resolver gives a domain name to DNS, what it gets back are the resource records associated with that name. Thus, the primary function of DNS is to map domain names onto resource records.

A resource record is a five-tuple. Although they are encoded in binary for efficiency, in most expositions resource records are presented as ASCII text, one line per resource record. The format we will use is as follows:

Domain name Time to live Class Type Value

The Domain name tells the domain to which this record applies. Normally, many records exist for each domain and each copy of the database holds information about multiple

domains. This field is thus the primary search key used to satisfy queries. The order of the records in the database is not significant.

The Time to live field gives an indication of how stable the record is. Information that is highly stable is assigned a large value, such as 86400 (the number of seconds in 1 day). Information that is highly volatile is assigned a small value, such as 60 (1 minute). We will come back to this point later when we have discussed caching.

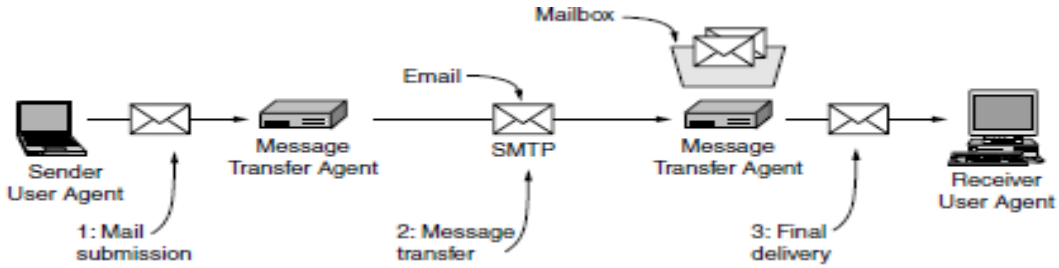
The third field of every resource record is the Class. For Internet information, it is always IN. For non-Internet information, other codes can be used, but in practice these are rarely seen.

The Type field tells what kind of record this is. There are many kinds of DNS records. The important types are listed. An SOA record provides the name of the primary source of information about the name server's zone (described below), the email address of its administrator, a unique serial number, and various flags and timeouts. ----------→**4M**

b) Illustrate e-mail architecture. 6M

Diagram---→3M Explanation----→3M

Ans: The architecture of the email system is shown in below Fig It consists of two kinds of subsystems: the user agents, which allow people to read and send email, and the message transfer agents, which move the messages from the source to the destination. We will also refer to message transfer agents informally as mail servers.



The user agent is a program that provides a graphical interface, or sometimes a text- and command-based interface that lets users interact with the email system. It includes a means to compose messages and replies to messages, display incoming messages, and organize messages by filing, searching, and discarding them. The act of sending new messages into the mail system for delivery is called mail submission. Some of the user agent processing may be done automatically, anticipating what the user wants. For example, incoming mail may be filtered to extract or reprioritize messages that are likely spam. Some user agents include advanced features, such as arranging for automatic email responses (''I'm having a wonderful vacation and it will be a while before I get back to you'').

A user agent runs on the same computer on which a user reads her mail. It is just another program and may be run only some of the time. The **message transfer agents** are typically system processes. They run in the background on mail server machines and are intended to be

always available. Their job is to automatically move email through the system from the originator to the recipient with SMTP (Simple Mail Transfer Protocol). This is the message transfer step. SMTP was originally specified as RFC 821 and revised to become the current RFC 5321. It sends mail over connections and reports back the delivery status and any errors. Numerous applications exist in which confirmation of delivery is important and may even have legal significance (‘‘Well, Your Honor, my email system is just not very reliable, so I guess the electronic subpoena just got lost somewhere’’).

(OR)

7.a) Explain www in brief.

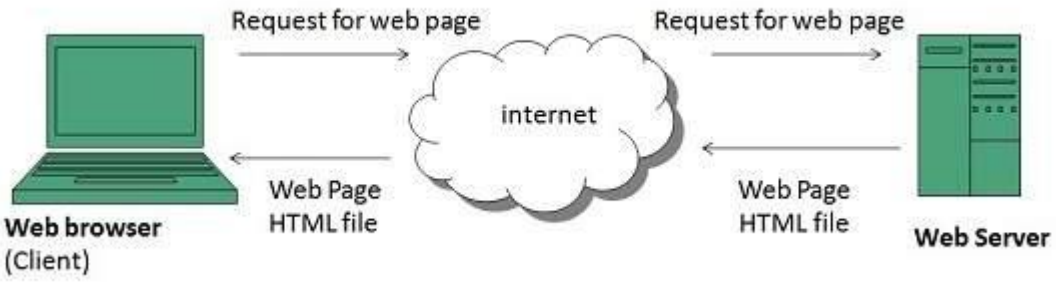
Diagram---→3M Explanation----→3M

Ans: WWW stands for World Wide Web. A technical definition of the World Wide Web is : all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

WWW Operation

WWW works on client- server approach. Following steps explains how the web works:

1. User enters the URL (say, http://www.tutorialspoint.com) of the web page in the address bar of web browser.
2. Then browser requests the Domain Name Server for the IP address corresponding to www.tutorialspoint.com.
3. After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.
4. Then web server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.
5. Now the web browser receives the web page, It interprets it and display the contents of web page in web browser’s window.



web page is a document available on world wide web. Web Pages are stored on web server and can be viewed using a web browser.

A web page can contain huge information including text, graphics, audio, video and hyper links. These hyper links are the link to other web pages

Static web pages are also known as flat or stationary web page. They are loaded on the client's browser as exactly they are stored on the web server. Such web pages contain only static information. User can only read the information but can't do any modification or interact with the information.

Dynamic web page shows different information at different point of time. It is possible to change a portaion of a web page without loading the entire web page. It has been made possible using **Ajax** technology.

Scripting languages are like programming languages that allow us to write programs in form of script. These scripts are interpreted not compiled and executed line by line.

b) Demonstrate video compression with example. 6M

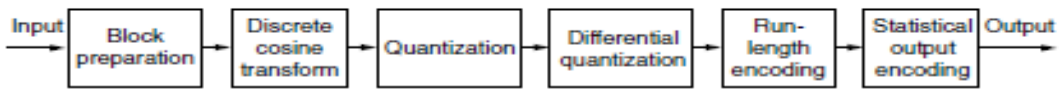
Ans: Diagram---→3M Explanation----→3M

Digital video that compression is critical for sending video over the Internet. Even a standard-quality video with 640 by 480 pixel frames, 24 bits of color information per pixel, and 30 frames/sec takes over 200 Mbps. This far exceeds the bandwidth by which most company offices are connected to the Internet.

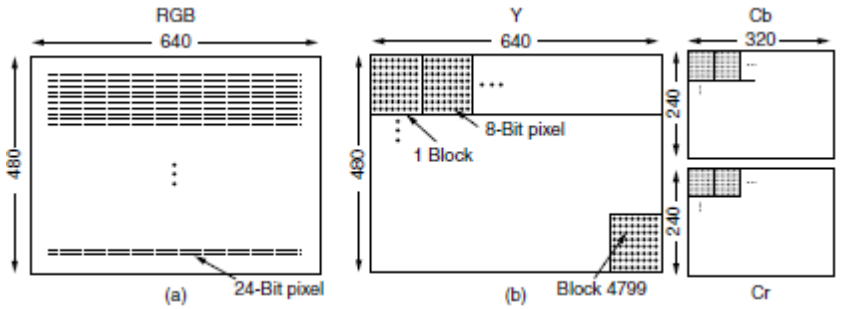
The JPEG (Joint Photographic Experts Group) standard for compressing continuous-tone still pictures (e.g., photographs) was developed by photographic experts working under the joint auspices of ITU, ISO, and IEC, another standards body. It is widely used (look for files with the extension jpg) and often provides compression ratios of 10:1 or better for natural images.

The algorithm is illustrated in Fig Step 1 is block preparation. For the sake of specificity, let us assume that the JPEG input is a 640 × 480 RGB image with 24 bits/pixel, as shown in Fig. 7-44(a). RGB is not the best color model to use for compression. The eye is much more sensitive to the luminance, or brightness, of video signals than the chrominance, or color, of video signals. Thus, we first compute the luminance, Y, and the two chrominances, Cb and Cr, from the R, G, and B components. The following formulas are used for 8-bit values that range from 0 to 255.

$$Y = 16 + 0.26R + 0.50G + 0.09B$$
$$Cb = 128 + 0.15R - 0.29G - 0.44B$$
$$Cr = 128 + 0.44R - 0.37G + 0.07B$$



Separate matrices are constructed for Y, Cb, and Cr. Next, square blocks of four pixels are averaged in the Cb and Cr matrices to reduce them to 320 × 240. This reduction is lossy, but the eye barely notices it since the eye responds to luminance more than to chrominance. Nevertheless, it compresses the total amount of data by a factor of two. Now 128 is subtracted from each element of all three matrices to put 0 in the middle of the range. Finally, each matrix is divided up into 8 × 8 blocks. The Y matrix has 4800 blocks; the other two have 1200 blocks each, as shown in fig.

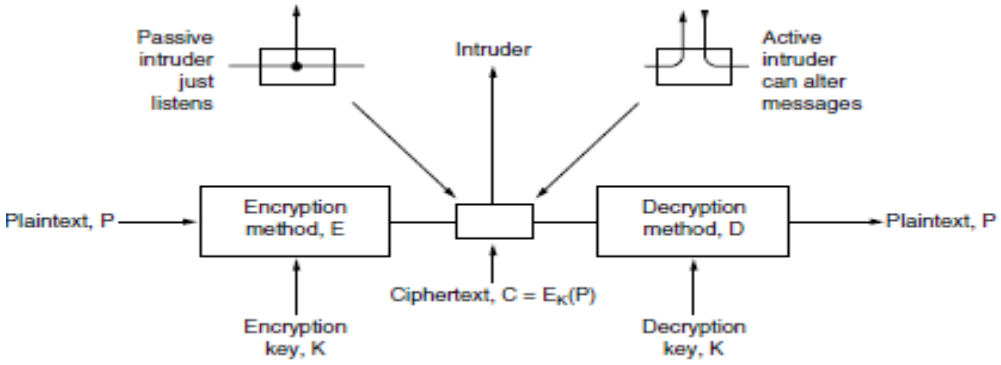


Step 2 of JPEG encoding is to apply a DCT (Discrete Cosine Transformation) to each of the 7200 blocks separately. The output of each DCT is an 8 × 8 matrix of DCT coefficients. DCT element (0, 0) is the average value of the block. The other elements tell how much spectral power is present at each spatial frequency. Normally, these elements decay rapidly with distance from the origin, (0, 0), as suggested by above Fig. Once the DCT is complete, JPEG encoding moves on to step 3, called quantization, in which the less important DCT coefficients are wiped out. This (lossy) transformation is done by dividing each of the coefficients in the 8 × 8 DCT matrix by a weight taken from a table. If all the weights are 1, the transformation does nothing. However, if the weights increase sharply from the origin, higher spatial frequencies are dropped quickly

8 a) Interpret the encryption model for symmetric key cipher with neat diagram. 6M

Ans: Diagram---→3M Explanation----→3M

The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key. The output of the encryption process, known as the ciphertext, is then transmitted, often by messenger or radio. We assume that the enemy, or intruder, hears and accurately copies down the complete ciphertext. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the ciphertext easily. Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver .

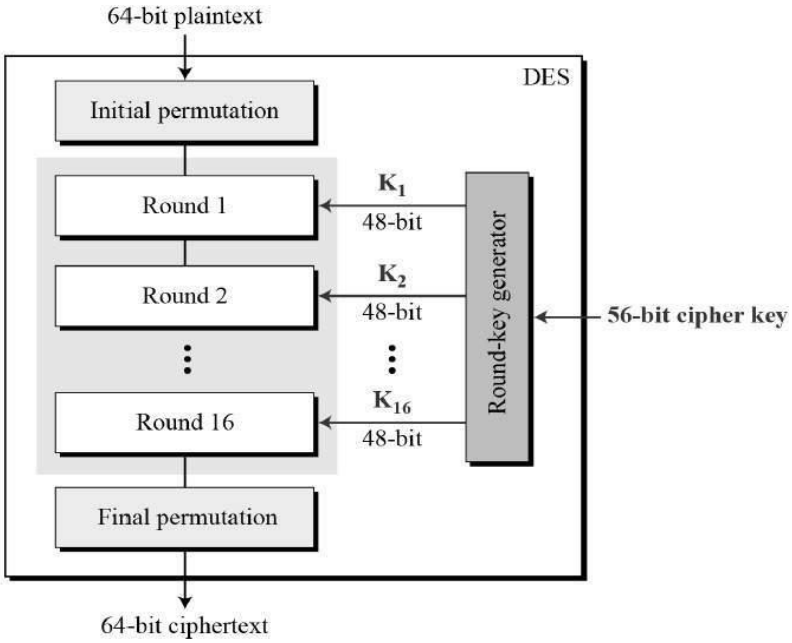


It will often be useful to have a notation for relating plaintext, ciphertext, and keys. We will use $C = E_K(P)$ to mean that the encryption of the plaintext P using key K gives the ciphertext C. Similarly, $P = D_K(C)$ represents the decryption of C to get the plaintext again. It then follows that $D_K(E_K(P)) = P$ This notation suggests that E and D are just mathematical functions, which they are. The only tricky part is that both are functions of two parameters, and we have written one of the parameters (the key) as a subscript, rather than as an argument, to distinguish it from the message.

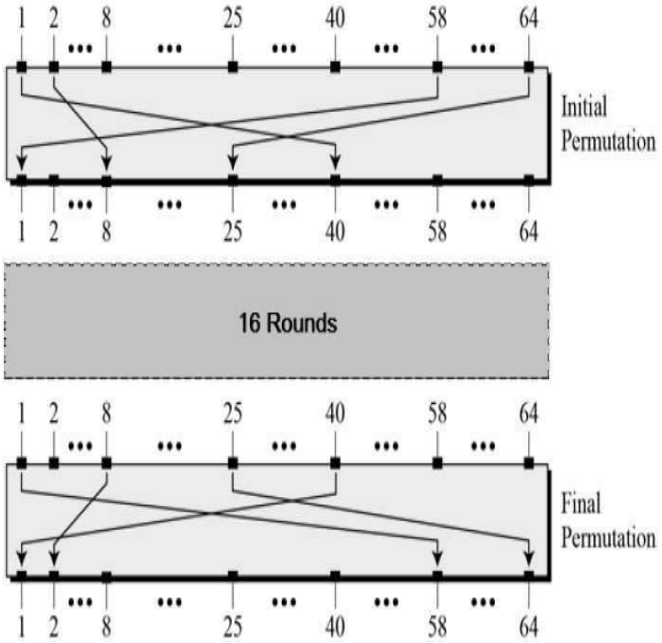
b) Explain DES.

Ans: Diagram---→3M Explanation----→3M

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration −

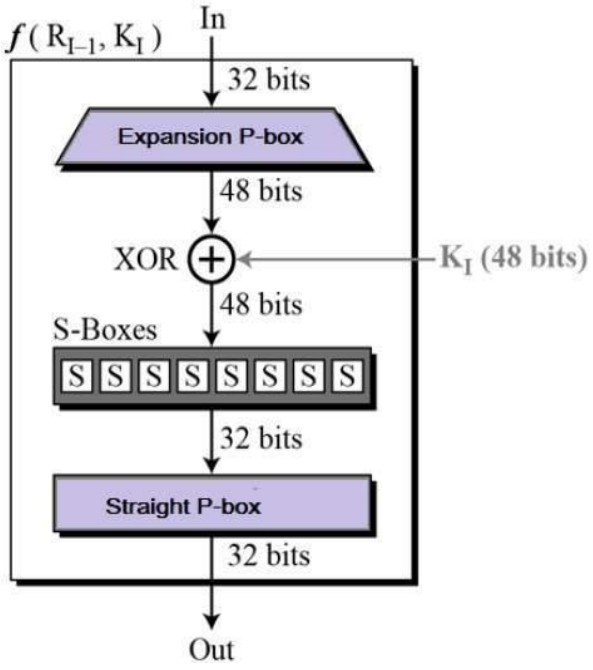


The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows



Round Function:

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



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.

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. Refer the following illustration

There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

(OR)

9.a) Authentication based on shared secret key. 6M

Ans: Diagram---→3M Explanation----→3M

Authentication protocol, we will assume that Alice and Bob already share a secret key, K_{AB}. This shared key might have been agreed upon on the telephone or in person, but, in any event, not on the (insecure) network. This protocol is based on a principle found in many authentication protocols: one party sends a random number to the other, who then transforms it in a special way and returns the result. Such protocols are called **challenge-response protocols**. In this and subsequent authentication protocols, the following notation will be used:

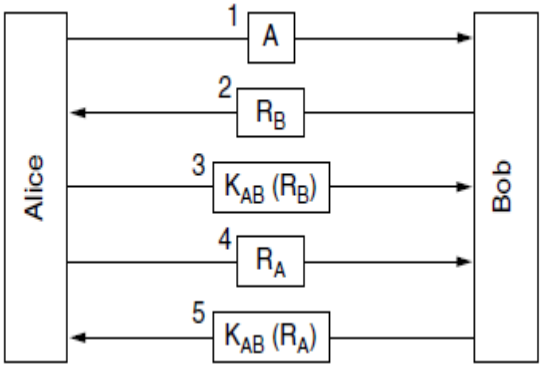
A, B are the identities of Alice and Bob.

R_i's are the challenges, where i identifies the challenger.

K_i's are keys, where i indicates the owner.

K_S is the session key.

In message 1, Alice sends her identity, *A*, to Bob in a way that Bob understands. Bob, of course, has no way of knowing whether this message came from Alice or from Trudy, so he chooses a challenge, a large random number, *RB*, and sends it back to ''Alice'' as message 2, in plaintext. Alice then encrypts the message with the key she shares with Bob and sends the ciphertext, *KAB*(*RB*), back in message 3. When Bob sees this message, he immediately knows that it came from Alice because Trudy does not know *KAB* and thus could not have generated it. Furthermore, since *RB* was chosen randomly from a large space (say, 128-bit random numbers), it is very unlikely that Trudy would have seen *RB* and its response in an earlier session. It is equally unlikely that she could guess the correct response to any challenge.



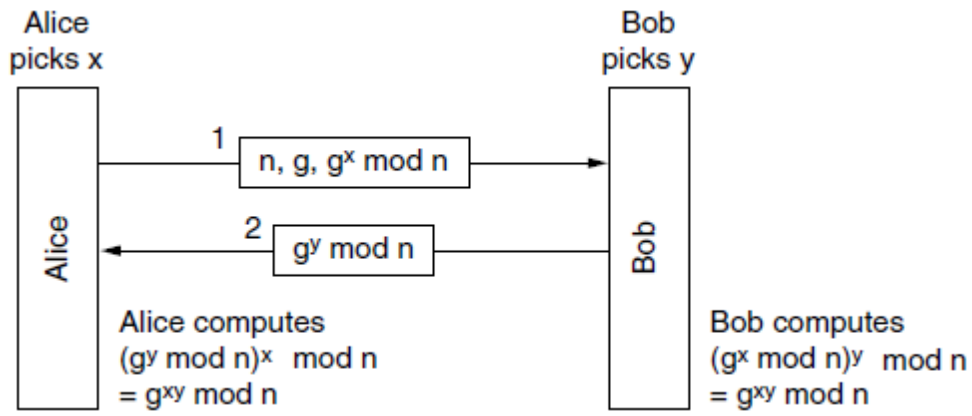
At this point, Bob is sure he is talking to Alice, but Alice is not sure of anything. For all Alice knows, Trudy might have intercepted message 1 and sent back R_B in response. Maybe Bob died last night. To find out to whom she is talking, Alice picks a random number, R_A, and sends it to Bob as plaintext, in message 4. When Bob responds with K_{AB}(RA), Alice knows she is talking to Bob. If they wish to establish a session key now, Alice can pick one, K_S, and send it to Bob encrypted with K_{AB}.

b) The Diffie - Hellman key exchange. 6M

Ans: Diagram---→3M Explanation----→3M

The protocol that allows strangers to establish a shared secret key is called the Diffie-Hellman key exchange and works as follows. Alice and Bob have to agree on two large numbers, n and g, where n is a prime, (n − 1)/2 is also a prime, and certain conditions apply to g. These numbers may be public, so either one of them can just pick n and g or tell the other openly. Now Alice picks a large (say, 1024-bit) number, x, and keeps it secret. Similarly, Bob picks a large secret number, y.

Alice initiates the key exchange protocol by sending Bob a message containing (n, g, g^x mod n), as shown in Fig below. Bob responds by sending Alice a message containing gy mod n. Now Alice raises the number Bob sent her to the xth power modulo n to get (g^y mod n) ^{x} mod n. Bob performs a similar operation to get (g^x mod n) ^{y} mod n. By the laws of modular arithmetic, both calculations yield g^{xy} mod n. Lo and behold, as if by magic, Alice and Bob suddenly share a secret key, g^{xy} mod n.



Trudy, of course, has seen both messages. She knows g and n from message 1. If she could compute x and y, she could figure out the secret key. The trouble is, given only g^x mod n, she cannot find x. No practical algorithm for computing discrete logarithms modulo a very large prime number is known.

Scheme Prepared By: P RATNA PRAKASH HOD, I.T.
I.T. Dept,