# CBCS SCHEME

USN □□□□□□□□□□

18CS52

## Fifth Semester B.E. Degree Examination, July/August 2022
## Computer Networks and Security

Time: 3 hrs.

Max. Marks: 100

Note: ***Answer any FIVE full questions, choosing ONE full question from each module.***

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

### Module-1

1 a. Explain the steps involved in transferring a web page from server to client in case of HTTP with non – persistent connection. Also brief the Back of the Envelope calculation for time needed to request and receive the file. **(10 Marks)**

b. Consider an e – commerce site that wants to keep a purchase record for each of its customers. Describe with neat diagram how this can be done with cookies. **(10 Marks)**

**OR**

2 a. Explain with neat diagram, the socket related activity of client – server communication over the TCP along with client and server code. **(10 Marks)**

b. Explain FTP with its Commands and Replies. **(10 Marks)**

### Module-2

3 a. Describe the various fields of UDP segment structure. Suppose you have the following three 16 – bit words 0110011001100000 , 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 , 1000111100001100. Find the checksum. How does the receiver detect errors? Is it possible that 1 – bit errors will go undetected? **(10 Marks)**

b. Explain Sender and Receiver side Finite State Machine (FSM) representation for rdt 2.1 protocol. **(10 Marks)**

**OR**

4 a. Draw TCP Segment structure. Describe the various fields of TCP segment structure. **(10 Marks)**

b. Explain with neat diagram, the causes and costs of congestion considering the following scenarios.

Scenario 1 : Two sender , A Router , with Infinite Buffer.
Scenario 2 : Two sender , A Router , with Finite Buffer. **(10 Marks)**

### Module-3

5 a. Write Link state Routing Algorithm. Apply it to the following graph [Refer Fig. Q5(a)] with source node as "U". Draw the least cost path tree and the forwarding table for node "U". **(10 Marks)**

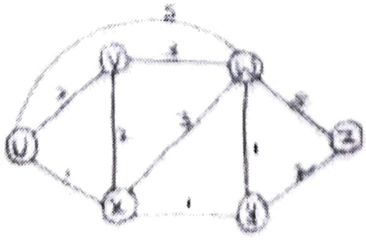


Fig. Q5(a)

b. Draw IPV4 datagram format. Mention the significance of each field. **(10 Marks)**

OR

6 a. Write distance Vector Routing Algorithm and apply it to the following graph. [Refer Fig. Q6(a)]. **(10 Marks)**

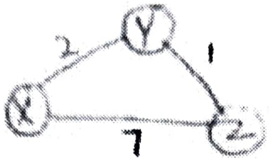


Fig. Q6(a)

b. Draw IPV6 datagram format. Mention the significance of each field. **(10 Marks)**

## Module-4

7 a. Explain Diffie – Hellman Key Exchange Protocol. Suppose two parties A and B wish to set up a common secret key between themselves using Diffie Hellman Protocol selecting generator as 3 and prime number as 7. Party A chooses 2 and Party B chooses 5 as their respective secret. Find the Diffie Hellman Key. **(10 Marks)**

b. Explain Data Encryption Standard (DES) algorithm. **(10 Marks)**

OR

8 a. Explain three phases of RSA Algorithm. For an encryption of a 4 – bit message "1000" or M = 9 we choose a = 3 and b = 11. Find the Public and Private keys for this security action and show the Cipher text. **(10 Marks)**

b. Write short notes on :

i) Security Implementation in wireless IEEE 802.11.

ii) Firewalls. **(10 Marks)**

## Module-5

9 a. Explain how DNS Redirects a User's request to a CDN Server. **(10 Marks)**

b. Explain RTP Basics and RTP packet Header fields. **(10 Marks)**

OR

10 a. Explain the properties of Audio and Video. Also mention the three key distinguishing features of Streaming Stored Video. **(10 Marks)**

b. With neat diagram, explain Session Initiation Protocol (SIP) Call establishment. **(10 Marks)**

Subject name: Computer N/WS and Security

Subject Code: 18CS52.

Subject Incharge: Ravindra P.

Q. P : July / August 2022.

1. a. Explain the steps involved in transferring a web page from server to client in case of HTTP with non-persistent conn. Also brief the Back of the Envelope calculation for time needed to request and receive the file.

→ • A non-persistent connection is closed after the server sends the requested-object to the client.

• The conn is used exactly for one request and one response. (7M)

Steps: Client site Server site

1a HTTP client initiates TCP conn to HTTP server @ www.someschool.edu on port 80

1b HTTP server at host www.someschool.edu waiting for TCP conn at port 80 "accepts" conn, notifying client

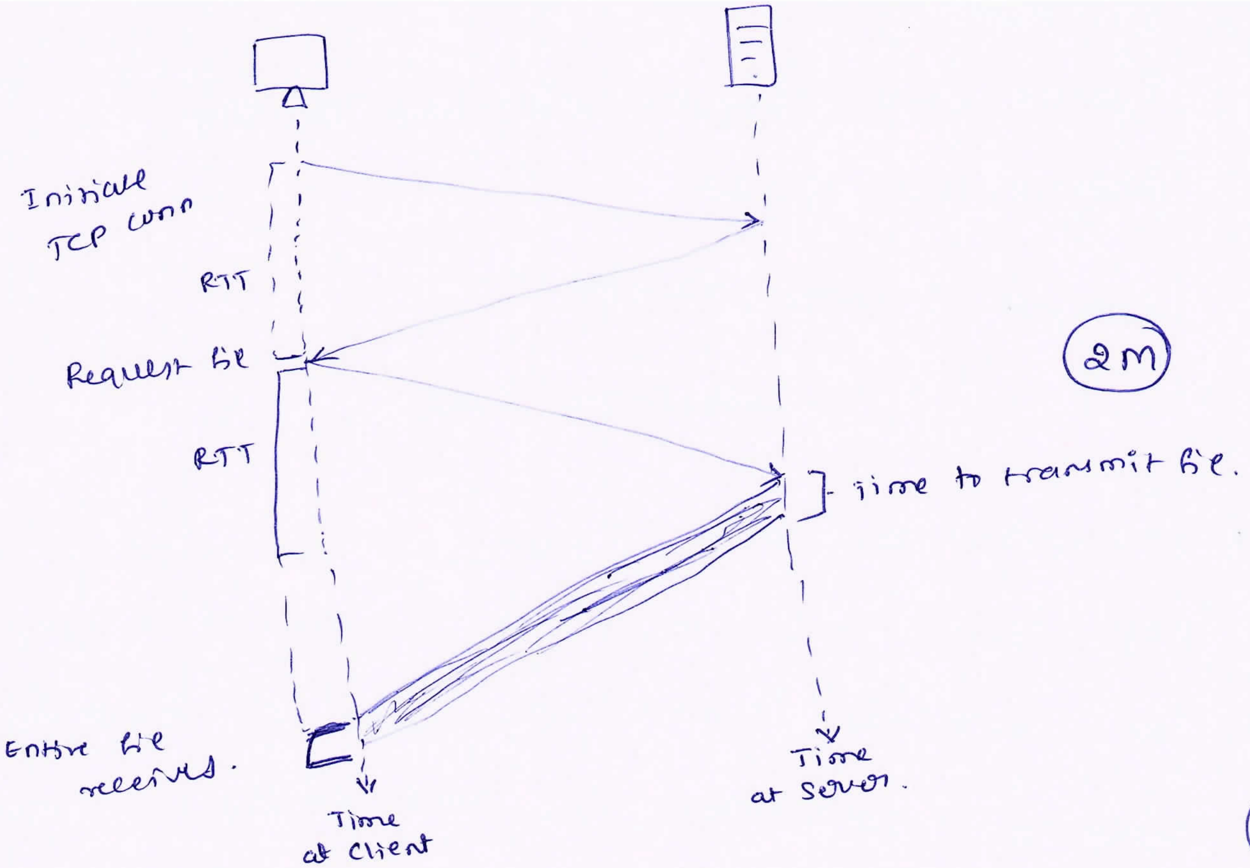
2 HTTP client sends HTTP req msg.

3. HTTP server receives req msg.

4. HTTP server closes TCP conn

5 HTTP client receives response msg containing html file display HTML

6. Steps 1-5 repeated for ~~for~~ more than one object requests



2m

1m

Total Response time is 2 RTT plus the transmission time at the server of the file

ie 2(RTT) + File transmition time

1.b. Consider an E-commerce site that wants to keep a purchase record for each of its customers. Describe with neat Diagram how this can be done with cookies.

→ For answer refer Feb/mar-2022 QP. solution 1. b. answer.

2. a. Explain with neat diagram, the Socket relates activity of client - server communication over the TCP along with client and server code.

→

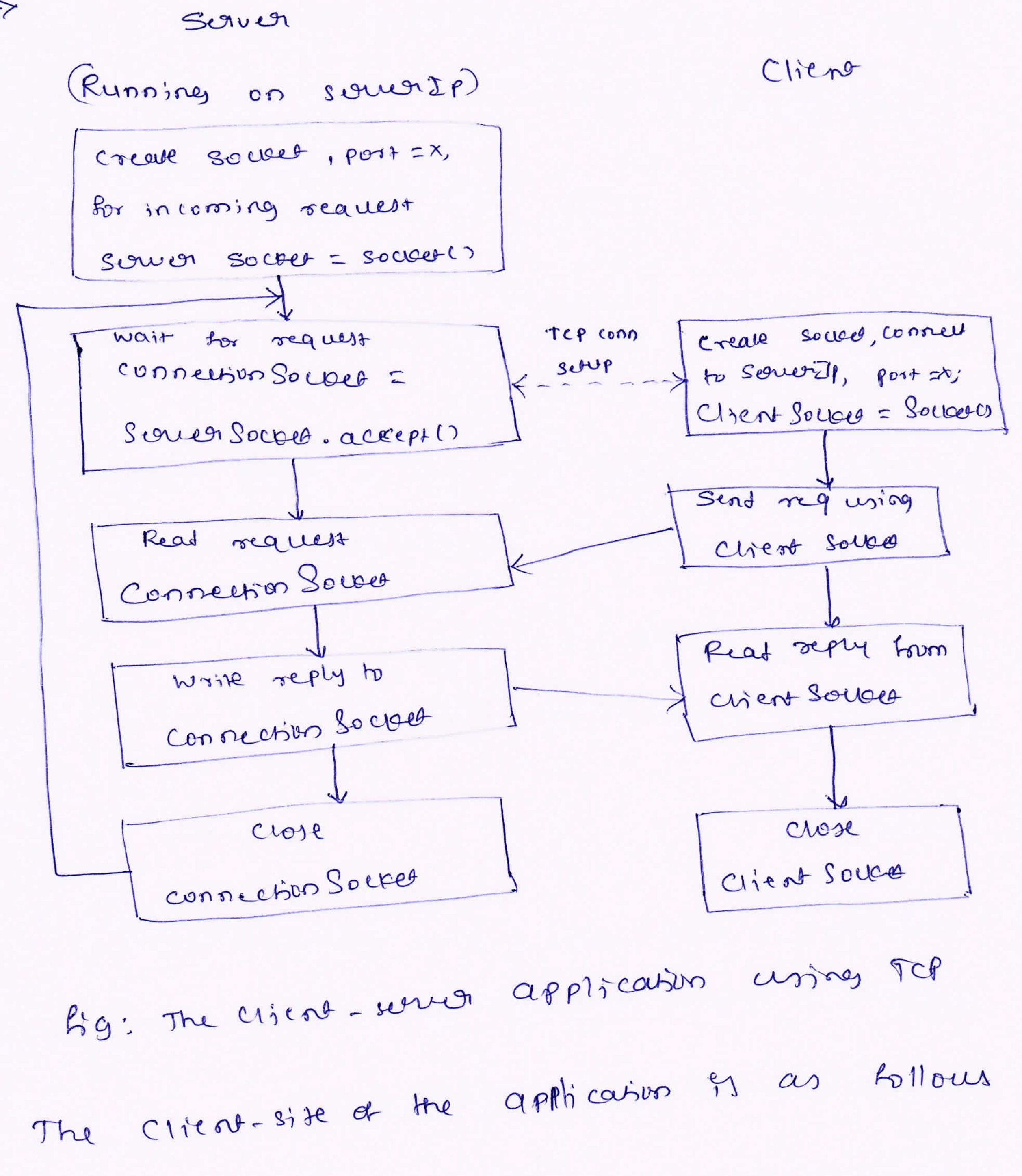


fig: The client - server application using TCP

The client - site of the application is as follows

```
from Socket import *
ServerName = 'servername'
ServerPort = 12000
ClientSocket = Socket(AF_INET, SOCK_STREAM)
Client Socket. connect((ServerName, server Port))
```

```
Sentence = raw-input ('Input lowercase sentence:')
Client Socket . send ( sentence)
modifiedSentence = ClientSocket . recv (1024)
print 'From server:' modified Sentence
ClientSocket . close ().
```

3M

The server side of the application (code) is as follows

```
from socket import
serverPort = 12000
serverSocket = socket (AF-INET, SOCK-STREAM)
server Socket . bind (('', ServerPort))
Server Socket . listen (1)
print 'The server is ready to receive'

while 1:

connection Socket , addr = serverSocket . accept()
Sentence = connection Socket . recv (1024)
CapitalizedSentence = sentence . upper()
Connection Socket. send (Capitalized Sentence )
Connection Socket . close()
```

3m

2 b. Explain FTP with its commands and replies

→ FTP command are

1. USER username

used to send the user identification to the server.

2. PASS password.

Used to send the user password to the server.

3. LIST

used to ask the server to send back a list of all the files in the current remote directory.

5M

4. RETR filename.

used to retrive a file from the current directory of the remote-host.

5. STOR filename.

used to store a file into the current of the remote host.

FTP replies are.

5M

1) 331 username OK, password requires.

2) 125 Data connection already open; transfer starting

3) 425 Can't open Data connection

4) 452 Error writing file.

3. a. Describe the various fields of UDP segment structure

Suppose you have the following three 16-bit words

0110011001100000, 0101010101010101, 1000111100001100.

Find the checksum. How does the receiver detect errors?

Is it possible that 1 bit errors will go undetected?

→

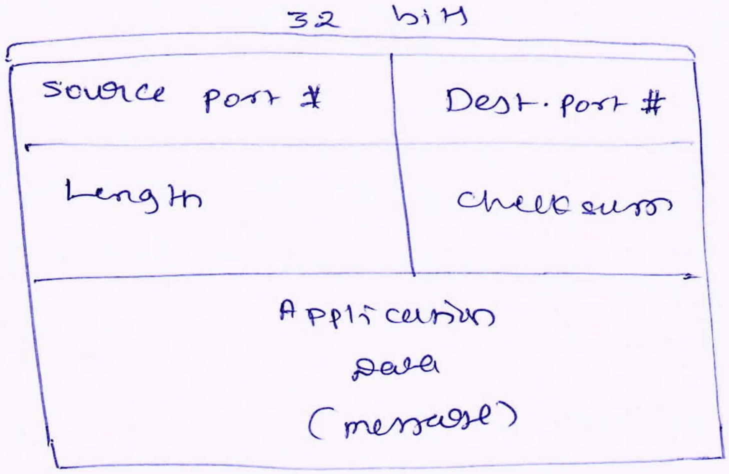


fig: UDP Segment Structure.

2 m

① Application Data: this field occupies the data-field of the segment.

② Destination port no: This field used to deliver the data to correct process running on the destination host.

③ Length: this field specifies the number of bytes in the segment. (header + data).

④ Checksum: this field is used for Error-detection.

Steps to calculate checksum on the sender side.

1) All the 16 bit words in the segment are added to get a sum

2) Then, the 1's complement of the sum is obtained to get a result.

3) Finally, the result is added to the checksum field inside the segment.

How to check for Error on the receiver

1) All the 16 bit words in the segment

i) For no Errors: In the sum, all the bits are 1.

ii) For any Error: In the sum, at least one of the bits is a 0.

0 110011001100000
0 101010101010101
1000111100001100

Sum of all 16 bit words 0100101011000010
1011 0101 00111101 1's complement

1's complement value is called as checksum which is added inside the segment.

On the receiver

- All the 16 bit words are added, including the checksum

i) if no Errors are introduced into the pkt, then clearly the sum will be 1111111111111111

ii) If one of the bits is 0, then Errors have been introduced into the pkt.

All 1-bit Errors are detected.

3 b. Explain sender and Receiver side finite state Machine (FSM) representation for rdt 2.1 protocol.

→

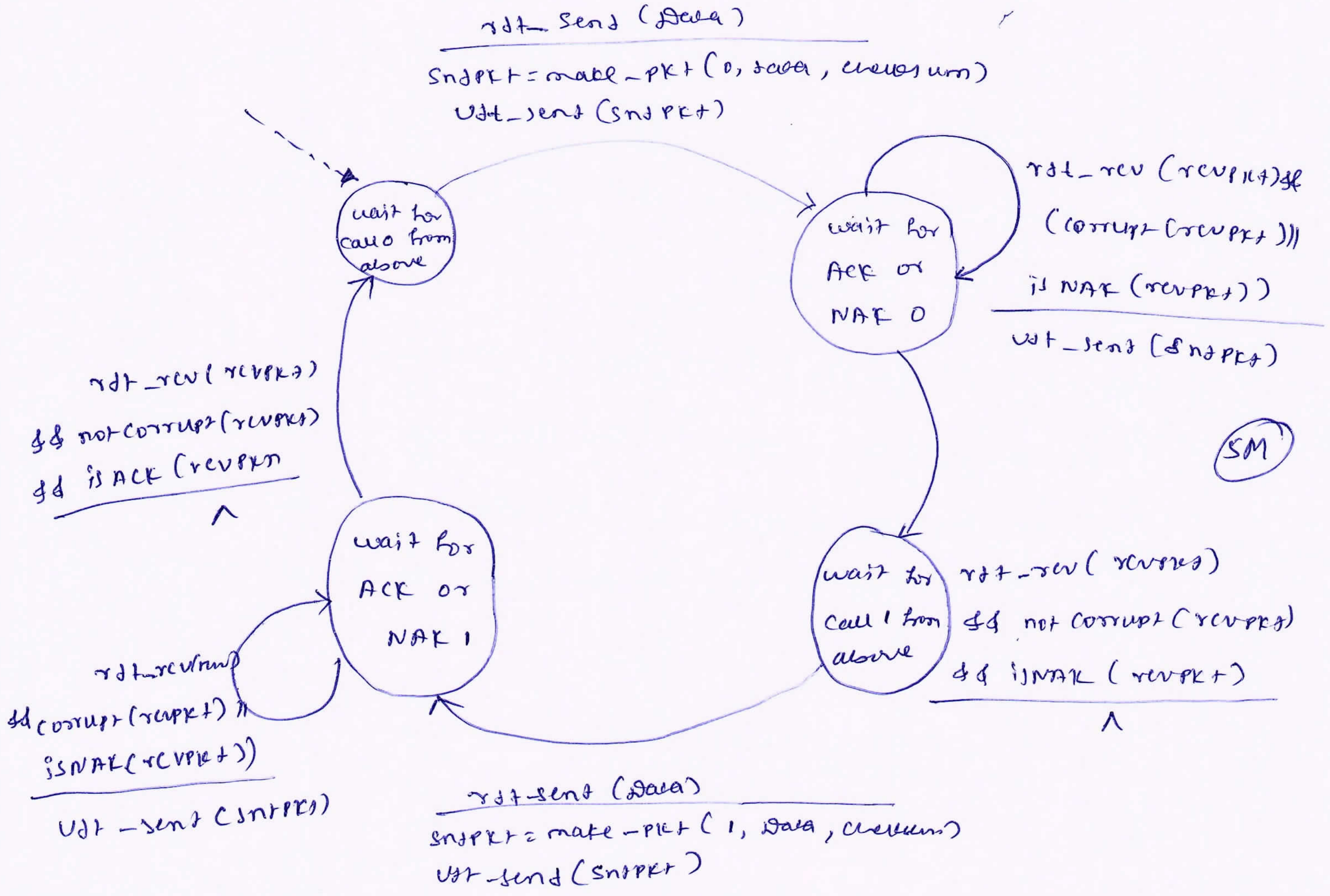

rdt_send (Data)
sndpkt = make_pkt (0, data, checksum)
udt_send (sndpkt)
wait for call 0 from above
wait for ACK or NAK 0
rdt_rcv (rcvpkt) && (corrupt (rcvpkt)) || isNAK (rcvpkt))
udt_send (sndpkt)
rdt_rcv ( rcvpkt) && notcorrupt (rcvpkt) && isACK (rcvpkt)
Λ
wait for ACK or NAK 1
rdt_rcv(rcvpkt) && corrupt (rcvpkt) || isNAK(rcvpkt))
udt_send (sndpkt)
wait for call 1 from above
rdt_rcv ( rcvpkt) && not corrupt (rcvpkt) && isNAK ( rcvpkt)
Λ
rdt_send (Data)
sndpkt = make_pkt ( 1, Data, checksum)
udt_send (sndpkt)
5M

fig : rdt 2.1 sender.

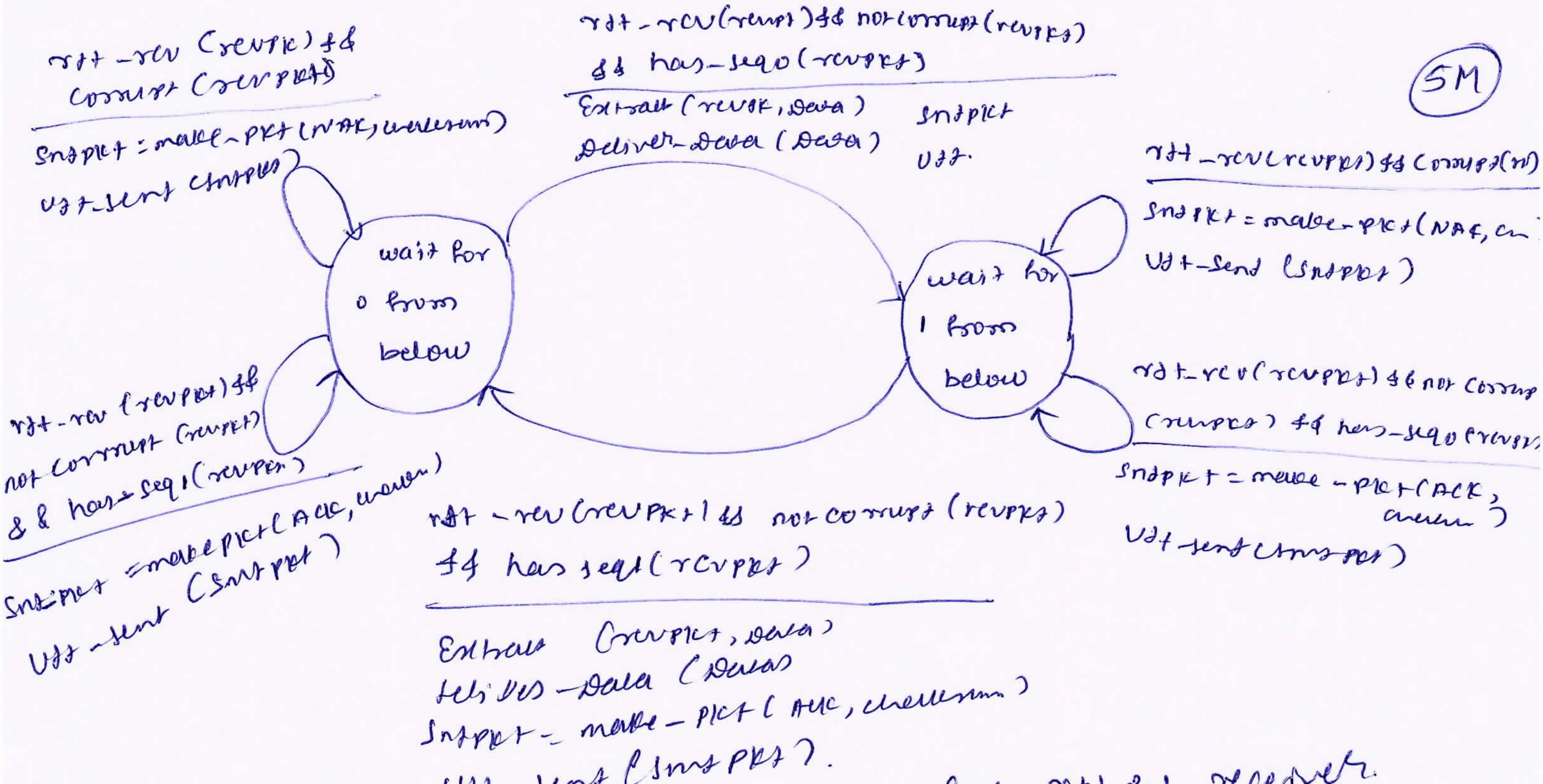

rdt_rcv (rcvpkt)&& notcorrupt(rcvpkt) && has_seq0 (rcvpkt)
Extract (rcvpkt, Data)
Deliver_Data (Data)
sndpkt
udt.
rdt_rcv (rcvpkt) && corrupt (rcvpkt)
sndpkt = make_pkt (NAK, checksum)
udt_sent (sndpkt)
wait for 0 from below
rdt_rcv (rcvpkt) && not corrupt (rcvpkt) && has_seq1 (rcvpkt)
sndpkt = make pkt (ACK, checksum)
udt_sent (sndpkt)
wait for 1 from below
rdt_rcv (rcvpkt) && corrupt (rcvpkt)
sndpkt = make_pkt (NAK, ch
udt_send (sndpkt)
rdt_rcv (rcvpkt) && not corrupt (rcvpkt) && has_seq0 (rcvpkt)
sndpkt = make_pkt (ACK, checksum)
udt_sent (sndpkt)
rdt_rcv (rcvpkt) && not corrupt (rcvpkt) && has seq1 (rcvpkt)
Extract (rcvpkt, data)
deliver_Data (Data)
sndpkt = make_pkt ( ACK, checksum)
udt_send (sndpkt).
5M

fig: rdt 2.1 receiver.

4. a. Draw TCP-segment structure. Describe the various fields of TCP segment structure.

→

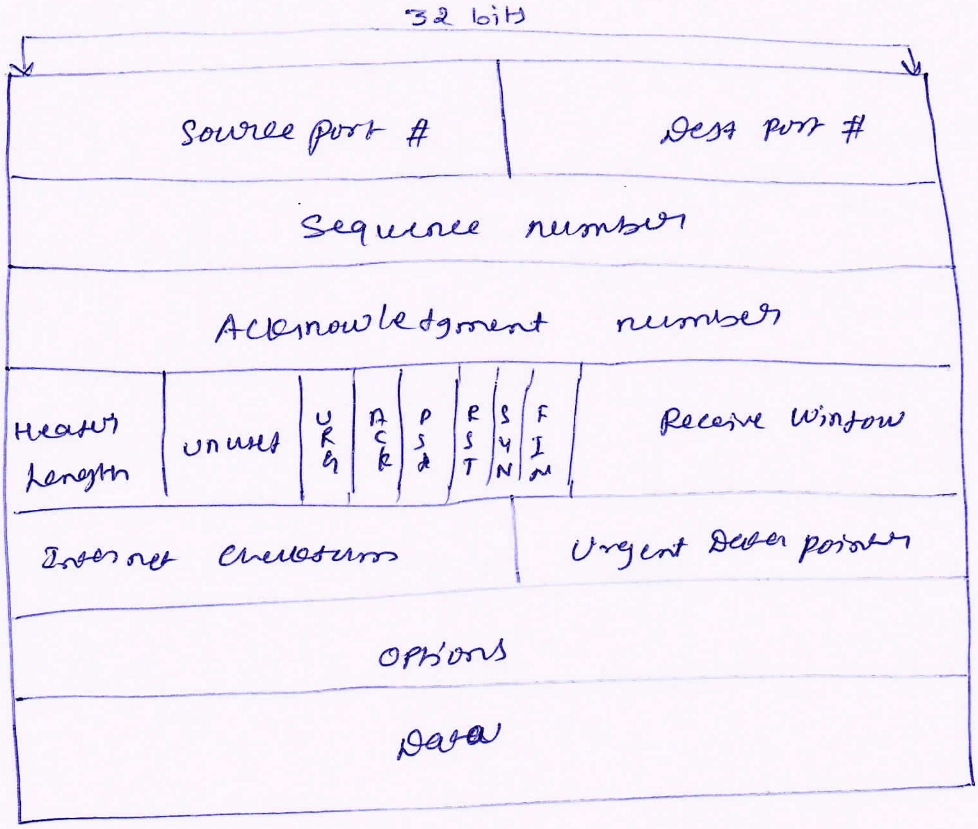


fig :- TCP segment structure.

The fields of TCP segment are as follows:

1) Source & Destination port number:
used for multiplexing / Demultiplexing data from / to upper layer applications.

2) Seq no & Ack no:
used to implement reliable data-transfer service

3) Header length:
Specifies the length of the TCP header

4) Flag: This field has 6 bits.

i) ACK ii) RST iii) SYN iv) FIN.

5) Receive window:
This field defines receiver's window size

6) Checksum: this field is used for Error detection

7) Urgent Data pointer: this field indicates the location of the last byte of the urgent data.

8) Options:

this field is used when a sender & receiver negotiate the mss for use in high-speed networks.

4. b. Explain with neat Diagrams, the causes and cost of congestion considering the following. Scenarios.

Scenario 1 : Two Senders, A Router, with Infinite Buffer

Scenario 2 : Two Sender, A Router, with finite Buffer.

→

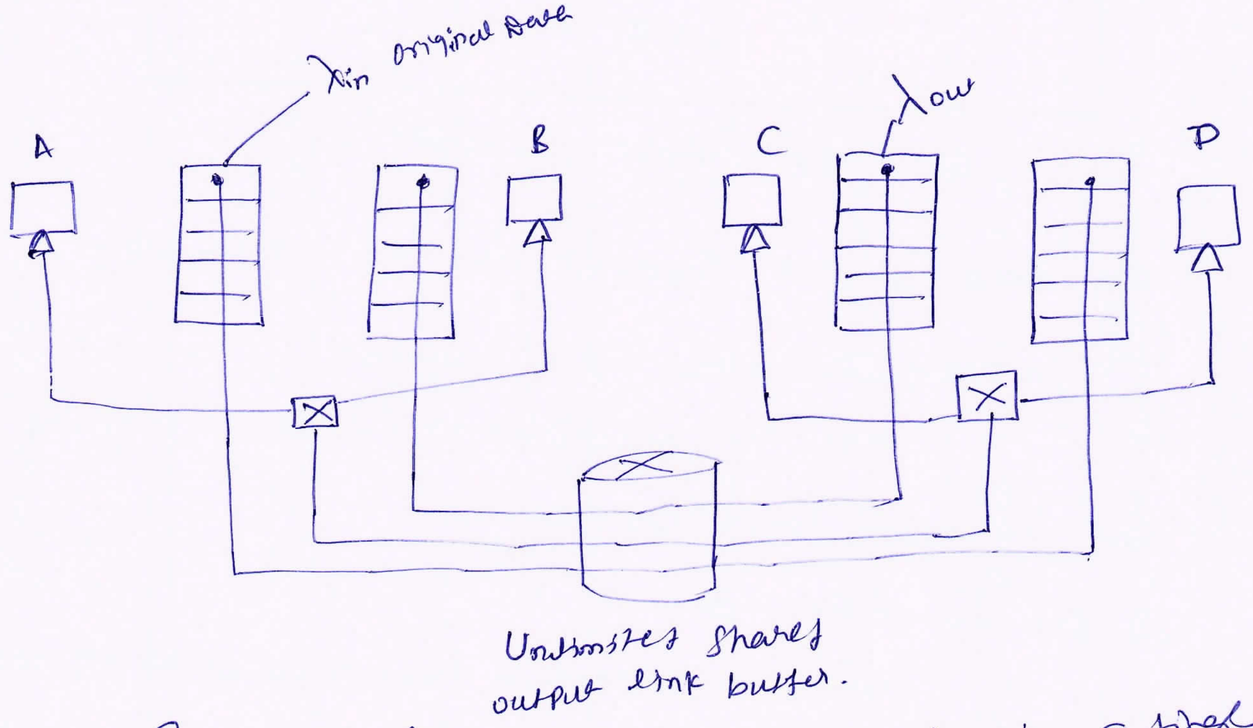


fig: Congestion Scenario 1 : Two conn sharing a single hop with infinite buffers.

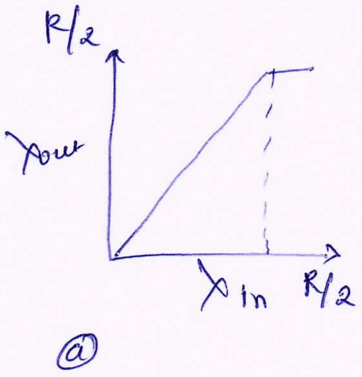
let sending-rate of host-A = λin bytes/sec

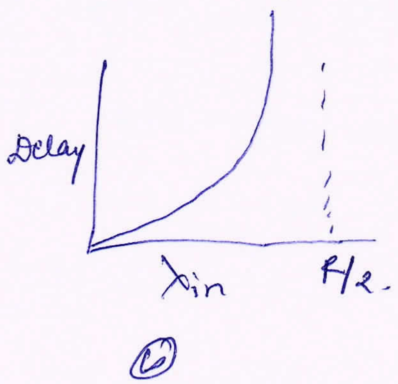
outgoing links capacity = R.

- packets from Host A & B pass through a router & over a shared outgoing link

- the router has buffers

- the buffers stores incoming pakets when packet arrival rate exceeds the outgoing links capacity.





Scenario 2:

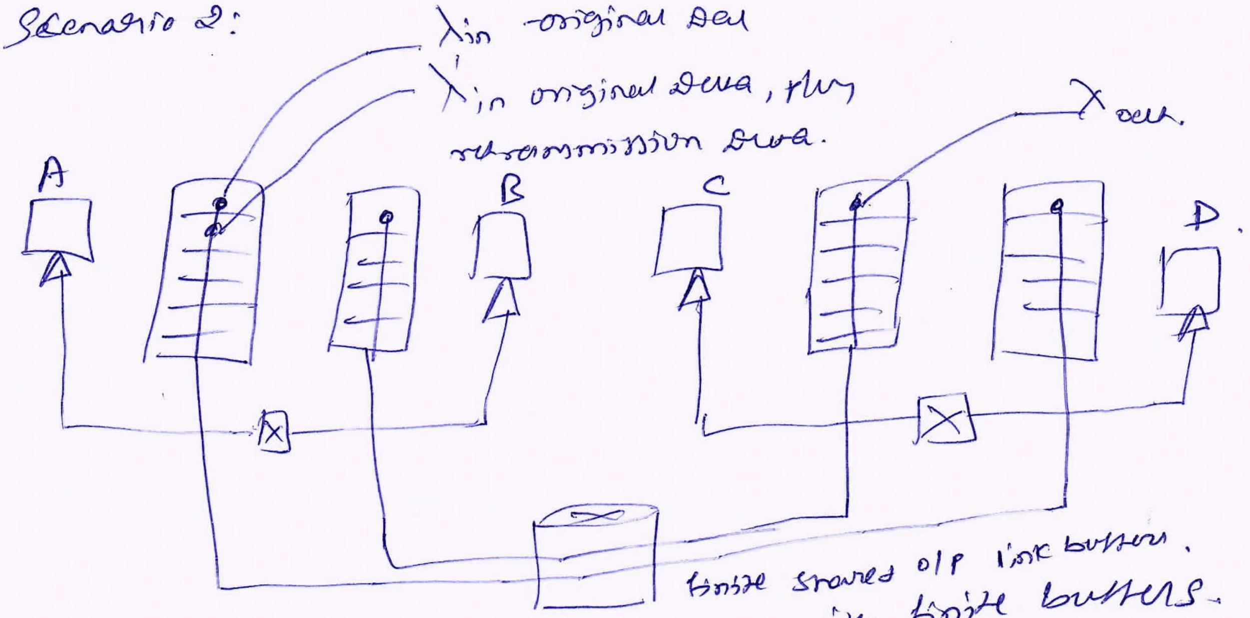
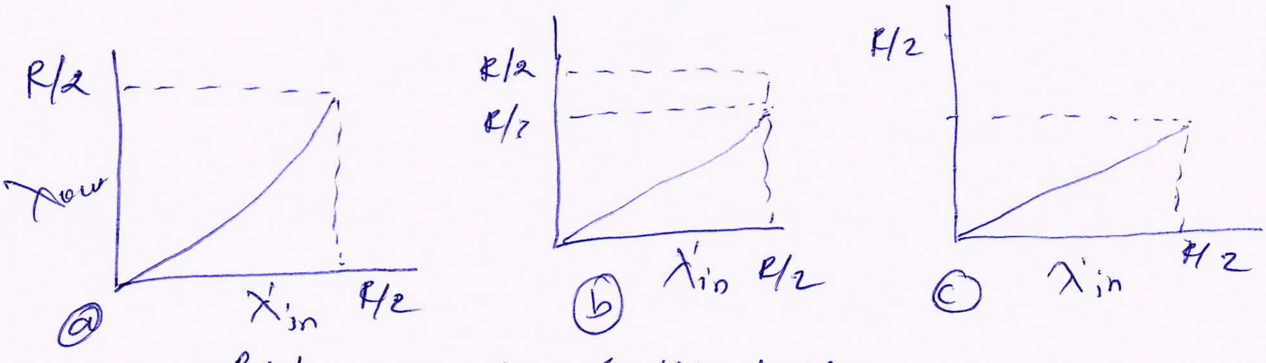

λin original data
λ'in original data, plus retransmission data.
λout.
A
B
C
D.
finite shared o/p link buffers.

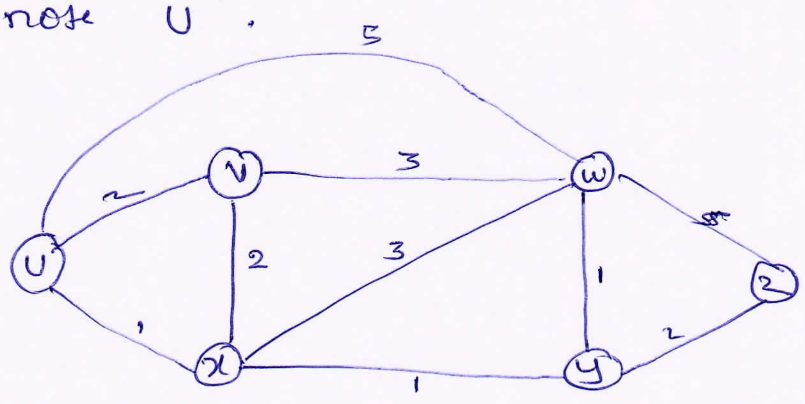
fig: 2 hosts and a router with finite buffers.

- Host A sends a pkt only when a buffer is free
- In this case
  - no loss occurs.
  - λin will be to λ'in and
  - throughput of the conn will be Equal to λin.



Performance with finite buffer.

5 a. Write link state routing algorithm. Apply it to the following graph with source node as "U". Draw the least cost path tree and the forwarding table for node "U".



→ For answer refer Q.P Feb/Mar. 2022 solution Question 6.a answer.

5 b. Draw IPv4 Datagram format. Mention the significance of each field.

→

<table>
<tr><td>Version</td><td>Header Length</td><td>Type of service</td><td colspan="2">Datagram length</td></tr>
<tr><td colspan="3">16 bit identifier</td><td>Flag</td><td>13 bit Fragmentation offset</td></tr>
<tr><td colspan="2">Time-to-live</td><td>Upper layer protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">32 bit Source IP address</td></tr>
<tr><td colspan="5">32 bit Destination IP address</td></tr>
<tr><td colspan="5">options (if any))</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

4M

fig: IPv4 Datagram format.

1) Payload or Data: Represent Data to be Delivered to the destination

2) Heater : It contains info Essential to routing and Delivery. It contain following fields.

1) Version : specifies the version of the IPv4 Datagram.

2) Heater length : Specifies length of heater.

3) TOS : specifies priority of packet based on paramete such as Delay, throughput

4) Datagram length : specifies total length of the Datagram (heater + Data).

Max length = 65535 bytes.

5) TTL : Defines life time of the Datagram. in hops.

6) protocol : TCP = 6 UDP = 17 specifies upper layer protocol.

7) Heater checksum : used to verify integrity of heater only.

8) Source IP address & Destination IP address :

These fields contains source & destination addresses.

9) options :

This field allows the pkt to request special features such as.

→ security level.

→ route to be taken by packet at Each router.

6. a. Write Distance Vector Routing algorithm and Apply it to the following graph.

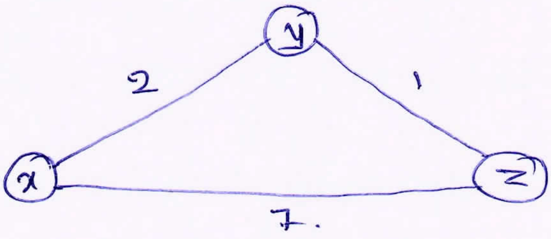


fig 6.a.

→ For answer refer Q.P Feb/Mar. 2022 Question number 5. c answer.

6. b. Draw IPv6 Datagram format. Mention the significance of Each field.

→

<table>
<tr><td>Version</td><td>Traffic class</td><td colspan="2">Flow label</td></tr>
<tr><td colspan="2">Payload length</td><td>Next hdr</td><td>Hop limit</td></tr>
<tr><td colspan="4">Source address<br>(128 bits)</td></tr>
<tr><td colspan="4">Destination Address<br>(128 bits)</td></tr>
<tr><td colspan="4">Data.</td></tr>
</table>

fig: IPv6 Datagram format

1) version: specifies the IP Version ie 6.

2) Traffic class: It indicates the priority of the packet.

3) Flow Label: This field is used to provide special handling for a particular flow of Data

4) payload length: shows the length of the IPv6 payload.

7. b. Explain DES algorithm.

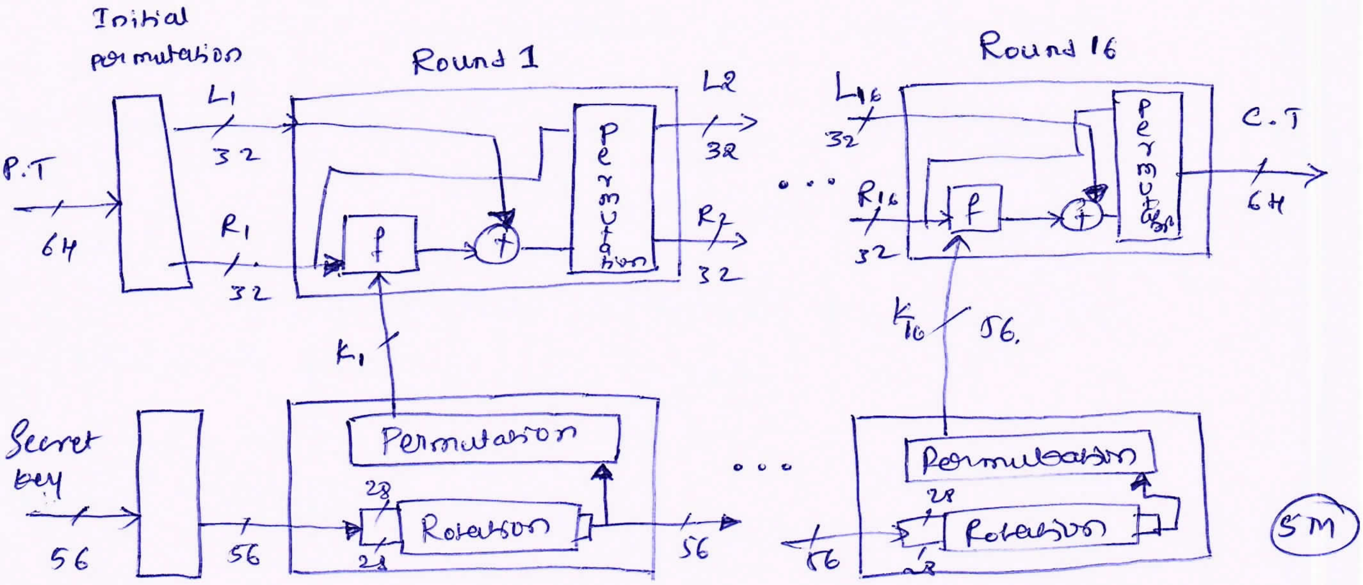


fig: Data Encryption Standard.

1. Initialize. Before round 1 begins, all 64 bits of an incoming message and all 56 bits of the secret key are seperately permutes (shuffles).

2. Each incoming 64 bit msg is broken into 2 32 bi halves denotes by $L_i$ ant $R_i$ resp$^{ly}$.

3. The 56 bits of the key are also broken into 2 28 bi halves and each half is rotates one or 2 bit posi Depends on the round.

4. All 56 bits of the key are permutes, producing $K_i$ the key on round i.

5. In this step, is a logic Exclusive-OR, the description of fun F() appears next. then $L_i$ & $R_i$ are Determined by $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$.

6. All 64 bits of a msg are permutes

5) Next header : It indicates type of Extension header that follows the basic header.

6) Hop limit : It shows the max number of routes the packet can travel . (6M)

7) Source & Destination Addresses:
It indicates the Source & Destination address of the packet.

8) Data : This field is the payload portion of the datagram.

7. a. Explain Diffie - hellman key Exchange protocol . Suppose 2 parties A and B wish to set up a common secret key between themselves using Diffi Helmann protocol selecting generator as 3 and prime numbers as 7 . party A choose 2 & party B chooses 5 as their respective secret . Find the Diffie hellman key. .

→ Explanation of Diffie Hellman protocol refer Q.P Feb. Mar - 2022 Q. No: 8. a answer. (5M)

$$\left.\begin{array}{l}
g = 3 \quad a = 7 \quad x_1 = 2 \quad x_2 = 5 \\
y_1 = 3^2 \bmod 7 = 9 \bmod 7 = \boxed{2} \\
y_2 = g^{x_2} \bmod a = 3^5 \bmod 7 = \boxed{5} \\
K_1 = y_2^{x_1} \bmod a = 5^2 \bmod 7 = \boxed{4} \\
K_2 = y_1^{x_2} \bmod a = 2^5 \bmod 7 = \boxed{4}
\end{array}\right\} 5M.$$

8. a. Explain 3 phases of RSA algorithm. For an Encryption of a 4 bit msg '1000' or M = 9 we choose a = 3 & b = 11 Find the public & private keys for this security action and show the Cipher text.

→ For 3 phases of RSA algorithm refer Q.P Feb/Mar-22 7.b. answer.

(5m)

Given data: m = "1000" or M = 9   a = 3   b = 11

Soln: $n = ab = 3 \times 11 = \boxed{33}$

selecting $x = 3$ which is relatively prime to $(a-1)(b-1) = \boxed{20}$

From $x, y \bmod (a-1)(b-1) = 3y \bmod 20 = 1$

$$\boxed{y = 7}$$

public key = $\{3, 33\}$

private key = $\{7, 33\}$

(5m)

Encrypt the message $c = m^x \bmod n$

$= 9^3 \bmod 33 = 3$

$$\boxed{C = 3}$$

Decrypting the message $m = c^y \bmod n$

$= 3^7 \bmod 33$

$$\boxed{M = 9}$$

8. b. Write short on

i) Security Implementation in wireless IEEE 802.11.

The mobility and productivity benefits of 802.11 wireless LAN don't have to put your info assets at risk. while the attention on the pitfalls of WLAN has inspired some Enterprises to ban WLANs altogether, many security - conscious Enterprises are confidently deploying secure WLANs by implementing the following practical steps to protect their info assets & identify vulnerabilities.

1. Discovery & mitigation of Rogue WLANs & vulnerabilities

2. Lock Down all Access points & devices

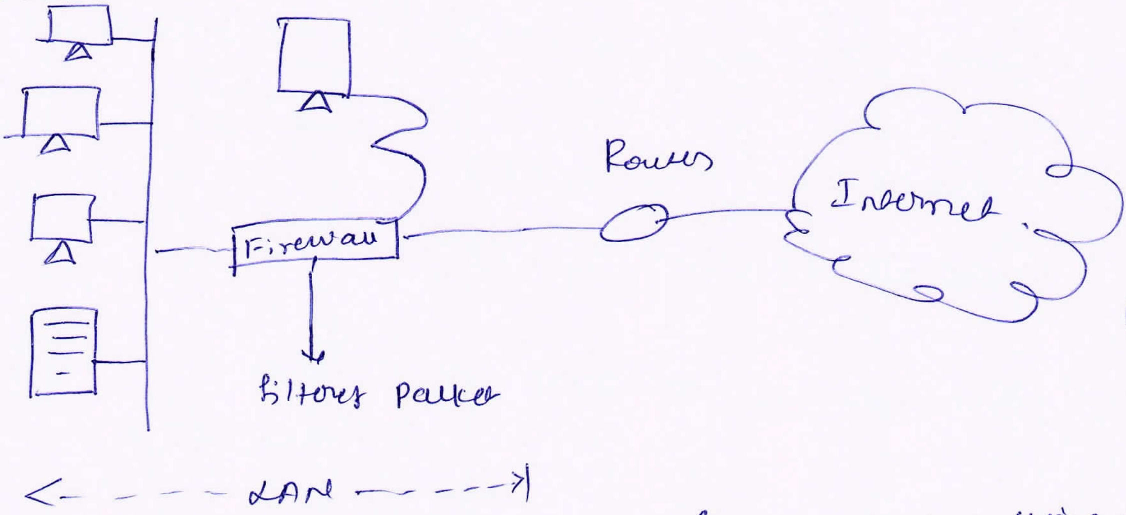
SM

3. Encryption and Authentication (VPN).

4. Set and Enforce WLAN policies.

5. Intrusion detection & protection.

ii) Firewalls.



SM

fig: A simple Configuration of a secured n/w using a firewall

* A firewall can be a S/w program or a H/w device.
* A firewall is a simple router implemented with a special program.
* This unit is placed between hosts of a certain N/w and the outside world. shown in above fig. & the rest of the n/w.
* A firewall is used to protect the n/w from unwanted websites and potential hackers.
° Generally H/w firewalls are more secure compared to S/w firewalls.

9. a. Explain how DNS Redirects a user's request to a CDN Server

→ For answer refer Q.P - Feb/Mar 2022 Question number 9.a answer.

9. b. Explain RTP Basics & RTP packet Header fields.

→ RTP can be used for transporting common formats such as

→ MP3 for sound and
→ MPEG for video.

• It can be used for transporting proprietary sound & video formats.

RTP Basics:

- RTP runs on top of UDP.
- It composed of i) RTP Header ii) Audio chunk.
- The header includes
  i) Type of audio Encoding
  ii) sequence number &
  iii) Timestamp.

RTP Packet Header fields:

fig: RTP header fields.

| | | | | |
|---|---|---|---|---|
| Payload type | Sequence number | Timestamp | Synchronization source identifier | Miscellaneou fields |

1) Payload type:

For an audio-stream, this field is used to indicate type of audio Encoding that is being used.
Ex: PCM

2) Sequence number: It is used by the receiver to detect packet loss and to restore packet sequence.

3) Time Stamp: It reflects the sampling instant of the first byte in the RTP Data packet.

4) Source Identifier (SRC) : • This field identifies the Source of the RTP Stream.

• Typically, Each Stream in an RTP session has a distinct SRC.

10 a. Explain the properties of Audio & video. Also mention the 3 key distinguishing features of Streaming Store & Video

→ properties of Audio.

• PCM is a technique used to change an analog signal to digital Data. digitization.

PCM consist of 1) Encoder at the Sender 2) Decoder at the receiver.

• PCM Encoder.

• Digital audio has lower b.w requirement than video.

• Consider how analog. audio is converted to a Digital signal.

• The analog audio signal is sampled at some fixed rate This referred to as Sampling.

Ex: 8000 samples per second.

• The value of Each sample is an arbitrary real number.

• Each sample is then rounded to one of a finite number of values. This process is called quantization.

This process is called Encoding.

• PCM Decoder:

For playback through audio speakers, the digital -signal can be converted back to an analog-signal.

This process is called decoding.

properties of video.

1) High Bit rate:

The higher the bit-rate

→ better the image quality &

→ better the overall user viewing Experience.

2) Video Compression:

- A video can be compressed, thereby trading off video-quality with bit-rate.

. A video is a sequence of images, Displayed at a ~~compressed~~ constant rate

There are 2 types of redundancy

① Spatial Redundancy.

② Temporal Redundancy.

3 Key distinguishing features of Streaming Stored video.

① Streaming:

The Client begins video playout within few seconds after it begins receiving the video from the server.

② Interactivity:

The media is prerecorded, so the user may pause, reposition or fast-forward through video-content.

③ Continuous playout:

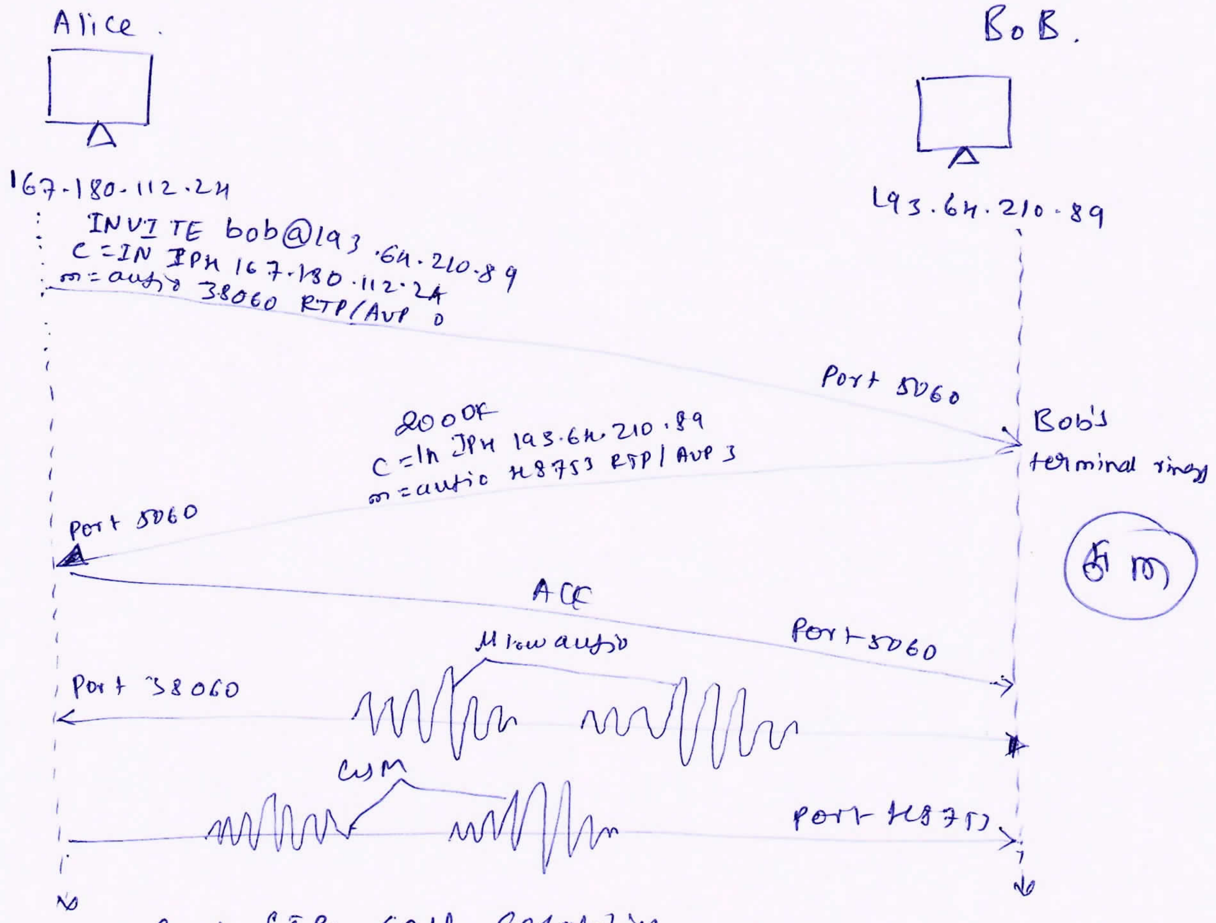
Once playout of the video begins, it should proceed according to the original timing of the recording.

10 b. With neat diagram, Explain Session Initiation Protocol (SIP) Call Establishment.

→ SIP is an open & lightweight protocol.

- It provides mechanisms for establishing calls b/w a caller and a callee over an IP n/w.
- It allows the caller to notify the Callee that it wants to start a call.

4 m



6 m

fig: SIP call Establishment when Alice know Bob's IP address.

The following Events occurs.

① An SIP session begin when Alice sends ~~an~~ Bob an INVITE message

② This INVITE msg is sent over UDP to the well-known port 5060 for SIP.

③ Bob sends an SIP response msg.

③ then, Alice Sends BoB an SIP ack msg.

④ Finally, Bob and Alice ~~[illegible] msg~~ can talk.

⑥

Staff Incharge

HOD

HOD
Computer Science & Engineering
KLS Vishwanathrao Deshpande
Institute of Technology, Haliyal.

Dean Academic

Dean, Academics
KLS VDIT, HALIYAL.