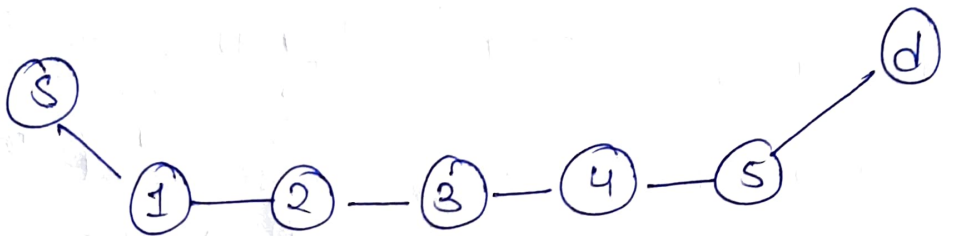07/09/21
Date.

CSPC-53 : CN

CT-01

106119100
Rajneesh Pandey

Question ①

Given

TCP checksum is an end-to-end checksum

So, its computed by source device &
verify by destination devices

therefore,

> Number. of times TCP checksum is
> calculated is one (1).

IP checksum is a node-to-node checksum
It is computed everytime it reaches a
new node

> Hence, Number of times IP checksum is
> calculated is (6) six

Question ②

In the cryptographic technique, Monoalphabetic substitution technique is the substitution type Traditional cipher.

cryptographic technique in which.

the Plain text all the characters shifted to left or right (k) times.

So, for example.

Plain text: TATA and k=3

cipher text: WDWD

Now, if the k=26 then the plain text again become the prev. plain text

hence, we wouldn't achieve the crypto here

hence,

the range of keys (k) = 1 to 25

to apply this technique.

encryption

$E(P) = (P + k) \% \mod 26.$

Decryption

$D(c) = (c - k) \mod 26$

Question ③

Plain text = "rajneeshpandeyrajneeshpand"

Given

Keys : | 5 3 2 6 4 1 |

Applying transposition technique:

PT ⇒

5	3	2	6	4	1
r	a	j	n	e	e
s	h	p	a	n	d
e	y	r	a	j	n
e	e	s	h	p	a
n	d	$	$	$	$
$	$	$	$	$	$

CT ⇒

1	2	3	4	5	6	7
e	j	a	e	r	n	
d	p	h	n	s	a	
n	r	y	j	e	a	
a	s	e	p	e	h	

encryption →

$ → no value.

column.

$$ 6 → 1, 1 → 5, 2 → 3, 3 → 2, 4 → 6, 5 → 4 $$
rowwise encryption:

CT = "ejaernd phnsa nr yjea a sepeh"
$$ \$\$d\$n\$ $$

using key, decryption.

r	a	j	n	e	e
s	h	p	a	n	d
e	y	r	a	j	n
e	e	s	h	p	a
n	d				

Question (4)

A1 : Sends mail to (D1)
(S1) (gmail)

A2 : mail server of (D1) (both server (some)
to store from

A3 : D1 box created a new folder. to store the mail.
S1, S7 downloads the mail.

IMAP.

user agent
D1
Mail server

SMTP →

Internet

M
mail server

user Agent
S1
HTTP
LAN/WAN
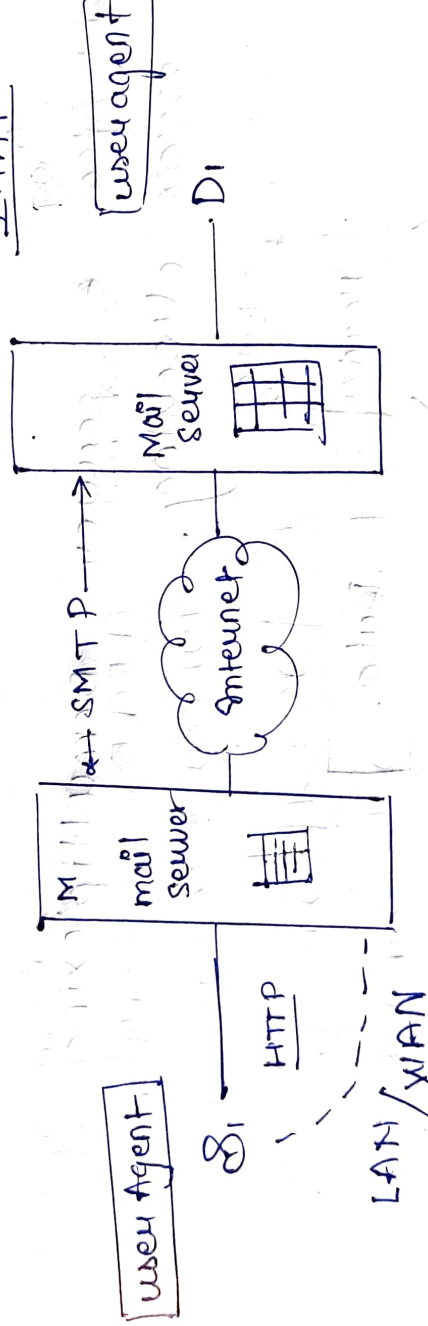
IMAP protocol because
POP 3 doesn't support
creating new forder.
(server).

Question ⑤

(a) <u>UDP (User Datagram Protocol)</u>

Question:

Give the UDP header information.
↳ Beyond IP, UDP provide additional services.

so

UDP Also, • sewer Demultiplexing &
error checking.

fixed size

(b) TCP :

Question
Lets suppose, TCP server an Client running on two different machine.

After completion of data transfer.

TCP client calls close to terminate the connection. A FIN segment is sent to the TCP server. Server-side TCP respond. by sending an ACK which is received by client-side TCP. As per TCP diagram., which state does the client -side TCP connection wait for the FIN from server- side TCP?

Solution

There are two possibility

client receives
Ack for its FIN

client has sent FIN segment but didn't ACK till the time.

so,
the ACK for its own FIN, After. receiving ACK, client will move to TIME - WAIT state.

so, FIN-WAIT - 2