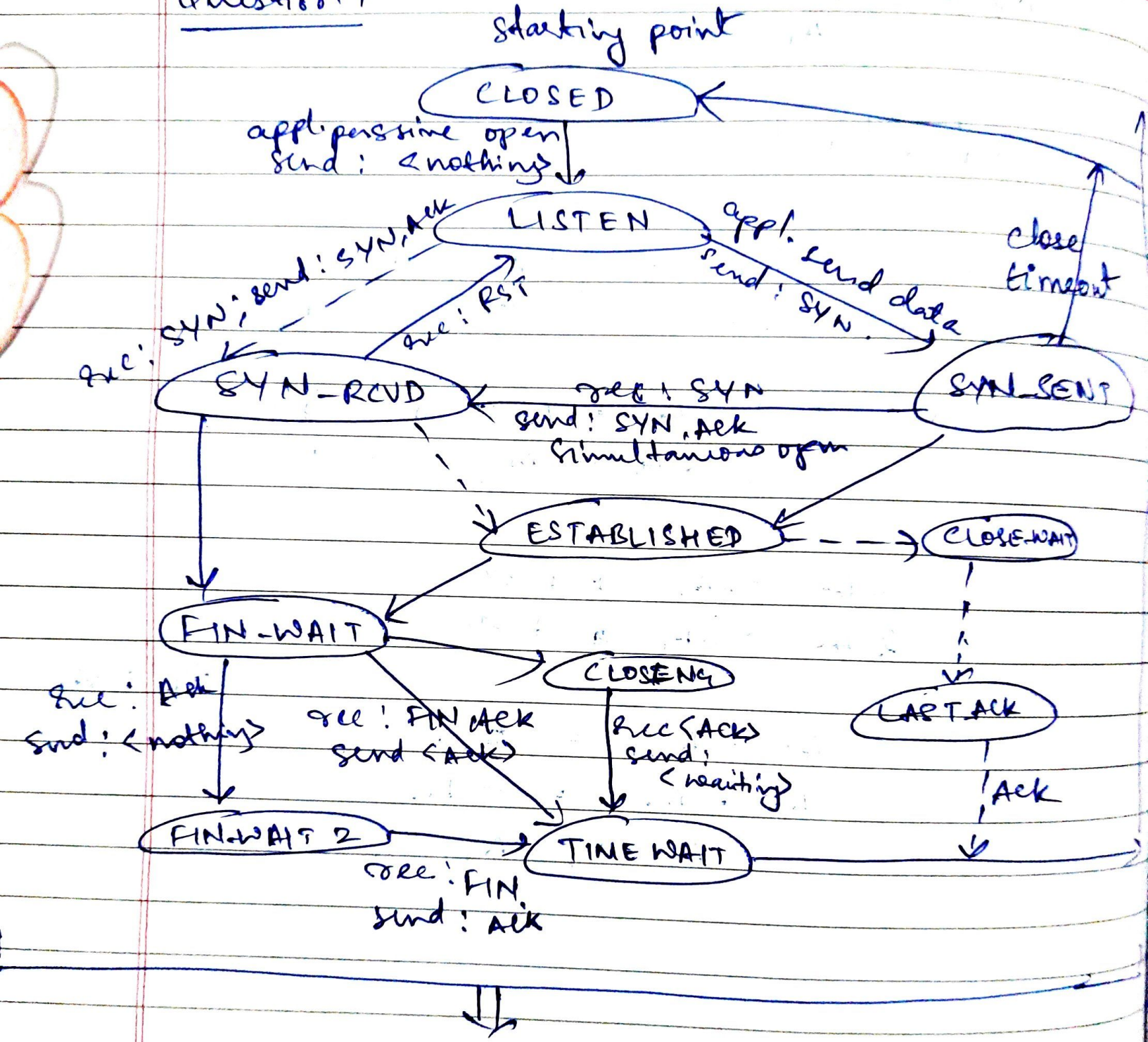
DIGITAL ASSIGNMENT - 1
Network & Communication.

Name : Kulvir Singh

Reg No. : 19BLE2074.

Question 1



TCP State Transition Diagram.

The figure shows 2 FSMs used by the TCP client and server combined in one diagram. The ovals represent the state and the transition from one state to other is shown using directed lines.

The dotted lines in the figure represent the transition that a server normally goes through, the solid lines show the transitions that a client normally goes through.

→ Closed :-
No connection exists

→ LISTEN :-
Passive open recieved, waiting for SYN

→ SYN-SENT :-
SYN sent, waiting for ACK

→ ESTABLISHED :
connected, data transfer in progress.

→ FIN-WAIT 1 :
First FIN sent, waiting for ACK

→ FIN-WAIT 2 :
ACK to first FIN recieved, ~~and~~ waiting for second FIN.

→ CLOSE-WAIT :
First FIN recieved, ACK sent, waiting for application to close

→ TIME-WAIT :
Second FIN recieved, ACK sent, waiting for 2MSL timeout.

→ LAST-ACK :
Second FIN sent, waiting for ACK.

→ CLOSING :
Both sides decided to close simultaneously.

Question 2

In SCTP - multi streaming, FTP controls and data connections are combined on a single multistreamed SCTP association. That is only one association exists for the entire multiple file FTP session. An FTP client establishes an ~~SCTP~~ SCTP association with the server with two streams opened in each direction. The clients and the server send controlled information on their respective streams 0. All data are transfered over their respective stream 1. This approach maintains semantics for streams analogous to control and data connections in FTP over TCP.

To detect EOF using one SCTP associations, the SIZE command is used. The SIZE command is already widely used in FTP for the purpose of detecting restart markers. The end of data transfers is detected using the no. of bytes read by receiving call provided by STCP socket API.

For a multiple file retrieval, the client sends out requests on outgoing streams 0 and receives the files sequentially on incoming stream 1.

Question 3

Internet congestion is the reduced quality of service that occurs when a network node or link is carrying more data than it can handle. Effects include queuing delay, packet loss or the blocking of new connections.

Mechanisms to prevent network congestion or to deal with a network collapse :-

(i) Network scheduler - active queue management which selectively drops packets in the presence of congestion.

(ii) Explicit Congestion Network - an extension to IP & TCP communications protocols that adds a flow control mechanisms.

(iii) TCP congestion control uses a network congestion - avoidance algorithm.

Techniques to improve the quality of service:

a) Scheduling: Packets from different flows arrive at a switch or router for process. A good scheduling Tech. treats the different flows in a fair & appropriate manner.

b) Traffic shaping:
Mechanism to control the amount of traffic & rate of traffic sent to the network.

c) Resource Reservation:
Quality increases if resources are reserved before hand!

d) Admission Control.

Question 1

Layered communication typically separates communication tasks into several layers, with a clear description of the functionality of each layer. In a layered communication stack, interaction among layers occurs through well defined standardised interfaces in a strictly layered communication stack.

In contrast, cross-layer approaches attempt to exploit a richer interaction among communication layers to achieve performance gains. Protocol design by the violations of a reference layered communication architecture is cross-layer w.r.t. the particular layered architecture

Functions of Application Layer-

→ Network Virtual Terminal

→ File Transfer, Access & Management (FTAM)

→ Addressing

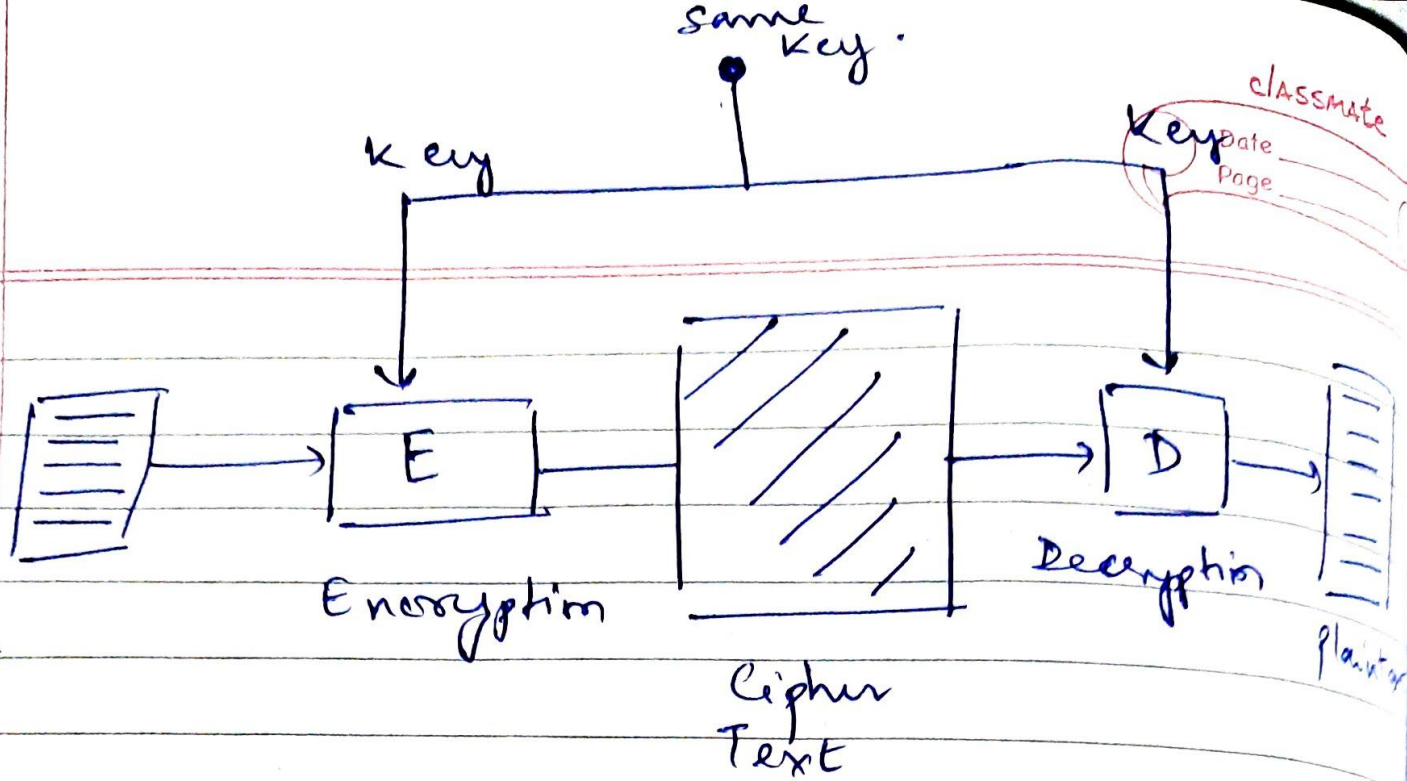
→ Mail, Email services

Question 5

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Symmetric Encryption

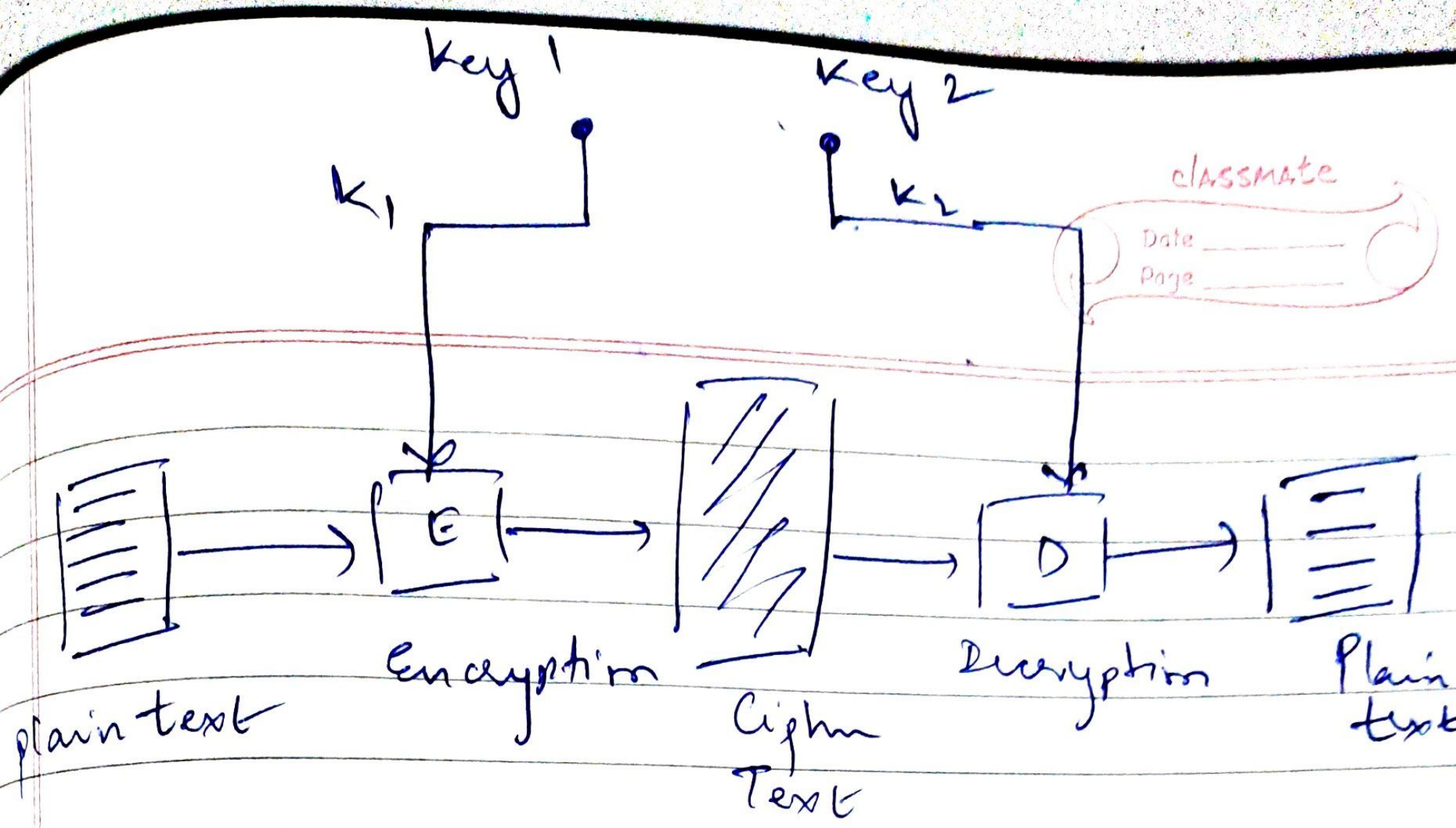
→ Requires a single key for both encryption and decryption.
→ The size of ciphr text is same or smaller than the original text
→ Encryption process is fast
→ Used when large amount of data is required to transfer.
→ provides only confidentiality.



SYMMETRIC ENCRYPTION

Assymmetric Encryption

→ Requires 2 keys, one to encrypt and one to decrypt
→ Size of cipher text is same or larger than plain text
→ Encryption process is slow
→ used to transfer small amounts of data
→ provides confidentiality, authenticity and non-repudiation.



~~ASYMMETRIC~~

ASYMMETRIC

ENCRYPTION