FOURTH SEMESTER BCA DEGREE EXAMINATION MAY 2016

1 (a)What is communication network? List out examples of communication network.

Ans: A communication network can be defined as “When two or more devices are connected together through a wired medium or wireless medium and If they are able to exchange information among them it forms a communication network.”

1. Source.
2. Transmitter.
3. Transmission system.
4. Receiver
5. Destination

For example, telephone network, telegram network, LAN, MAN, WAN etc.

(b) Explain the key factors in communication network education.

Ans: There are 4key factors in communication network evaluation,

1. Role of Market
2. Role of Technology
3. Role of Standard
4. Role of Regulations

1.Role of Market:

The existence of a market for a new service is the first factor involved determining the success of a new service. This success is ultimately determined by customers to pay, which, of course, depends on the cost, usefulness, and appeal of the services.

EX: Telephone or email service is of limited use if the number of reachable destinations is small.

2.Role of Technology:

Technology always plays a role in determining what can be built. The capability of various technologies is improved dramatically over the past two centuries.

This improvement in capability has been accompanied by reduction in cost. As a result many systems that were simply impossible two decades ago have become not only feasible but cost effective.

3. Role of Standard:

Standard are basically agreement, with industry wide, national, and possibly international scope that allows equipment manufactured by different vendors to be interoperable.

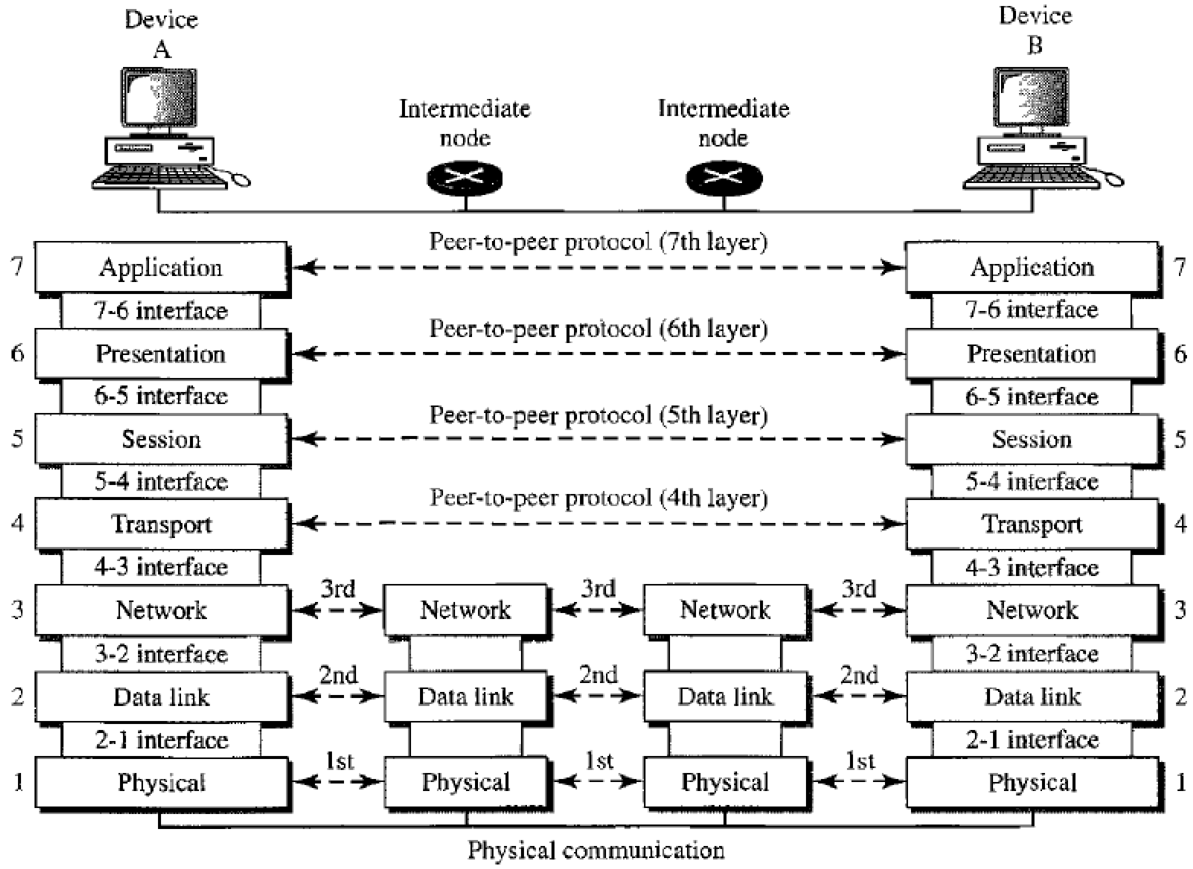
Standard can arise in a number of ways. In the strict sense, demure stands result from a consultative process that occurs on a national and possible international basis.

EX: Many communications stands, especially for telephony, are developed by international telecommunication union (ITU),

4. **Role of Regulations:**

Traditional communication services in the form of telephony and telegraphy have been government regulated. Because of the high cost in deploying the requisite infrastructure and importance of controlling communications, governments often chose to operate communication network was done over time horizons spanning several decades.

C) Explain OSI reference model in detail.



Physical Layer : It coordinates the functions required to carry a bit stream over a physical medium. It deals with mechanical and electrical specifications of the interface and transmission medium. It is also responsible for physical characteristics of interface and medium, Transmission modes and physical topology.

2)Data Link Layer : It transforms the physical layer, It makes the physical layer appear error free to the upper layer. It is also responsible for framing of data packets, physical addressing, Error control and flow control.

3)Network Layer : It is responsible for the source to destination delivery of packets across multiple networks, whereas the data-link layer oversees the delivery of the packet between two systems on the same network, the network layer ensures that each packet delivered in different networks. It is responsible for logical addressing.

4)Transport Layer : It is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas network source-to-destination delivery of individual packets, it doesn't recognise any relationship between those packets. It is also responsible for segmentation and reassembly of data packets.

5)Session Layer : The services provided by the first three layers(Physical, Data-link and Network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains and synchronises the interaction among communication system.

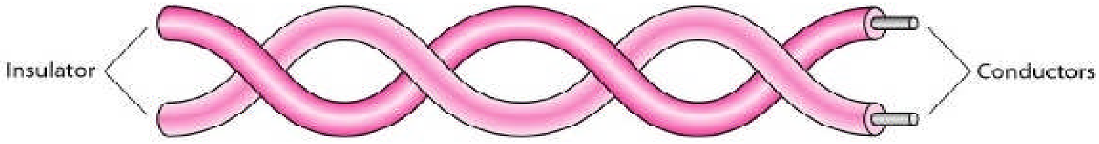
6)Presentation Layer : It is concerned with the syntax and semantics of the information exchange between two systems. It is also responsible for Translation, Encryption and Compression.

7)Application Layer : It enables the user to access the network. It provide user interfaces and support applications. It is also responsible for File transfer, access and Network Virtual Terminal.

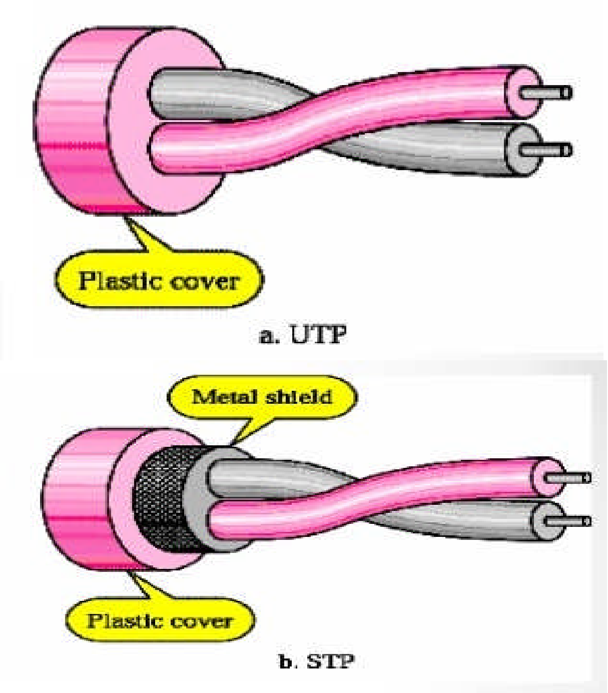
2 (a) Explain twisted pair and co-axial cable transmission media in detail.

In telecommunication, transmission media can be divided into Guided and Unguided media. Guided media are those that provide a transmission channel from one device to another. It includes Twisted pair, Coaxial cable and fibre optic table.

Twisted Pair Cable : It consists of two conductors which are insulated by using a plastic cover as shown in figure below. One of the wire is used to carry signals to the receiver and other is used only as aground reference.



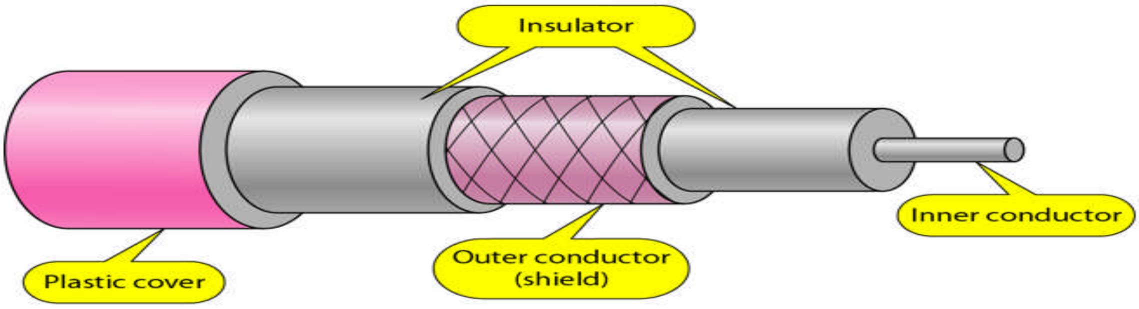
The most common twisted pair cable used in communication is Unshielded Twisted Pair(UTP). IBM has also produced a version of twisted pair cable called Shielded Twisted Pair(STP).



a. UTP

b. STP

Coaxial Cable : It carries signal of higher frequency ranges then those in twisted pair cable because two media are constructed differently. Instead of having two wires coaxial has central core conductor usually copper enclosed in an insulating sheath which is intern covered with outer conductor of metal foil, braid or combination of the two. The outer metallic wrapping serves both as a sheath against noise also as second conductor which completes the circuit.



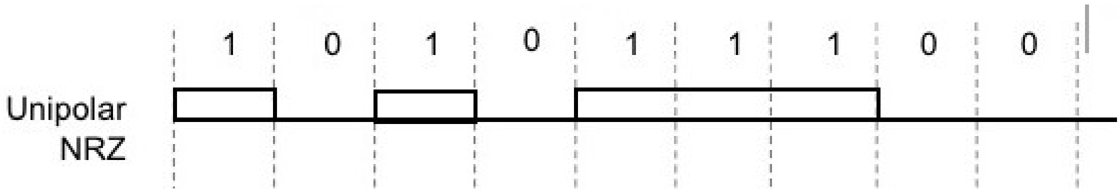
(b) What is line coding? Explain line coding methods in details.

Ans: Line coding:

Line coding is the method of conversation of digital data digital signals is called as line coding.

There are 2 types of line coding methods:

1) **Unipolar**
   - NRZ (non return zero)

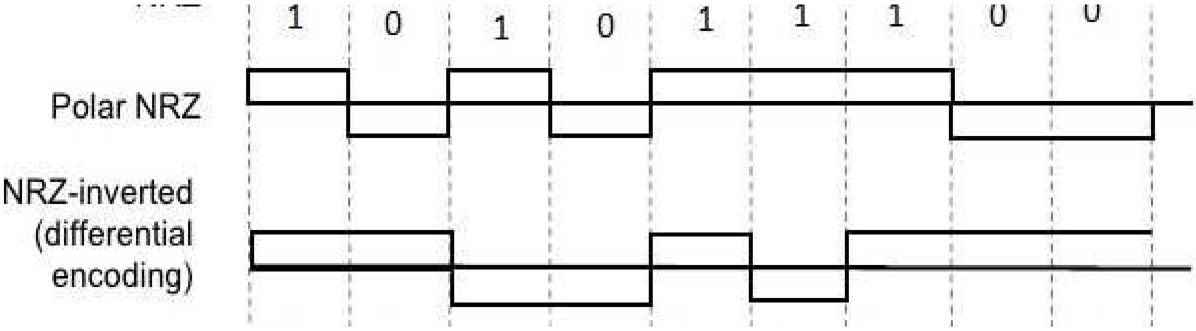


Unipolar NRZ is simply a square wave with +AV being a binary 1, and 0V being 0. NRZ is convenient because computer circuits use unipolar NRZ internally, and it requires little effort to expand this system outside the computer. Unipolar NRZ has a DC term, but a relatively narrow bandwidth.

1-Highlevel

0-Low level (on the Base line)

2) **Polar**
   - Level and invert (NRZ)



Non-return to zero level. This is the standard positive logic signal format used in digital circuits.

1-forces a High level

0-fotces a low level

Non-return to zero invert. This is the positive logic signal format used in digital circuits.

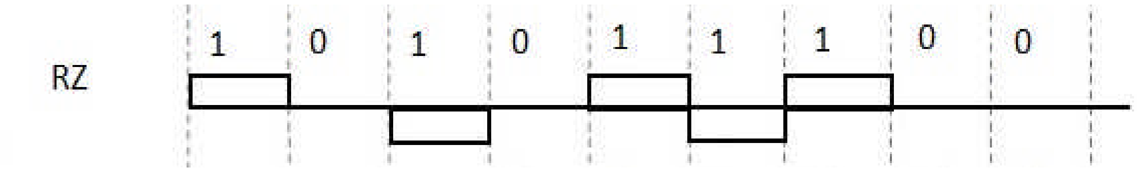
First bit 1- High level

0-low level

Next bit 1-no inversion

0-inversion

RZ (return zero)



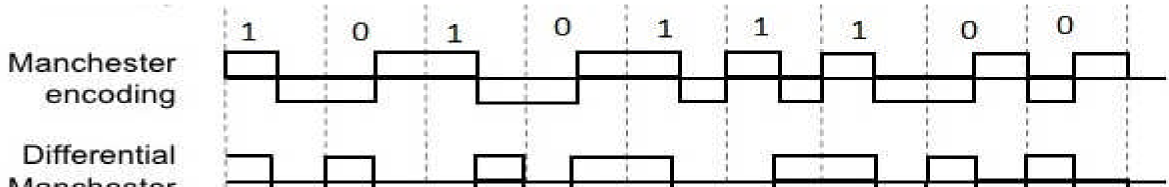
Return to zero. This is the standard positive logic signal format used in digital circuits.

1-Goes high for half the bit period

0-does nothing (low)

Biphase

1. Manchester and Differential Manchester



In Manchester encoding, the transition at the middle of the bit is used for both synchronization and bit representation.

1-is represented as

0-is represented as

In Differential Manchester encoding, the transition at the middle of the bit is used for both synchronization and bit representation.

First bit 1-represented as

0-represented as

Next bit 1-non inversion

0-inversion

3. (a) What is modulation ? Explain ASK, ISK, PSK digital modulation techniques in detail.

Ans: Modulation:

Modulation is a process of superimposing the information contents of a modulating signal on a carrier signal (Which is of high frequency) by varying the characteristic of carrier signal according to the modulating signal.

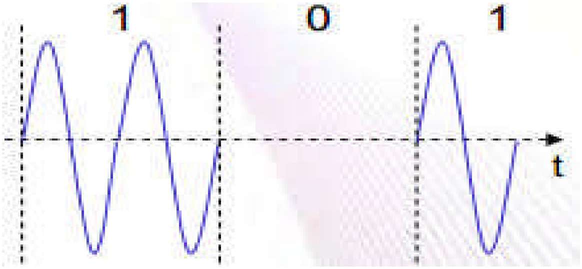
Amplitude shift keying (ASK):

ASK- strength of carrier signal is varied to represent binary 1 or 0.

Pros:

- Both frequency and phase remain constant while amplitude changes.
- Commonly, one of the amplitudes is zero.

Example: Many legacy wireless systems,



Phase shift keying (PSK):

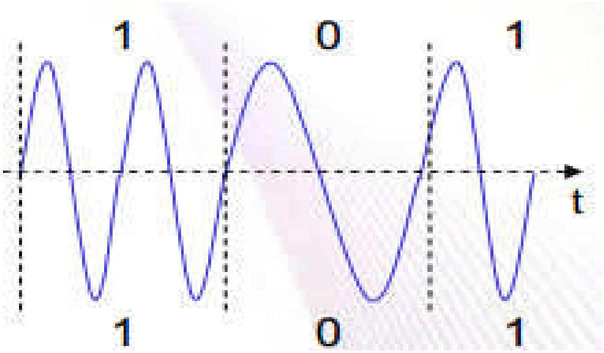
PSK- phase of carrier signal is varied to represent binary 1 or 0.

Pros:

- Peak amplitude and frequency remain constant during each bit interval.
- Less susceptible to noise.
- Bandwidth efficient.

- Requires synchronization in frequency and phase and complicates receivers and transmitter.

Example: IEEE 802.15.4



(b) Explain single parity check &two dimensional parity check to detect error.

Ans: single parity check:

The most familiar error detecting code is a simple parity check code. In this code a single bit is added to the data word, this bit is called parity bit.

There are two ways of adding the parity bit.

1. Adding even parity bit.
2. Adding odd parity bit.

In Even parity bit the redundant bit will be 1 is added if the number of bits in the data word are added if the number if bits (1) are even. Consider the following

1011011	1

Data bit parity bit

In Odd parity a parity bit is added to the data word. This bit will be 1 if the number of 1^s in data word are even and 0 is added if the number of 1^s is odd.

Drawbacks:

There are two major drawbacks to adding the single parity bit;

1. If 2 bits simultaneously change due to the transmission error. Where 1 become 0 will go undetected as it does not effect the number of occurrences of 1 remains same.
2. If the parity bit its self is changed due to transmission error over then it goes undetected.

Two dimensional parity check: To over come the drawback of one dimensional parity check, two dimensional check is used. In this method the data is organised in a table which contains rows and columns here instead of sending only 1 data word multiple data words are added each parity for every row & every column to get an addition parity word.

Example:

D1101100111

D210101011 1

D301011010 0

D4110101011

10010111 0

As shown in the figure above the 2 dimensional parity check detects the most of the errors that occur any where in the table however the error affecting 4 bits may not be detected.

© Define Shannon- Channel capacity.

Ans: Shannon-channel capacity:

It reality we can have a noise less channel; the channel is always noisy in 1994, the calved Shannon introduced formula called Shannon capacity to determine the theoretical height data rate the noise channel.

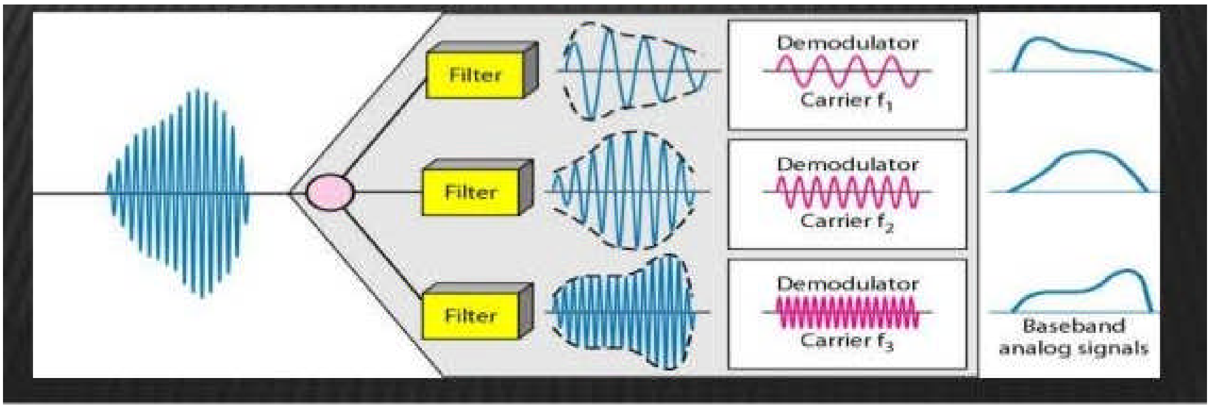
Capacity=bandwidth*log2 (1+SNR)

4.(a) What is multiplexing? Explain following:

Multiplexing is a technique that allows simultaneous transmission of multiple signal lines into a single data link. Multiplexing is done using a device called Multiplexer that combine n input line to generate single output line.

(i) FDM (Frequency Division Multiplexing)

Ans:



It arises from the simulataneous use of a transmision medium by multiple pairs of entities.s

We imagien FDM as providing each pair with a provide transfmission pathoas if the pair had a separate physical transmission medium

Practical fdm system – there are some limitations

-if the frequencies of two channels are too close , interference can

Occure

-Furthermore, demultiplexing hardware that receives a combine signal must be able to divide the signal into separate carriers

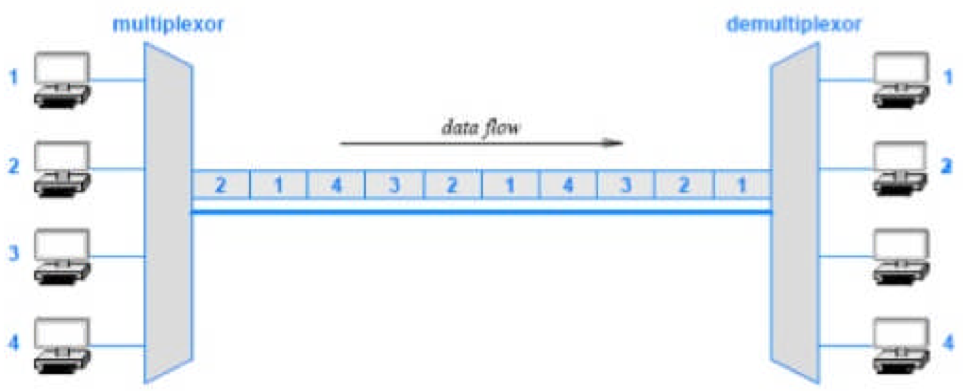
-FCC in usa regulates stations to insure adequate spacing occurs between the carriers

-designers choosing a set of carrier frequencies with a gap between them known as guard band that allocates 200 KHz to each of 6 channels with a guard band of 20 KHz between each .

(ii) TDM (Time Division Multiplexing)

Time Division Multiplexing

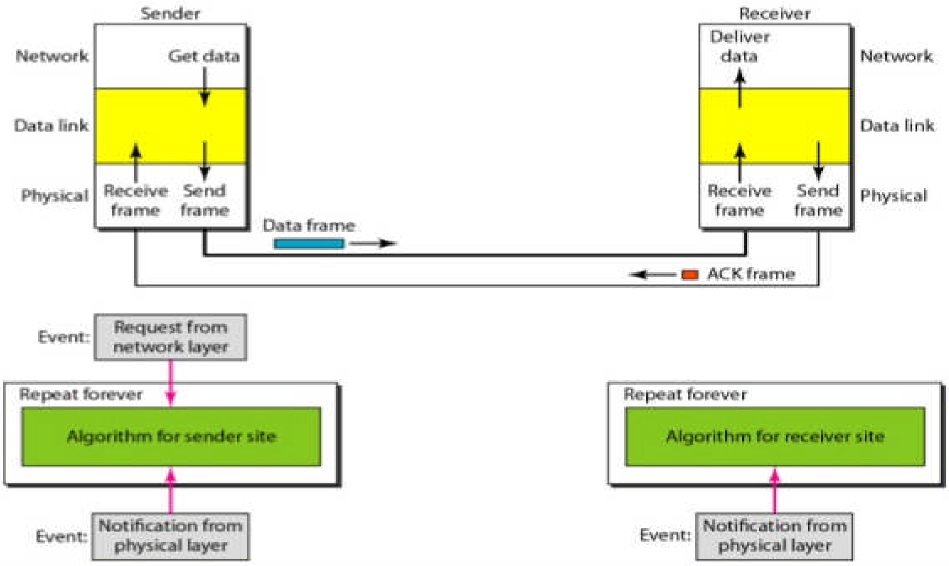
- It is the digital multiplexing technique.
- Channel/Link is divided on the basis of time not on the basis of frequency.
- Total time available in the channel is divided between several users.
- Each user is allotted a particular time interval called Time slot or Slice.
- In TDM, the data rate capacity of transmission medium should be greater than the data rate required by sending device.



(b) What is ARQ? Explain stop and wait ARQ in detail.

Automatic repeat request (**ARQ**) is a **protocol** for error control in data transmission. When the receiver detects an error in a packet, it automatically requests the transmitter to resend the packet.

Stop –and – wait ARQ



In this protocol, the sender sends one frame at a time and waits for an acknowledgment
before sending the next one. To detect corrupted frames, we need to add a CRC to each data frame. When a frame arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded. The silence of the receiver is a signal for the sender that a frame was either corrupted or lost. Every time the sender sends a frame, it starts a timer. If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame (if it has one to send). If the timer expires, the

sender resends the previous frame, assuming that the frame was either lost or corrupted. This means that the sender needs to keep
a copy of the frame until its acknowledgment arrives. When the corresponding
acknowledgment arrives, the sender discards the copy and sends the next frame if it is
ready. Error detection in Stop-and-wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the time expires. In Stop-and-wait ARQ, we use sequence numbers to number the frames. The sequence numbers are based on modulo-2 arithmetic. In Stop-and -wait ARQ, the acknowledgement number always announces in modulo-2 arithmetic the sequence number of the next frame expected.

5. **(a) Explain CSMA with I- persistent, non- persistent and P – persistent.**

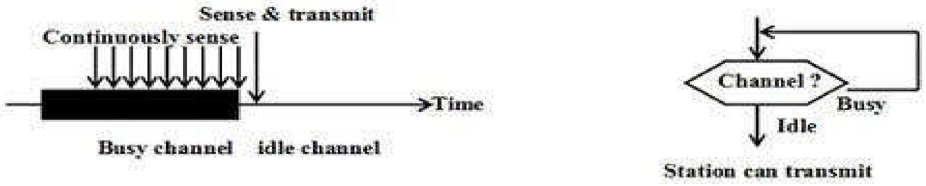
Ans: CSMA (Carrier Sense Multiple Access):

CSMA requires that each station first listen to the medium or check a state of a medium before sending. In other words CSMA is based on the principle sense before transmit or listen before talk.

CSMA can reduce possibility of collision but it cannot eliminate it there are various ways in which carrier is sense (persistent method). **The 3 persistence methods are,**

1) **1-Persistence Scheme:**

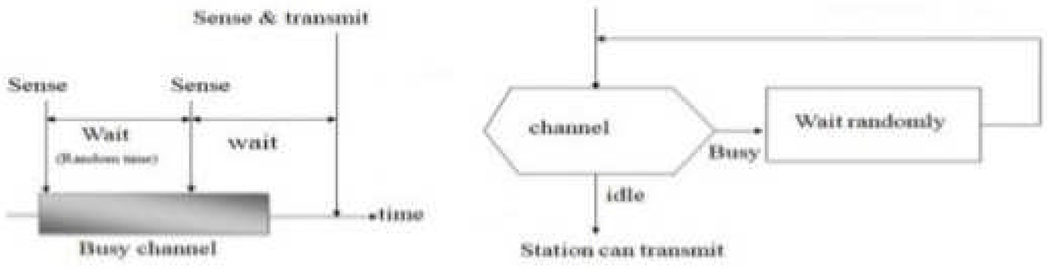
This method is simple and straight forward. In this method after the station finds line idle it sends his frame immediately this method has the highest chances of collision because two or more stations may find the line idle and sends the frame immediately.



1-persistent CSMA

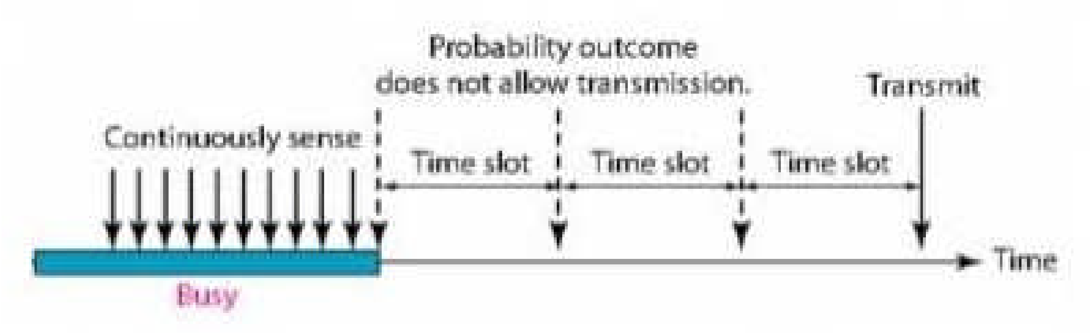
2) **Non-Persistence:**

In Non-persistence method station that has a form to send sense the line. If the line is idle it sends immediately if the line is not idle waits random amount of time and then sense line agin. The non-persistence approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously however this method reduces the efficiency of the network because the medium remains idle when there may be stations with frame to send.



3) P-Persistence:

This method is used if the channel has time slot with the slot duration equal or greater than a maximum propagation time the P-persistence approach combine the advantages of two strategy produces chances of collision and improves efficiency.



(b) Explain IEEE 802-3 MAC frame structure.

Ans: 802.3 MACframe

Preamble: 56 bits of alternating Is and as .

1) D Preamble. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating Os and Is that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56- bit pattern allows the station to miss bits at the beg inning of the frame.The preamble is actually added at the physical layer and is not (formally) part of the frame.

2) D Start frame delimiter (SFD). The second field(1 byte: 10101011) signals the beginning of the frame. The SFD warms the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.
3) Destination (DA). The DA field is also 6 bytes and contains the physical address of the destination station or station to receive the packet.
4) Source address (SA). The SA field is also 6 bytes and contains the physical address of the sender of the packet.
5) Length or type. This field is defined as a type or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.
6) Data. This field carries data encapsulated from upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
7) CRC. The last field contains error detection information, in this case a CRC-32

6. **(a) Explain ALOHA in detail.**

Ans: In 1970 Norman Abramson and his colleagues devised a new and elegant method to solve channel allocation problem. Abramson's work, called ALOHA system, used ground-based ratio broadcasting, the basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel. There are two types of aloha-Pure and Slotted.

Pure Aloha: The basic idea of aloha system is simple. Let users transmit whenever they have data to be sent. There will be collisions, of course, and the colliding frames will be damaged. However due to the feedback property of broadcasting, a sender can always find out whether its frame was destroyed by listening to the channel, the same way the other users do.

If you have a packet just send it.
if multiple people try it and so there is collision then try resending it later.
Theoretical analysis(based on Passion distribution) shows through put of 18% to reach the destination.

Slotted Aloha:

Synchronous that is time is divided into slots.

Slot size is equal to the transmission time of packet.
When you are ready to transmit at the start of the time slot.
Doubles the efficiency of Aloha.

But requires Synchronisation.

(b) Differentiate between datagram packet switching and virtual circuit packet switching.

Issue circuit setup	**Datagram packet switching** **Not needed**	**Virtual circuit packet switching** **Required**
Addressing	Each packet is contains the full source and destination address.	Each packet contains a short virtual circuit network.
State information	Routers do not hold state information about connections.	Each virtual circuit requires router table space per connection.
Routing	Each packet is routed independently.	Route chosen when virtual circuit is set up; all packets follow it.
Effect of router failure	None, expect for packets lost during the crash.	All VC's that passed through the failed router are terminated.
Quality of services.	Difficult.	Easy if enough resources can be allocated in advanced for each VC.
Congestion control	Difficult.	Easy if enough resources can be allocated in advanced for each VC.

(c) What is a modem?

Ans: A modem is a network device that both modulated and demodulates analog carrier signals (called sine waves) for coding and decoding digital information for processing. Modems accomplish both of these tasks simultaneously and, for this reason, the term modem is a combination of "modulate" and "demodulate."

7. **(a) What is congestion. Explain the leaky- bucket algorithm for congestion control.**
   Congestion is an important issue that can arise in packet switched network. Congestion is a situation in communication Networks in which too many packets are present in a part of the subnet, performance

degrades. Congestion in a network may occur when the load on the network (i.e the number of packets sent to the network) is greater than the capacity of the network(i.e. the number of packets a network can handle)

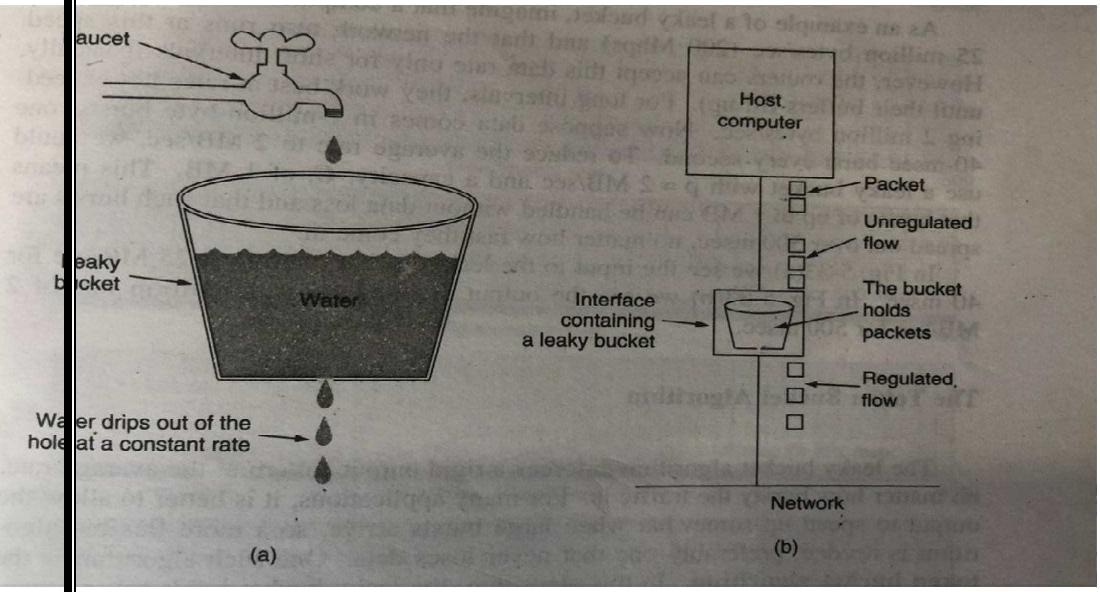
leaky- bucket algorithm for congestion control

Leaky bucket algorithm is a method of temporarily storing a variable number of requests and organising them into a set-rate output of packets in an asynchronous transfer mode(ATM) network.

The leaky bucket is used to implement traffic policing and traffic shaping in Ethernet and cellular data networks. The algorithm can also be used to control metered-bandwidth internet connections to prevent going over the allotted bandwidth for a month, thereby avoiding extra charges.

The leaky algorithm works similarly to the way an actual leaky bucket hold water: The leaky bucket takes data and collects it up to a maximum capacity. Data in the bucket is only released from the bucket at a set rate and size of packet. When the bucket runs out of data, the leaking stops. If incoming data would overfill the bucket, then the packet is considered to be non-conformant and is not added to the bucket. Data is added to the bucket as space becomes available for conforming packets.

The leaky bucket algorithm can also detect both gradually increasing and dramatic memory error increases by comparing how the average and peak data rates exceed set acceptable background amounts.



(b) Explain shortest path first and flooding routing algorithm in detail.

Ans: To create a least-cost tree for itself, using the shared LSDB, each node needs to run the famous **Dijkstra Algorithm.** This iterative algorithm uses the following steps:

1. The node chooses itself as the root of the tree, creating a tree with a single node,

and sets the total cost of each node based on the information in the LSDB.

2. The node selects one node, among all nodes not in the tree, which is closest to the root, and adds this to the tree. After this node is added to the tree, the cost of all other

nodes not in the tree needs to be updated because the paths may have been changed.
3. The node repeats step 2 until all nodes are added to the tree.

The heart of distance-vector routing is the famous **Bellman-Ford** equation. This equation is used to find the least cost (shortest distance) between a source node, **x**, and a destination node, ***y***, through some intermediary nodes (**a, b, c,** . . .) when the costs between the source and the intermediary nodes and the least costs between the intermediary nodes and the destination are given. The following shows the general case in which D***ij***is the shortest distance and c***ij***is the cost between nodes ***I*** and ***j***.
D*xy*= min {(*cxa*+ D*ay*), (*cxb*+ D*by*), (*cxc* + D*cy*), }

In distance-vector routing, normally we want to update an existing least cost with a least cost through an intermediary node, such as **z**, if the latter is shorter. In this case, the equation becomes simpler.
Flooding

Flooding is a computer network routing algorithm in which every incoming packet is sent through every outgoing link except the one it arrived on.

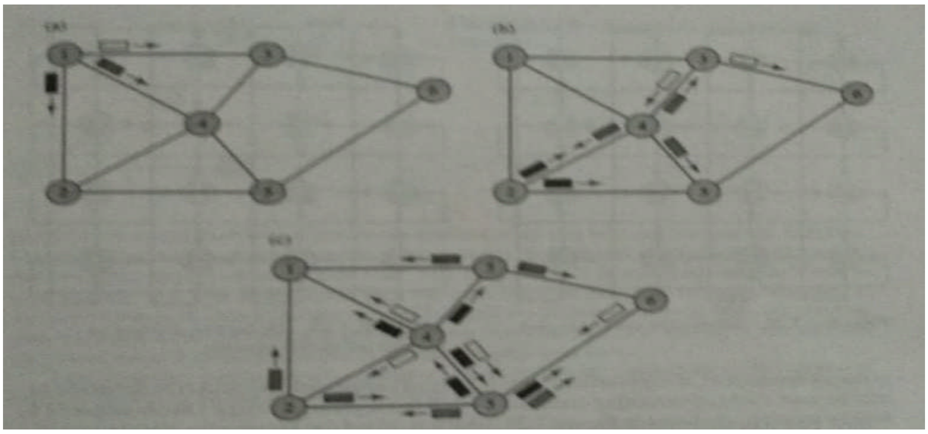
Flooding is used in bridging and in systems such as Usenet and peer-to-peer file sharing and as part of some routing protocols, including OSPF, DVMRP and those used in ad-hoc wireless networks.

There are several varieties of flooding algorithms. Most work through as follows-

i)Each node act as both transmitter and a receiver.

ii)Each node tries to forward every message to every one of its neighbours except the source node.

Algorithms may need to be more complex than this, since, in some case, precautions have to be taken to avoid wasted duplicate deliveries and infinite loops, and to allow messages to eventually expire from the system.

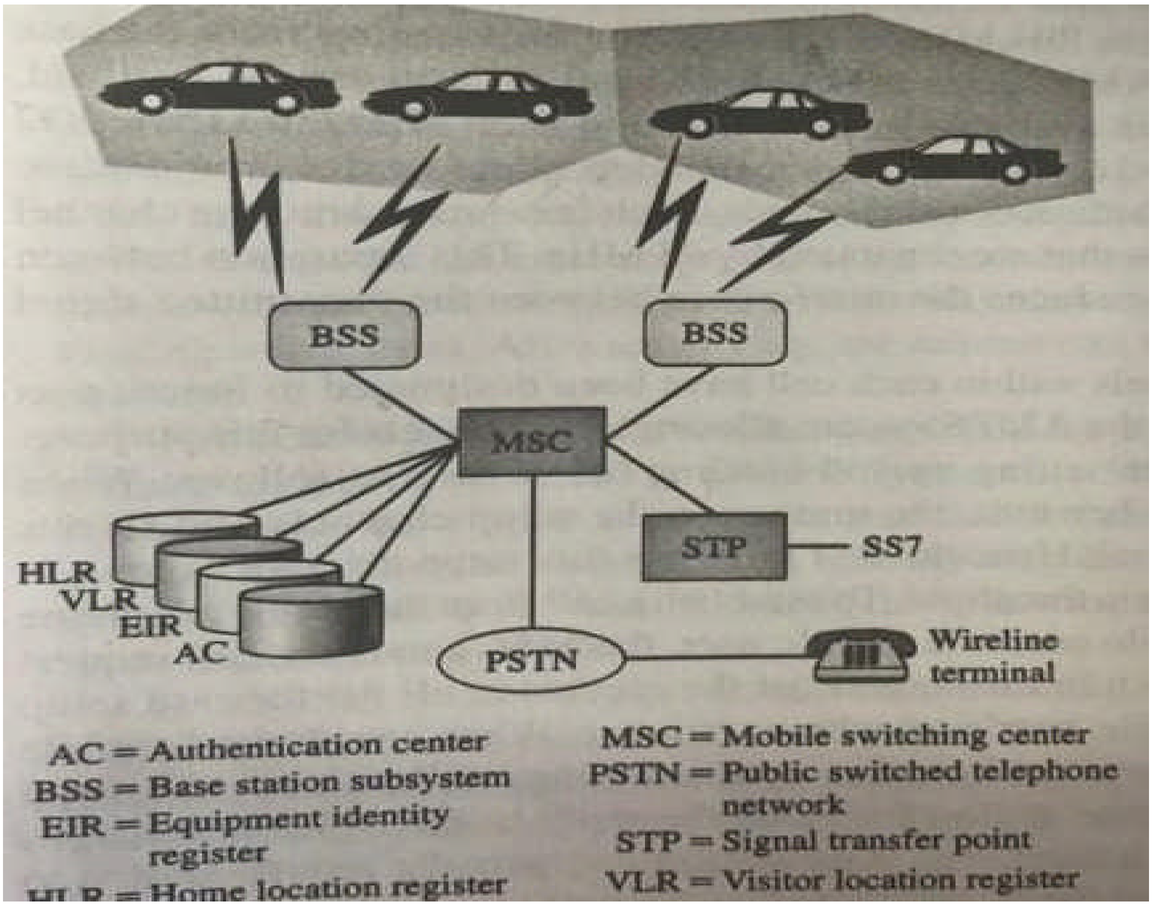


8. Write short notes on any four of the following:

(a) Cellular telephone network.

The first generation of cellular telephone networks extend the basic telephone service to mobile users with portable telephones. Unlike conventional telephone service where the call to a telephone number is directed to a specific line that is connected to a specific switch, in cellular phony the telephone number specifies a specific subscriber's mobile station(telephone). Much of the complexity in cellular phony in results from the need to track the location of the mobile station. In this section we discuss how radio transmission system and the telephone network infrastructure are organised to make this service possible.

In cellular radio communications, a region, for example, a city, is divided into a number of graphical areas called cells and users within a cell communicate using a band of frequencies. Cell areas are established based on the density of the subscribers. Large cells are used in rural areas, and small cells are used in urban areas. The base station is placed near the centre of each cell. The base station has an antenna that is used to communicate with mobile users in its vicinity.


BSS
BSS
MSC
STP
SS7
HLR
VLR
EIR
AC
PSTN
Wireline terminal
AC = Authentication center
BSS = Base station subsystem
EIR = Equipment identity register
HLR = Home location register
MSC = Mobile switching center
PSTN = Public switched telephone network
STP = Signal transfer point
VLR = Visitor location register

(b) HDLC

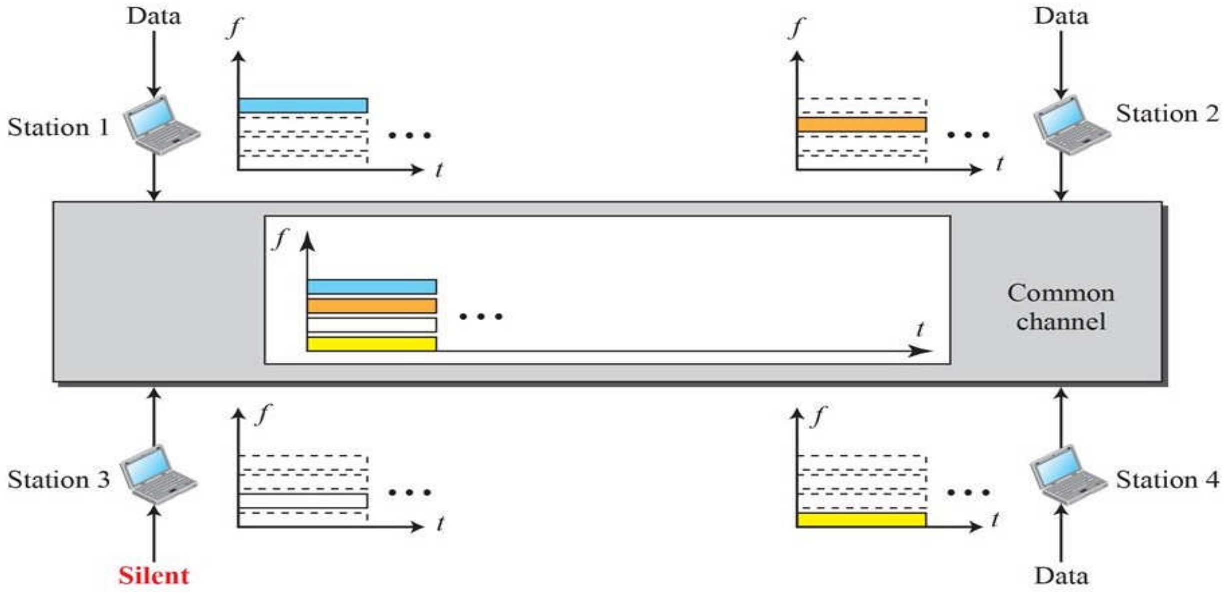
High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. It implements the Stop-and-Wait protocol we discussed earlier. Although this protocol is more a theoretical issue than practical, most of the concept defined in this protocol is the basis for other practical protocols such as PPP, which we discuss next, or the Ethernet protocol, which we discuss in wired LANs or in wireless LANs

(c) FDMA

Ans: FDMA (Frequency Division Multiple Access)

Frequency Division Multiplexing (FDMA) is a networking technique in which multiple data signals are combined for simultaneous transmission via a shared communicztion medium. FDMA uses a carrier signal at a discreate frequency for each stream and then combines many moduleted signals.

When FDMA is used to allow multiple users to shared a single physical communications medium, the technology is called Freuency-Division multiple access(FDMA).



Advantages of FDMA:

- It allocates dedicated frequencies to different stations.
- Moreover, there are separate bands for both uplink and downlink. Hence stations transmit and receive continuously at their allocated frequencies.
- It is very simple to implement with respect to hardware resources.

(d) Polling

Ans: Polling: Each station on the network is polled in some predetermined order. When polled, a station uses the full data rate of the connecting channel to transmit its backlog of the central computer. Between polls, stations accumulate message in there queues, but do not transmit until they are polled.

Transmission between stations takes place through the central computer, which receives all incoming packets and transmits them to the appropriate locations.

(e) CRC

Cyclic redundancy checks (CRC):

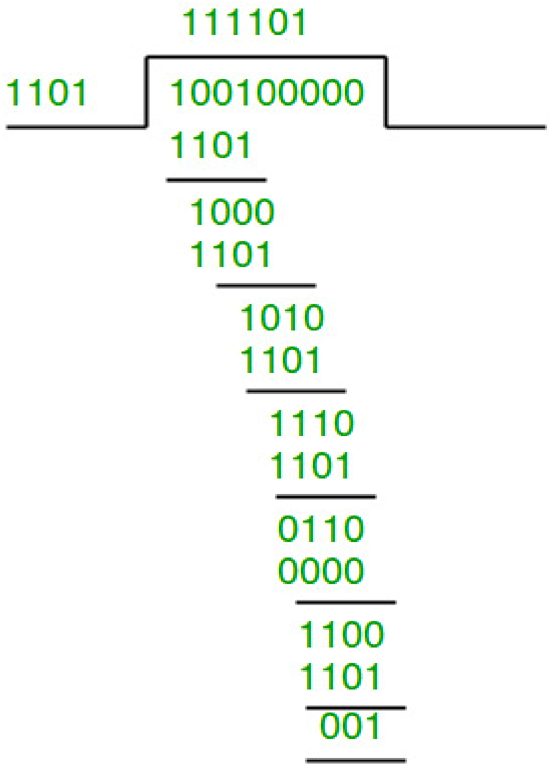
CRC is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these system get a short check value attached, based on the remainder of a polynomial division of their contents.

CRC are so called because the check value is a redundancy and the algorithm is based on cyclic codes. CRC are popular because they are simple to implement in binary hardware, easy to analyse mathematically, and particularly good at detecting common errors caused by noise in transmission channels. Because the check value has a fixed length, the function that generates it is occasionally used as a hash function.

Example 1: (No error in transmission)

Key – 1101 [or generator polynomial x^3+ x+1]

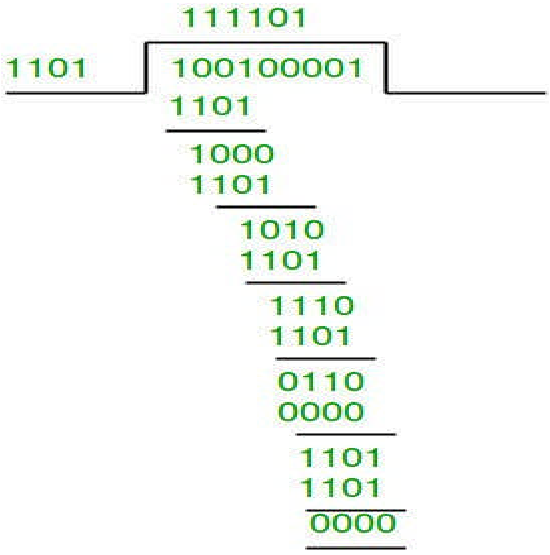
Sender side:



Therefore, the remainder is 001 and hence the encoded data sent is 100100001.

Receiver side:

Code word received at the receiver side 100100001



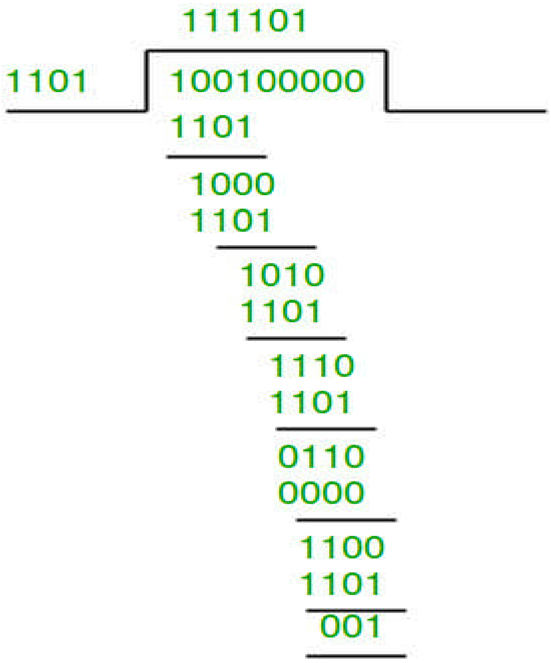
Therefore, the remainder is all zeros, hence, the data received has no error.

Example 2: (Error in transmission)

Data word to be sent – 100100

Key – 1101

Sender side:



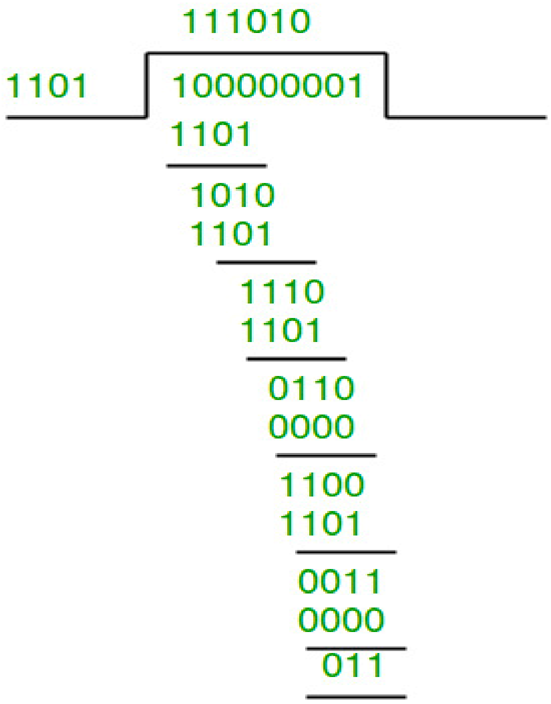
```
             111101
1101    | 100100000 |
          1101
          ----
           1000
           1101
           ----
             1010
             1101
             ----
              1110
              1101
              ----
               0110
               0000
               ----
                1100
                1101
                ----
                 001
```

Therefore, the remainder is 001 and hence the code word sent is 100100001.

Receiver side:

Let there be error in transmission media

Code word received at the receiver side – 100000001



```
             111010
1101    | 100000001 |
          1101
          ----
           1010
           1101
           ----
             1110
             1101
             ----
              0110
              0000
              ----
               1100
               1101
               ----
                0011
                0000
                ----
                 011
```

Since the remainder is not all zeroes, the error is detected at the receiver side.