**Class A:** Starts with 1-126. Major networks. N.H.H.H

**Class B:** Starts with 128-191. Large networks. N.N.H.H

**Class C:** Starts with 192-223. Small networks (easy to get). N.N.N.H

**Class D:** Starts with 224-239. Multi-cast addresses.

**Class E:** Starts with 240-254. Experimental addresses.

**Class A** has subnet mask 255.0.0.0 or /8,

**Class B** has subnet mask 255.255.0.0 or /16 and

**Class C** has subnet mask 255.255.255.0 or /24.

**For example**, with a /16 subnet mask, the network 192.168.0.0 may use the address range of 192.168.0.0 to 192.168.255.255. Network hosts can take any address from this range; however, address 192.168.255.255 is reserved for broadcast within the network.

**7 LAYESERS OF ISO / OSI MODEL**

**1.PHYSICAL LAYER:-**

**2.DATA LINK LAYER:-**

A **bridge** operates at the data link layer, giving it access to the physical address of all stations connected to it. Answer is physical addresses.

**MAC**(Media Access Control) and **LLC**(Logical Link Control) are the sublayer of DATA LINK LAYER

**3. NETWORK LAYER:-**

**4.TRANSPORT LAYER:-**

**5.SESSION LAYER :-**

This layer establishes, maintains, and synchronizes the interactions between communicating devices.

**6.PRESENTATION LAYER :-**

This layer ensures interoperability between communicating devices through transformation of data into a mutually agreed upon format.

**7.APPLICATION LAYER:-**

**10 BASE T DEFINITION :-**

**The number 10**: At the front of each identifier, 10 denotes the standard data transfer speed over these media - ten megabits per second (10Mbps).

**The word Base**: Short for Baseband, this part of the identifier signifies a type of network that uses only one carrier frequency for signaling and requires all network stations to share its use.

**The segment type or segment length**: This part of the identifier can be a digit or a letter:

**Digit** - shorthand for how long (in meters) a cable segment may be before attenuation sets in. For example, a 10Base5 segment can be no more than 500 meters long.

**Letter** - identifies a specific physical type of cable. For example, the

**T** at the end of 10BaseT stands for twisted-pair.

**10Base2**—An Ethernet term meaning a maximum transfer rate of 10 Megabits per second that uses baseband signaling, with a contiguous cable segment length of 100 meters and a maximum of 2 segments.

A 10 BASE-2 network is limited to 30 stations per segment.

**10Base5**—An Ethernet term meaning a maximum transfer rate of 10 Megabits per second that uses baseband signaling, with 5 continuous segments not exceeding 100 meters per segment.

**10BaseT**—An Ethernet term meaning a maximum transfer rate of 10 Megabits per second that uses baseband signaling and twisted pair cabling.

Bits per second = baud per second x the number of bits per baud.

**Hot Potato Routing:** When a packet comes to a node, it tries to get rid of it as fast as it can, by putting it on the shortest output queue without regard to where that link leads.

**Serial Communications**

****

**Data bits:-**Real chunk of data

**Synchronization bits** :- The synchronization bits are two or three special bits transferred with each chunk of data. They are the start bit and the stop bit(s).

**Parity bits** : - It is for low-level error checking.

**Star topology**

A star topology is a topology for a Local Area Network (LAN) in which all nodes are individually connected to a central connection point, like a hub or a switch

**Bus topology**

A bus topology is a topology for a Local Area Network (LAN) in which all the nodes are connected to a single cable.

**Hub**

Hub is a basic Network Device that sent data from one network device and sent to all devices because Hub is a broadcasting device.

**Switch**

Switch is a unicasting device and sent data to particular another device according to MAC address

**Bridges**

A bridge is a computer networking device that builds the connection with the other bridge networks which use the same protocol. It works at the Data Link layer of the OSI Model and connects the different networks together and develops communication between them. It connects two local-area networks; two physical LANs into larger logical LAN or two segments of the same LAN that use the same protocol.

**Routers**

Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. It has the ability to connect dissimilar LANs on the same protocol

**SLIDING WINDOW PROTOCOL :-**

1. **GO BACK N**

Maximum Window Size = Sequence Number Space – 1

http://www.cse.iitk.ac.in/users/dheeraj/cs425//lec09.html

1. **SELECTIVE REPEAT**

Maximum Window Size = Sequence Number Space / 2

**X.25** is a standard suite of protocols used for packet switching across computer networks. The X.25 protocols works at the physical, data link, and network layers (Layers 1 to 3) of the OSI model.

**Question** :-

A packet has arrived with an M bit of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

**Solution**:

If the M bit is 0, it means that there are no more fragmentations; the fragment is the last one. However we cannot say if the original packet was fragmented or not. A non-fragmented packet is considered the last fragment.

**Question** :-

A packet has arrived with an M bit of 1. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

**Solution**:

If M bit is 1, it means that there is at least one more fragment. This fragment can be the first one or the middle one, but not the last one. More information is needed to say whether it is the first or middle one but we can say that the original packet was fragmented because the M bit vale is 1.

**Question** :-

A packet has arrived with an M bit of 1 and a fragmentation offset value of zero. Is this the first fragment, the last fragment, or a middle fragment?

**Solution**:

As the M bit is 1, it is either a first or a middle fragment. Since the offset is 0, it is supposed to be first fragment.

**Round-trip delay time(RTD)** or **Round-trip time (RTT)** is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received.

**Bandwidth Delay Product :-**

The most optimal window size depends on the bandwidth and delay of the link, we call this the bandwidth delay product. We can calculate it with the following formula:

Bandwidth Delay Product = bandwidth (bits per sec) \* round trip time (in seconds)

**ROUND TRIP DELAY:-**

The round-trip delay time (RTD) or round-trip time (RTT) is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received.

**BIT RATE AND BAUD RATE :-**

The bit rate measures the number of bits transmitted per second,

whereas the baud rate measures the number of symbols transmitted per second

A baud Rate is the number of times per second a signal in a communications channel changes.

and that is the major difference between the two

The baud rate will equal the bit rate only when there is just one bit per symbol.

Bit rate is the number of bits per second. Baud rate is the number of signal

units per second. Baud rate is less than or equal to the bit rate.

Baud rate determines the bandwidth required to send signal

Baud rate = bit rate / # bits per signal unit

***Ques:- An analog signal carries 4 bits in each signal unit. If 1000 signal units are sent per second, find the baud rate and the bit rate?***

**Ans:-**Baud rate = 1000 bauds per second (baud/s) Bit rate = 1000 x 4 = 4000 bps

***Ques:-The bit rate of a signal is 3000. If each signal unit carries 6 bits, what is the baud rate?***

**Ans:-**Baud rate = 3000/6 =500 bauds/sec

**HIERARCHICAL ROUTING WITH MINIMIZE THE ROUTING SIZE :-**

Clusters \* regions \* routers = 4800 for all options

so we use following

(clusters- 1) + (regions - 1) + routers , which option gives minimum is the answer

***Ques :- For n devices in a network, what is the number of cable links required for a mesh, ring, bus, and star topology?***

**Ans**: n(n-1)/2 cable link are required for mesh, n for ring, n-1 cable link for bus, and n cable link for star topology

**Internet Protocol Version 4 (IPv4)**

* It is a connectionless protocol
* This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model.
* Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.

**DATA FORMAT IN TCP/IP MODEL**

data unit in application layer is called data or message.

data unit in transport layer is called segment.

data unit in network layer is called packet.

data unit in data link layer is called frame.

data unit in physical layer is called bits.

**TCP HEADER FORMAT :-**



**FIN**: No more data from the sender. Receiving a TCP segment with the FIN flag does not mean that transferring data in the opposite direction is not possible.

**RST**: Reset the connection. The RST bit is used to RESET the TCP connection due to unrecoverable errors.

**SYN**: This flag means synchronize sequence numbers. Source is beginning a new counting sequence.

**PSH**: This flag means Push function. Using this flag, TCP allows a sending application to specify that the data must be pushed immediately.

**Congestion control algorithms -**

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

**Leaky Bucket Algorithm-**

Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.

1.When host wants to send packet, packet is thrown into the bucket.

2.The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.

3.Bursty traffic is converted to a uniform traffic by the leaky bucket.

4.In practice the bucket is a finite queue that outputs at a finite rate.



**Token bucket Algorithm :-**

Need of token bucket Algorithm:-

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket ƒ.

2. The bucket has a maximum capacity ƒ

3. If there is a ready packet, a token is removed from the bucket, and the packet is send.

4. If there is no token in the bucket, the packet cannot be send.



Let’s understand with an above example,

In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

Let’s understand with an example,

**Tunnel and Transport Modes:-**

**IPSec** can be run in either tunnel mode or transport mode.

**Tunnel mode** is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.

**Transport mode** is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host—for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.

**Shannon-Hartley Channel Capacity Theorem :-**

Shannon-Hartley equation relates the maximum capacity (transmission bit rate) that can be achieved over a given channel with certain noise characteristics and bandwidth

Here C is the maximum capacity of the channel in bits/second otherwise called Shannon’s capacity limit for the given channel,

B is the bandwidth of the channel in Hertz,

S is the signal power in Watts and N is the noise power, also in Watts.

The ratio S/N is called Signal to Noise Ratio (SNR).



**Nyquist Criteria for maximum data rate for noiseless channels**

C = 2 \* B \* log M

where C is the channel capacity in bits per second or data rate,

B is the maximum bandwidth allowed by the channel,

M is the number of different signaling values or symbols

log is to the base 2

For example, assume a noiseless 3-kHz channel.

1. If binary signals are used, then M= 2 and hence maximum channel capacity or achievable data rate is

C = 2 \* 3000 \* log 2 = 6000 bps.

2. Similarly, if QPSK is used instead of binary signaling, then M = 4. In that case,

the maximum channel capacity is C = 2 \* 3000 \* log 4 = 2 \* 3000 \* 2 = 12000bps

**Maximum data rate of a channel for a noiseless 3-kHz binary channel is**

Maximum data rate = 2 H log2 V bps,

where H is the bandwidth,

V is the discrete levels.

Here H is 3 kHz and V is 2.

So, data rate = 2\*3000 log2 bps = 6000 bps.

**Shannon’s channel capacity criteria for noisy channels**

Given a communication channel with bandwidth of B Hz. and

a signal-to-noise ratio of S/N,

where S is the signal power and

N is the noise power, Shannon’s

the maximum channel capacity or data rate C of such a channel is

***C = B log (1 + S/N)***

For example, for a channel with bandwidth of 3 KHz and with a S/N value of 30 DB,

like that of a typical telephone line,

the maximum channel capacity is C = 3000 \* log (1 + 30) = 30000 bps (approx.)

**RSA Algorithm:-**

**---------------------**

\*) Given data p, q, d, plain text

\*) n = p \* q

\*) m = (p-1) \* (q-1)

\*) Choose any integer, e, such that GCD(e, ((p-1) \* (q-1))) = 1 (ie., co prime to m )

\*)Find a small odd integer e, that is relatively prime to m. If e=3, then GCD(e,m)=1

\*) Encrypt Message E(s) = se mod n

\*) Find d, such that de % m = 1

\*) Decrypt Message E(s) = encryptedd mod n

http://pajhome.org.uk/crypt/rsa/rsa.html

**Cyclic Redundant Check (Sender Side)** :-

n : Number of bits in data to be sent from sender side.

k : Number of bits in the key obtained from generator polynomial.

1.The binary data is first augmented by adding k-1 zeros in the end of the data.

2.Use modulo-2 binary division to divide binary data by the key and store remainder of division.

3.Append the remainder at the end of the data to form the encoded data and send the same

Sample Example is shown below,



The process of modulo-2 binary division is the same as the familiar division process we use for decimal numbers. Just that instead of subtraction, we use XOR here.

**HAMMING CODE :-**

The minimum Hamming distance is 2t + 1, the code can correct up to t errors.

Let C be a binary linear code with minimum distance 2t + 1 then it can correct upto t bits of error.

For error detection, formula is t+1.

The Hamming Distance is a number used to denote the difference between two binary strings.

String 1: "1001 0010 1101"

String 2: "1010 0010 0010"

Number of difference is 6. So hamming distance is 6.

**Huffman Code Generation(Greedy Technique) :-**

It is a lossless data compression algorithm. The idea is to assign variable-legth codes to input characters, lengths of the assigned codes are based on the frequencies of corresponding characters. The most frequent character gets the smallest code and the least frequent character gets the largest code

the following general procedure has to be applied:

-search for the two nodes providing the lowest frequency, which are not yet assigned to a parent node

-couple these nodes together to a new interior node

-add both frequencies and assign this value to the new interior node

-The procedure has to be repeated until all nodes are combined together in a root node.

- For symbol can be computed in O( n log n ) times

- refer https://www.youtube.com/watch?v=YVU2dgPZFAA

**Example:** "abracadabra"

Symbol Frequency

a 5

b 2

r 2

c 1

d 1

****

**Encoding :-**

The original data will be encoded with this code table as follows:



encoded data: 23 Bit

original data: 33 Bit

**Decoding :-**

For decoding the Huffman tree is passed through with the encoded data step by step. Whenever a node not having a successor is reached, the assigned symbol will be written to the decoded data.



**Time complexity**: O(nlogn) where n is the number of unique characters. If there are n nodes, extractMin() is called 2\*(n – 1) times. extractMin() takes O(logn) time as it called minHeapify(). So, overall complexity is O( n log n ).

Given the following probability table, create a Huffman tree to encode each symbol.

Symbol A B C D E

Probability 0.3 0.3 0.2 0.1 0.1



**SLOTTED ALOHA :-**

Throughput, S = G e-G,

where G = Number of frames per T

T = Transmission time

**Pure ALOHA**

One of the newly discovered algorithms-protocols for allocating a multiple access channel is ALOHA. The idea is simple. Users transmit whenever they have data to be sent. Frames are destroyed when collision occurs. When a sender detects a collision waits for a random amount of time and retransmits the frame. With this method the best theoretical throughput and channel utilization we can have is 18%. Term throughput means the amount of work that a computer can do in a given time period

**Slotted ALOHA**

In slotted ALOHA time is divided into discrete intervals, each corresponding to one frame. A computer is not permitted to send whenever it has data to send. Instead it is required to wait for the next available slot. The best it can be achieved is 37% of slots empty, 37% success and 26% collision.



**IP DATAGRAM FRAGMENTATION FIELDS :-**

1. Identification: Identification number helps destination identification number helps destination in reassembling datagram

All fragments of this datagram will copy the same Identification

2. Flags: 3-bit field as shown:

1st bit is reserved

2nd bit is called “do not fragment do not fragment” bit

-if its value is 1, machine must NOT fragment datagram

3rd bit is called “more fragment more fragment” bit

- if its value is 1, datagram is not last fragment, there are more fragments after this one, either first or middle

- if its value is 0, this is last or only fragment

- M bit is 1, and the offset value is 0, then it is the first fragment.

*3. Fragmentation Offset: a 13-bit field, specifies the position of the fragment*

*in the original datagram in multiples of 8 bytes.*

**FIREWALL DUTIES LAYERWISE:-**

Layer 3 firewalls (i.e. packet filtering firewalls) filter traffic based solely on source/destination IP, port, and protocol.

Layer 4 firewalls do the above, plus add the ability to track active of network connections, and allow/deny traffic based on the state of those sessions (i.e. stateful packet inspection).

Layer 7 firewalls (i.e. application gateways) can do all of the above, plus include the ability to intelligently inspect the contents of those network packets. For instance, a Layer 7 firewall could deny all HTTP POST requests from Chinese IP addresses. This level of granularity comes at a performance cost, though.

**VLAN ( VIRTUAL LOCAL AREA NETWORK )**

In a layer 2 switched network, each network segment has its own collision domain and all segments are in same broadcast domain. Every broadcast is seen by every device on the network. A layer 3 device (typically a Router) is used to segment (divide) a broadcast domain to multiple broadcast domains.

**BIT STUFFING:-**

after 5 consecutive 1-bits, a 0-bit is stuffed.

Input bit sequence: 110101111101011111101011111110 (without bit stuffing)

Result bit sequence: 110101111100101111101010111110110 (with bit stuffing)

Eg)A bit-stuffing based framing protocol uses an 8-bit delimiter pattern of 01111110. If the output bit-string after stuffing is 01111100101, then the input bit-string is : 0111110101

**LAYER AND ITS PROTOCOL**:-

**Transport Layer:-**

TCP -> Transmission control protocol

UDP -> User Data Protocol

**Network Layer** : ICMP(Internet Control Message Protocol)

RIP ->Routing information protocol

OSPF -> Open shortest path first

IP -> Internet protocol

BGP(Border gateway protocol) -> It is a routing protocol.

EGP(Exterior gateway protocol) -> It is a vector routing protocol.

**Data Link Layer** :

ARP(Address Resolution protocol)

Resolve IP address to the corresponding Ethernet address.

RARP, DHCP, BOOTP(Three are same)

Resolve Data Link Layer Address to Network Layer Adddress

Resolve Ethernet MAC address to IP address

PPP(point to point protocol)

**Application Layer :**

SMTP -> Simple Mail Transfer Protocol

POP -> Post Office Protocol

IMAP -> Internet Message Access Protocol

SNMP -> Simple Network management Protocol

HTTP -> Hyper text transfer protocol

**Security Protocol** : PGP(pretty good privacy) is a popular program used to encrypt and decrypt email over the Internet, as well as authenticate messages with digital signatures and encrypted stored files.

**SMTP Protocol:**

-It is used by the Mail Transfer Agent (MTA) to deliver your eMail to the recipient's mail server.

-The SMTP protocol can only be used to send emails, not to receive them.

-Send an email from a mail client to a mail server

**POP(Post office protocol):-**

-Download an email from mailbox server to a mail client

-provides a simple, standardized way for users to access mailboxes and download messages to their computers.

**IMAP(Internet Message Access Protocol):-**

It is an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection

It is a client/server protocol in Protocol which e-mail is received and held for you by your Internet server

**Secure Electronic Transaction (SET) Protocol:-**

It is for secure credit card payment.

**Attenuation:-**

Reduction of signal strength during transmission. Attenuation is the opposite of amplification.

What Causes Attenuation?

Noise, Physical surroundings, Travel distance

**FDDI (Fiber Distributed Data Interface)** is a set of ANSI and ISO standards for data transmission on fiber optic lines in a local area network (LAN) that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol.

**Token Ring local area network (LAN)** technology is a communications protocol for local area networks. It uses a special three-byte frame called a "token" that travels around a logical "ring" of workstations or servers.



**Digital-to-Digital Conversion**

convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

**(I)Line Coding**

The process for converting digital data into digital signal is said to be Line Coding.

**(II)Block Coding**

To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding. It is normally referred to as mB/nB coding. It replaces each m-bit group with an n-bit group.

**(III)Scrambling**

Provides synchronization without increasing number of bits.

**asynchronous transmission:-**

In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (1s) at the end of each byte. There may be a gap between each byte.

**synchronous transmission:-**

In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits. Timing is very important because the accuracy of the information depends on an accurate counts of the number of bits received.

**PULSE CODE MODULATION:-**

PCM is one of the most commonly used method to convert analog data into digital form. It involves three steps:

**Sampling:-**

The analog signal is sampled every T interval. Most important factor in sampling is the rate at which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.



**Quantization:-**

Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.



**Encoding:-**

In encoding, each approximated value is then converted into binary format.



**What services does the internet layer provide?**

1.The internet layer packs data into data packets known as IP datagrams

2.Contain source and destination address information that is used to forward the datagrams between hosts and across networks.

3.The Internet layer is also responsible for routing of IP datagrams

4.The protocols include IP (Internet Protocol), ICMP (Internet Control Message Protocol),ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol)

**CSMA ACCESS MODES**

**1-persistent :-**

In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.

• If the channel is busy, the station waits until it becomes idle.

• When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called I-persistent CSMA.

**P-persistent :-**

• This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.

• Whenever a station becomes ready to send, it senses the channel.

• If channel is busy, station waits until next slot.

• If channel is idle, it transmits with a probability p.

**O-persistent :-**

**Non-persistent:-**

• In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval oftime.

• After this time, it again checks the status of the channel and if the channel is.free it will transmit.

**Non persistent method:-**

– If the medium is not idle, wait a random amount time and then senses again

– Reduce collision, reduce network efficiency

**Persistent method:-**

– If the medium is not idle, continuously sense the medium.

– p-Persistent method

**p-Persistent CSMA:-**

– Listen to the medium

– If there is no activity, transmit; otherwise, continue to monitor the medium.

– When the medium becomes idle, transmit with a probability p;

otherwise wait for the next time slot (probability 1-p) and repeat the above steps.

• If p = 1, we call it 1-persistent CSMA, which means it always transmits when the medium is quiet.

• If p = 0, we call it 0-persistent CSMA, which means it always waits for one time slot.

**CIPHER**

**MONO ALPHABETIC:-**

Mono-alphabetic Substitution Ciphers are probably the most common form of cipher. They work by replacing each letter of the plain-text with another letter (or possibly even a random symbol).

A mono-alphabetic substitution cipher, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plain-text, we replace it with the letter "R" in the cipher-text.

**POLY ALPHABETIC:-**

A polyalphabetic (or multialphabetic) cipher is any cipher based on substitution, using multiple substitution alphabets.

**TRANSPOSITIONAL CIPHER:-**

A transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. as same alphabet may have different positions in a text hence its cipher text will be different

**EXERCISE 1:-** CIPHER TEXT WITHOUT KEY



ciphertext "ALNISESTITPIMROOPASN"

**EXERCISE 2 :- CIPHER TEXT WITH KEY**



**EXERCISE 3:-**

****

The ciphertext is thus "TINES AXEOA HTFXH TLTHE YMAII AIXTA PNGDL OSTNH MX".

**Caesar Cipher :-**

Each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is named after Julius Caesar.

Eg:- The text we will encrypt is 'defend the east wall of the castle', with a shift (key) of 1.

plaintext: defend the east wall of the castle

ciphertext: efgfoe uif fbtu xbmm pg uif dbtumf