07/09/21
Date.

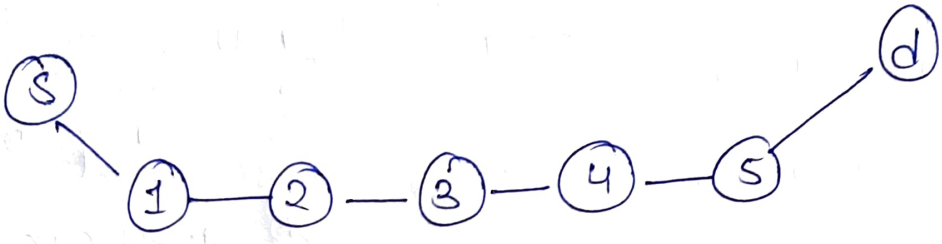
CSPC-53 : CN

CT-01

106119100
Rajneesh Pandey

Question (1)

Given



TCP checksum is an end-to-end checksum

So, it is 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. cryptograpic 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 achive the crypto here

hence,

the range of keys.(K) = 1 to 25

to apply this technique.

Encryption

$E(P) = (P+K) \% \text{ mod } 26.$

Decryption

$D(C) = (C-K) \text{ mod } 26$

Question (3)

plaintext = "rajneeshpandeyrajneeshpand"

Given keys: 5 3 2 6 4 1

Applying transposition technique:

5	3	2	6	4	1
1	2	3	4	5	6

PT ⇒

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	$	$	$	$

encryption →

CT ⇒

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

$ → no value.

Column:

6 → 1, 1 → 5, 2 → 3, 3 → 2, 4 → 6, 5 → 4

rowwise encryption:

CT = "ejaernd phnsa nryjea asepeh $$dn"

using key decryption.

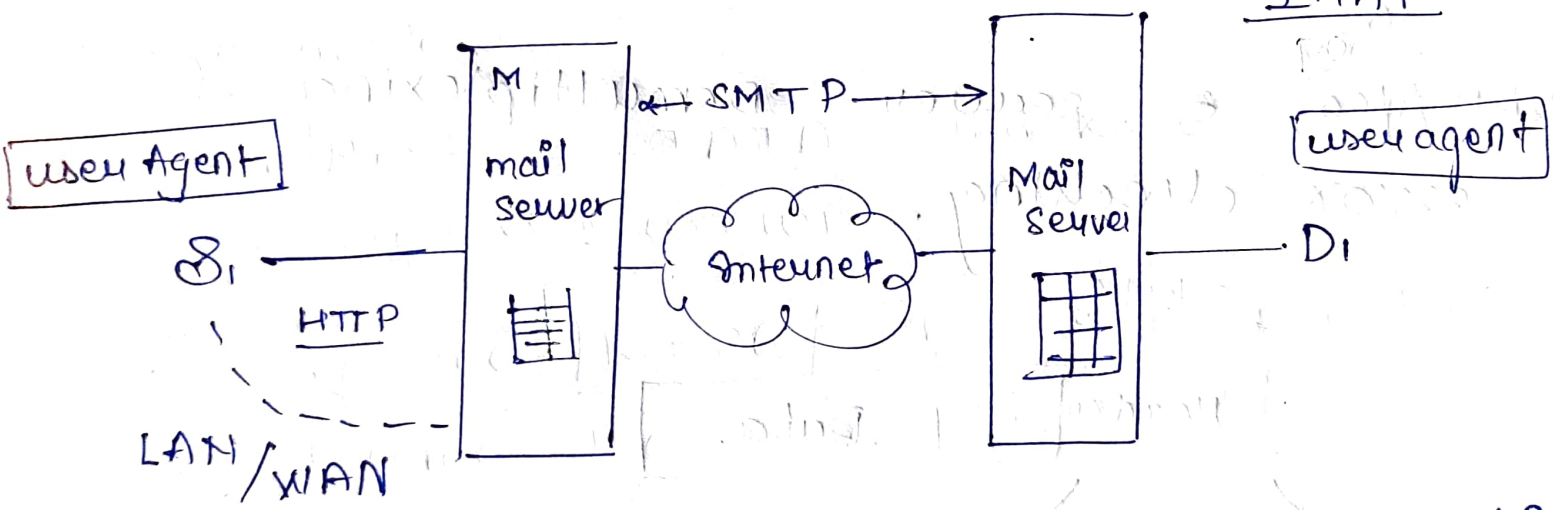
r	a	j	n	e	e
s	h	p	a	n	d
e	y	r	a	j	n
e	e	s	h	p	a
n	d	$	$	$	$

Question (4)

A1 : (S1) sends mail to (D1) (Gmail)

A2 : mail server of (D1) (both servers same)

A3 : D1 has created a new folder. to store from S1, it downloads the mail.



IMAP protocol because pop3 doesn't support creating new forders. service.

Question (5)

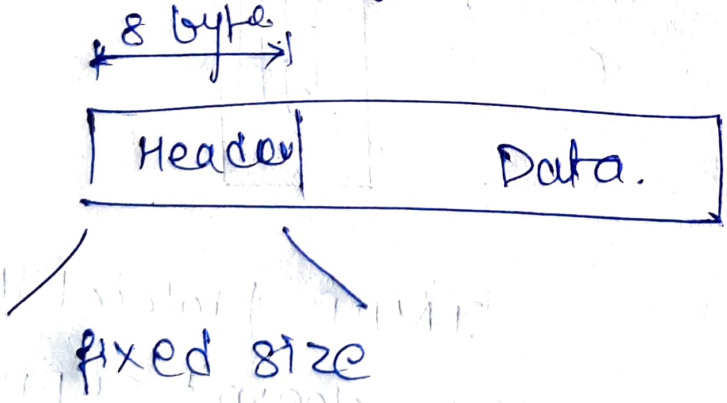
(a) UDP (User Datagram Protocol)

Question:

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

So

UDP Also, • server Demultiplexing & error checking.



(b) TCP :

Question

Lets suppose, TCP server an client running on two differerent machine.

After completion of data transfer. TCP client calls close to terminate the connection. A FIN segment is sent to the TCP server. Severer-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.