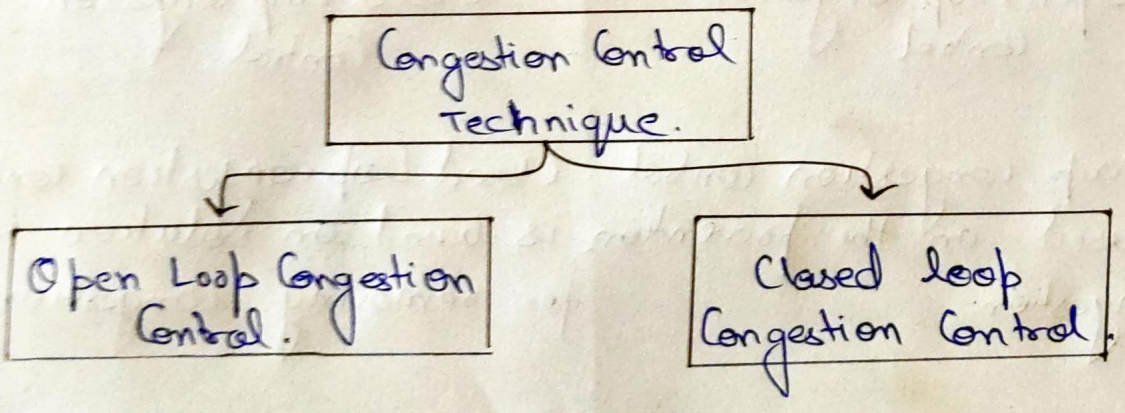
Name : Abhishek Srivastava
Reg No : 19BCE10071
Subject : Computer Networks
Slot : A11 + A12 + A13
Date : May 5, 2022.

Term End Examination.

Q2] (b)

Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be widely classified into two categories:



Open Loop congestion control policies are applied to prevent congestion before it happens. The congestion control is either handled by the source or the destination.

Close Loop congestion control is used to treat or alleviate congestion after it happens. To solve the issue there are several techniques used by different protocals.

Difference between open Loop congestion control and closed loop congestion control.

Open Loop Congestion Control.	Closed Loop Congestion Control.
Open loop congestion control is based on the prevention of congestion.	Closed Loop congestion control is based on solution for removing congestion.
It prevents congestion from happening.	It removes congestion after it took place.
It does not need an end-to-end feedback.	It adjust its data rate depending on some kind of feedback.

Mechanism are as follows:

i. Retransmission policy.
ii. Window policy.
iii. Acknowledgement policy.
iv. Admission policy.

Mechanism are as follows:

i. Back pressure
ii. Choke packet
iii. Implicit Signaling.
iv. Explicit Signaling.

1] a)

In general if it is a problem of Network bad enough to corrupt at the transport Layers 2 level, then the senders address is also corrupt. This is because the way a CRC checksum works.

When a packet arrives malformed the ~~the~~ checksum just tells the receiver the data is garbage, and the packet get tossed.

There is no way of an intermediate router to figure out the senders address at this point because the entire packet with both the senders and recievers address cannot be trusted, hence the packet is thrown out.

As another communication points out, TCP will retry based on the fact that it didnt received an acknowledgement (ACK), but

this is like waiting for a but which does not show up, so we will never know what happened to the bus (packet).

Unless the corruption caused by CRC for the packet to be valid, the packet would be discarded. With TCP, the sender would be timed out on the missing acknowledgement, and retransmit the packet. With UDP, the lost packet would not be detected as missing unless a higher level such as application spotted the loss.

4]

Minimum frame size is needed to ensure that collisions are detected properly. The minimum frame size ensures that before a frame is completely send, it ~~wo~~ would be notified of any possible collisions and hence collision detection works perfectly.

CSMA/CD can detect collision if below condition is satisfied:

$$TT \geq 2 * PT,$$

where TT = Transmission time
PT = Propagation time.

We know that,

$$TT = \frac{\text{Datasize}}{\text{Bandwidth}}, \text{ and}$$

$$PT = \frac{\text{Distance}}{\text{Velocity}}.$$

Given,

Bandwidth = 10^9 mbps

Velocity = 2×10^5 m/s

Therefore,

$$\frac{\text{Distance}}{\text{Bandwidth}} \geq 2 * \frac{\text{Distance}}{\text{Velocity}}$$

$$\frac{\text{Datasize}}{10^9} \geq \cancel{2} * \frac{1000}{\cancel{2} \times 10^5}$$

$$\text{Datasize} \geq \frac{10^{12}}{10^5}$$

$$\text{Datasize} \geq 10^7$$

Therefore. Minimum frame size $= 10^7$ or 10000000

Answer

3] a)

Symmetric Key Encryption.

Encryption is a process to change the form of any message in order to protect it. from reading by anyone. In Symmetric key Encryption, the message is encrypted using a key and the same key is used to decrypt the message. which makes it easy to use but less secure. It also requires a safe method to transfer key from one party to another.

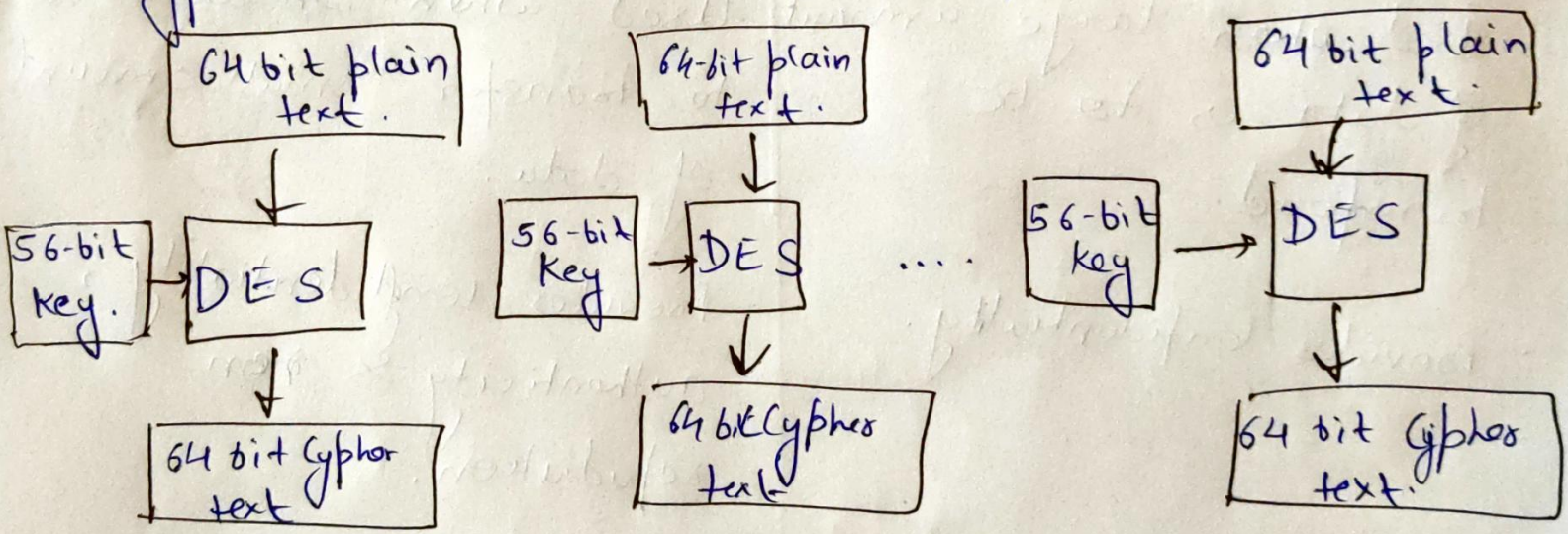
Asymmetric Key Encryption.

Asymmetric Key Encryption is based on public and private key encryption techniques. It uses two different keys to encrypt and decrypt the messages. It is much secure than Symmetric but slowed also well.

Symmetric Key Encryption.	Asymmetric Key Encryption.
• It requires single key for encryption and decryption.	• It requires two different keys for encryption and decryption.
• The size of cipher text is same or smaller than original text.	• The size of cipher text is same or larger than original text.
• Encryption is fast.	• Encryption is slow.
• Used when large amount of data is to be transfered.	• Used when we have to transfer small amount of data.
• Provides Confidentiality.	• Provides confidentiality, authenticity & non-repudiation.
• Eg: AES, DES, RC4, etc	• Eg: RSA, DSA, ECC, etc.

Data Encryption Standard. (DES)

It is a block cipher algorithm that takes plain text in blocks of 64 bits and converts them to cypher text using keys of 48 bits. It is a symmetric key algorithm, which means the same key is used to encrypt and decrypt the data, with minor differences.



DES is based on two fundamental attributes of cryptography:

1) Substitution [Confusion]
2) Transposition [Diffusion]

DES consists of 16 steps which are called as Rounds. And in each round the substitution and transposition steps are performed.

Here are the steps :-

1) The 64 bit plain block is handed over to an Initial permutation function.
2) Initial permutation is performed on plain text.
3) It produces two halves of the permuted block, says Left plain text (LPT) and Right plain text (RPT).
4) LPT and RPT go through 16 round of encryption process.
5) LPT and RPT are joined at the end and final permutation (FP) is performed.
6) Result of this process produces 64 bit cipher text.

5]

Here are the steps that occur when we type a URL in the Web browser.

1) You enter URL in a web browser
2) Browser look up the IP address via the Domain Name using DNS.
3) Browser sends an HTTP request to the server.
4) server sends back an HTTP response.
5) The Browser begins rendering the HTML.
6) Browser sends request if there are any additional element embedded in HTML like Images, Javascript, CSS.
7) Once the Page is loaded, the browser sends further request if needed.

So when we type "www.vithbhopal.ac.in" into our browser, the first thing that happens is a Domain Name Server matches "vithopal.ac.in" to an IP address.

Then the browser sends an HTTP request to the ~~ve~~ server and gets a response. The browser starts rendering VIT Bhopal HTML page while also requesting other static content like Images, CSS, JS. Then the Page is fully Loaded.