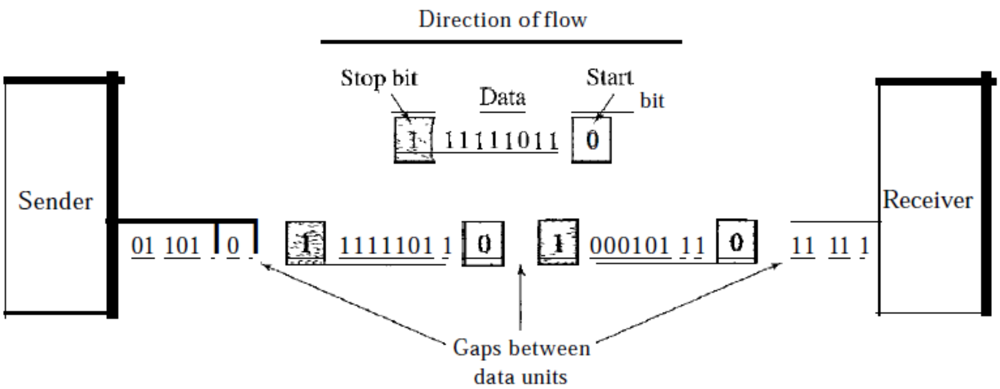
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY
THIRD SEMESTER B.TECH DEGREE EXAMINATION, JULY 2017

Course Name: IT 203 DATA COMMUNICATION (IT)
(ANSWER KEY AND SCHEME)
PART A
Answer any two questions.

1. a. Synchronous transmission - 2.5mark
   Asynchronous transmission. 2.5mark

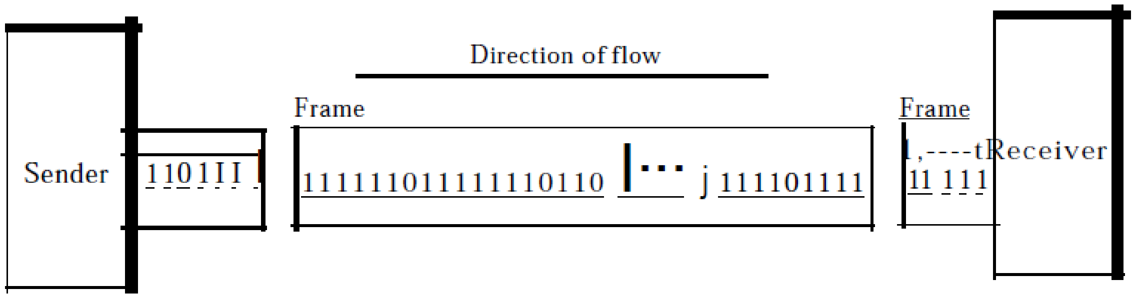
Asynchronous Transmission

Asynchronous transmission is so named because the timing of a signal is unimportant. Instead, information is received and translated by agreed upon patterns. Patterns are based on grouping the bit stream into bytes. Each 8 bit group is sent along the link as a unit. The sending system handles each group independently.Without synchronization, the receiver cannot use timing to predict when the next group will arrive. To alert the receiver to the arrival of a new group. In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (Is) at the end of each byte. There may be a gap between each byte. The start and stop bits and the gap alert the receiver to the beginning and end of each byte and allow it to synchronize with the data stream. Asynchronous here means "asynchronous at the byte level. but the bits are still synchronized; their durations are the same.



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. We have drawn in the divisions between bytes. In reality, those divisions do not exist; the sender puts its data onto the line as one long string. If the sender wishes to send data in separate bursts, the gaps between bursts must be filled with a special sequence of Os and Is that means *idle.* The receiver counts the bits as they arrive and groups them in 8-bit units.



b. Encode digital data 10110010

Draw NRZ-L, NRZ-I, AMI, Manchester and Differential Manchester Encoding –

1*5=5mark

c. Noise definition- 2marks

For any data transmission event, the received signal will consist of the transmitted signal, modified by the various distortions imposed by the transmission system, plus additional unwanted signals that are inserted somewhere between transmission and reception. The latter, undesired signals are referred to as noise. Noise is the major limiting factor in communications system performance.

Types of noise-Any three 1*3=3marks

1) Thermal noise:- **Thermal noise** is due to thermal agitation of electrons. It is present in all electronic devices and transmission media and is a function of temperature.
Thermal noise referred to as **white noise**

2) Intermodulation noise:- When signals at different frequencies share the same transmission medium

3) Crosstalk:- has been experienced by anyone who, while using the telephone, has been able to hear another conversation; it is an unwanted coupling between signal paths.

4) Impulse noise:- external electromagnetic disturbances, such as lightning, and faults and flaws in the communications system.

2. 1) Coaxial cable- 5mark
2) Twisted Pair cable- 5mark
3) Fibre Optic Cable - 5mark

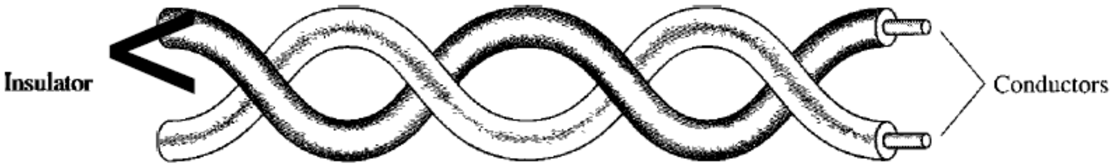
GUIDED MEDIA

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium.

.

Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

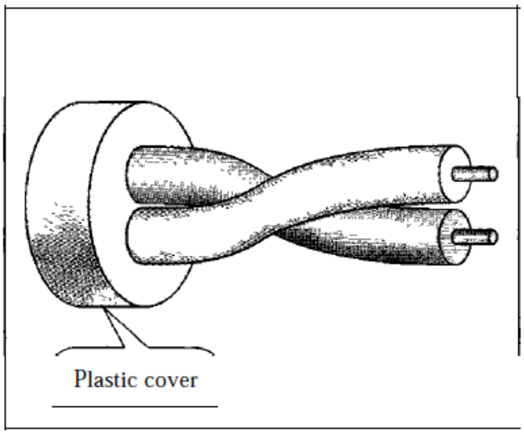


One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals. If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources. This results in a difference at the receiver. By twisting the pairs, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true. Twisting makes it probable that both wires are equally affected by external influences. This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly canceled out.

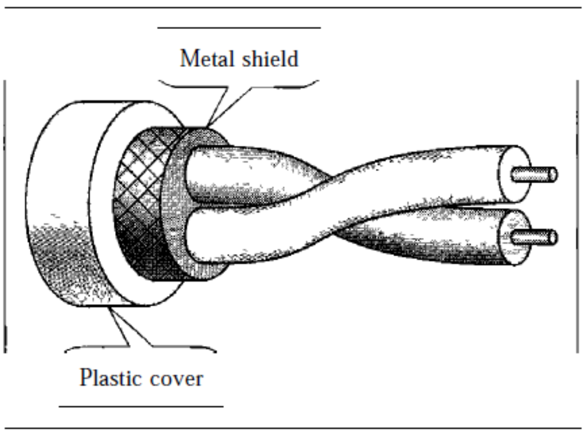
From the above discussion, it is clear that the number of twists per unit of length has some effect on the quality of the cable.

Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil or braidedmesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.



a.UTP

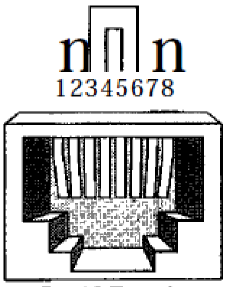


b.STP

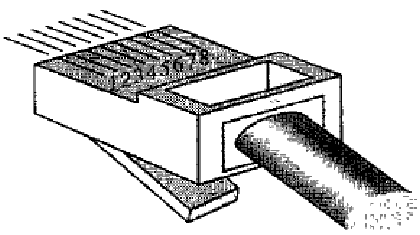
$

Category	*Specification*	*Data Rate (Mbps)*	*Use*
I	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-llines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
SE	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk: and increases the data rate.	600	LANs

UTP connector



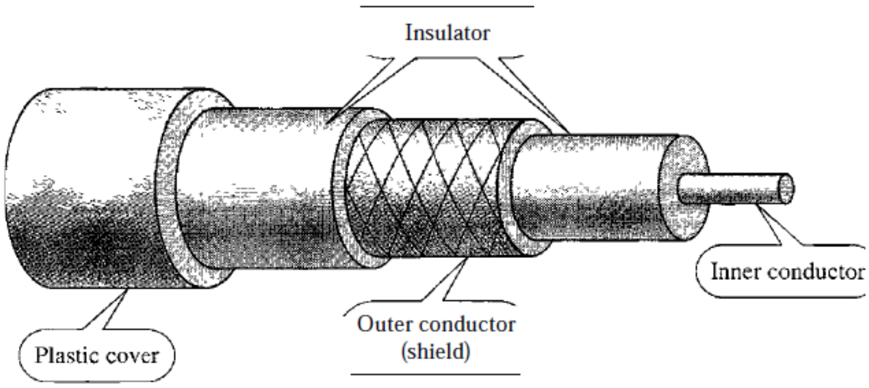
RJ-45 Female



RJ-45 Male

Coaxial Cable

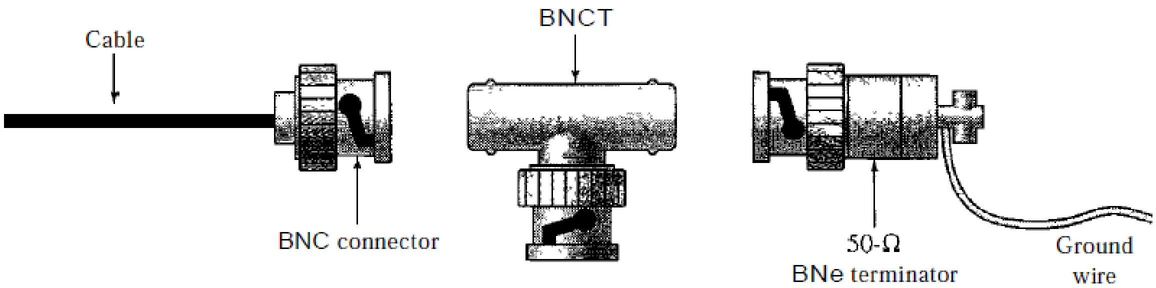
Coaxial cable (or *coax)* carries signals of higher frequency ranges than those in twisted pair. cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover



Coaxial cables are categorized by their radio government (RG) ratings

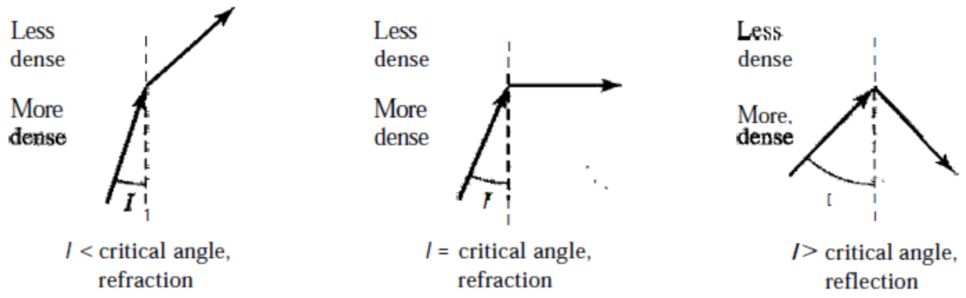
Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNC), connector.

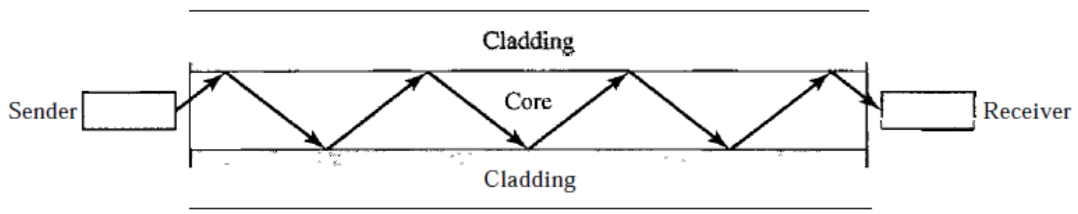


Fiber-Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance . the ray changes irection.



If the angle of incidence *I* is less than the critical angle, the ray refracts and moves closer to the surface. If the angle of incidence is equal to the critical angle, the light bends along the interface. If the angle is greater than the critical angle, the ray reflects and travels again in the denser substance.Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the
two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

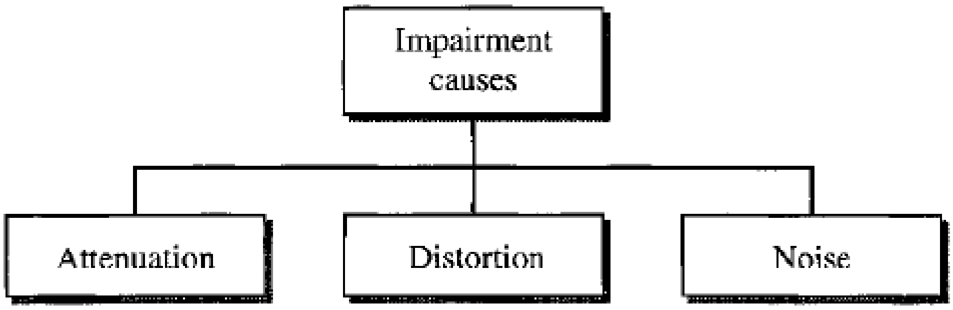


3. a. Transmission Impairments Definition- 1mark

1) Attenuation Explanation - 3mark

2) Delay distortion Explanation - 3mark

3) Noise- 3mark



Noise definition-

For any data transmission event, the received signal will consist of the transmitted signal, modified by the various distortions imposed by the transmission system, plus additional unwanted signals that are inserted somewhere between transmission and reception. The latter, undesired signals are referred to as noise. Noise is the major limiting factor in communications system performance.

Types of noise-Any three

1) Thermal noise:- **Thermal noise** is due to thermal agitation of electrons. It is present in all electronic devices and transmission media and is a function of temperature.
Thermal noise referred to as **white noise**

2) Intermodulation noise:- When signals at different frequencies share the same transmission medium

3) Crosstalk:- has been experienced by anyone who, while using the telephone, has been able to hear another conversation; it is an unwanted coupling between signal paths.

4) Impulse noise:- external electromagnetic disturbances, such as lightning, and faults and flaws in the communications system.

b. Step 1: SNR_{db} to SNR - 2mark

$SNR_{db}=10\log_{10}(SNR)$

$30=10\log_{10}(SNR)$

$SNR=\text{antilog}_{10}(3)$

Ans: 1000

Step 2: Find Channel Capacity- 3mark

$$C = B\log_2(1+SNR)$$
$$= 4000 * B\log_2(1+1000)$$

Ans: 39869bps

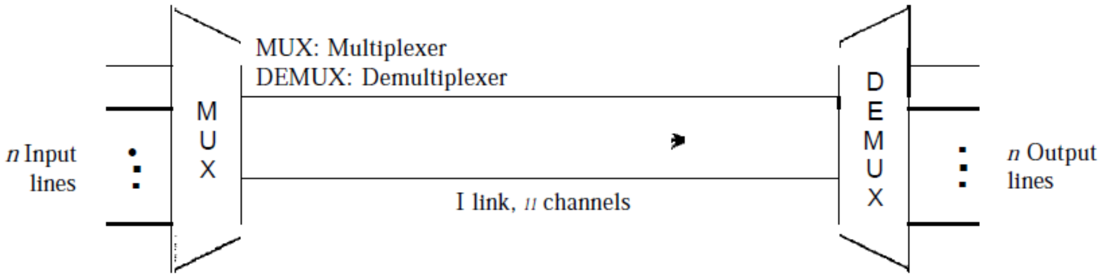
PART B

Answer any two questions.

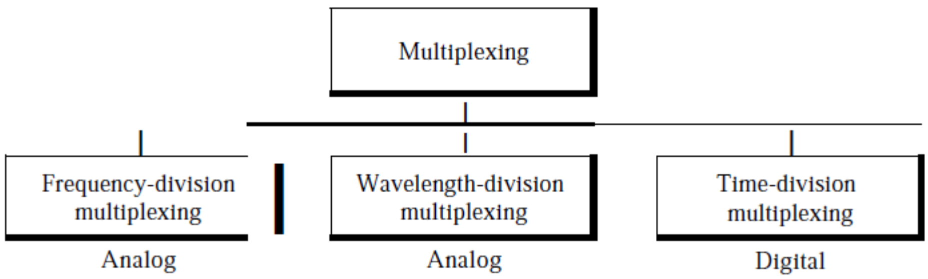
4. a. Multiplexing- 2mark
   1. FDM Explanation with figure (Transmitter-receiver) - 4mark
   2. TDM Explanation with figure (Transmitter-receiver) - 4mark

MULTIPLEXING

In a multiplexed system, *n* lines share the bandwidth of one link. The lines on the left direct their transmission streams to a multiplexer (MUX), which combines them into a single stream. At the receiving end, that stream is fed into a demultiplexer (DEMUX), which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines.

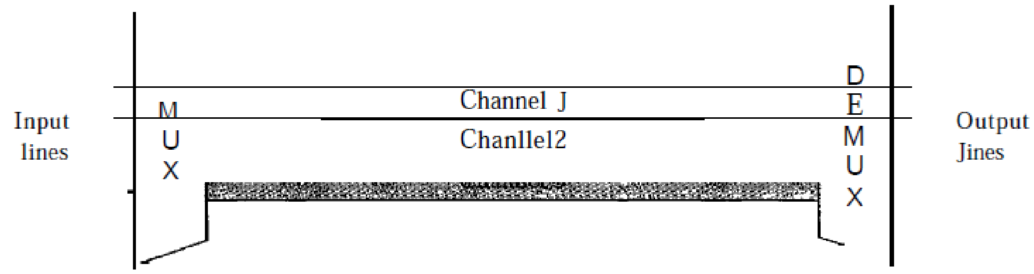


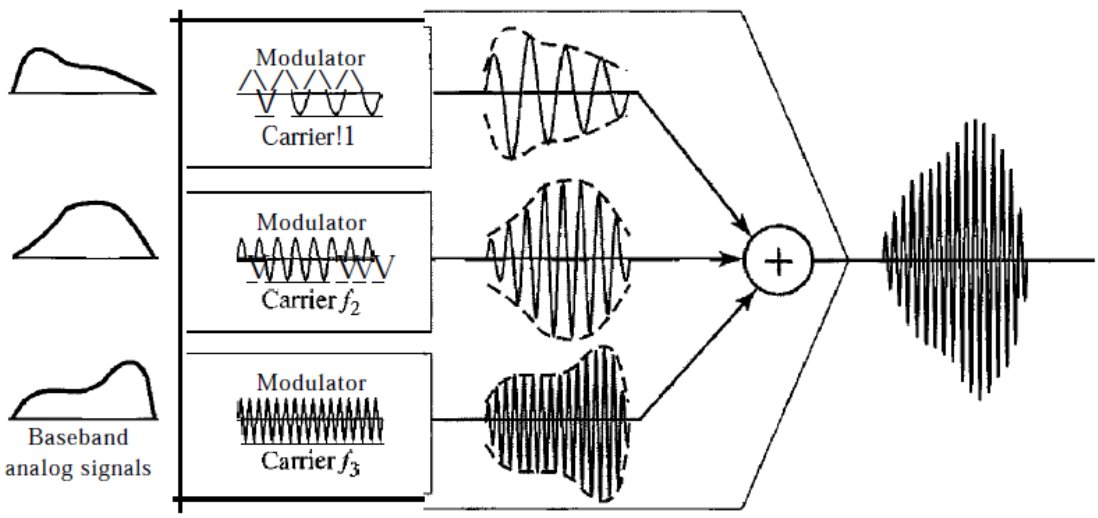
There are three basic multiplexing techniques: frequency-division multiplexing, wavelength-division multiplexing, and time-division multiplexing.



Frequency-Division Multiplexing

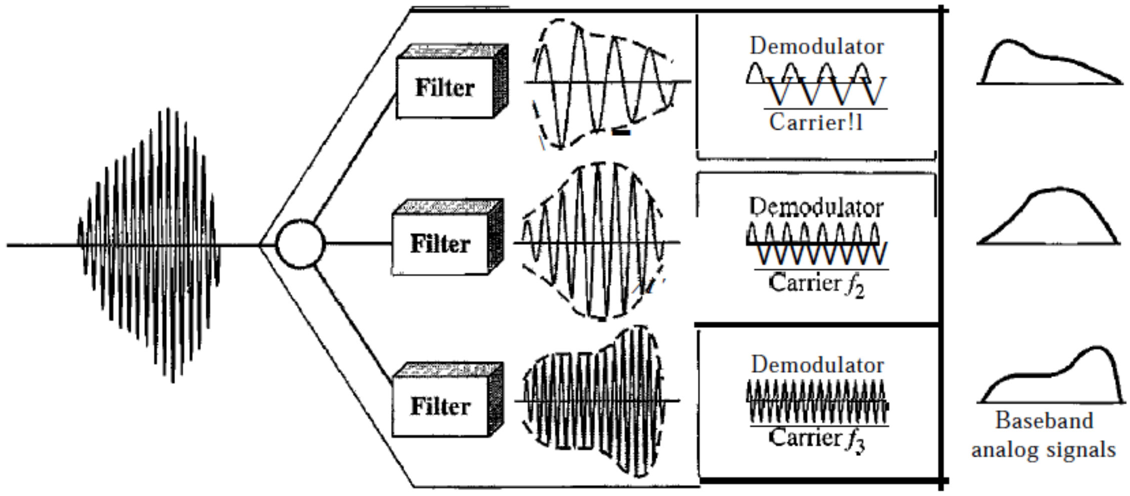
Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels can be separated by strips of unused bandwidth-**guard bands**-to prevent signals from overlapping.





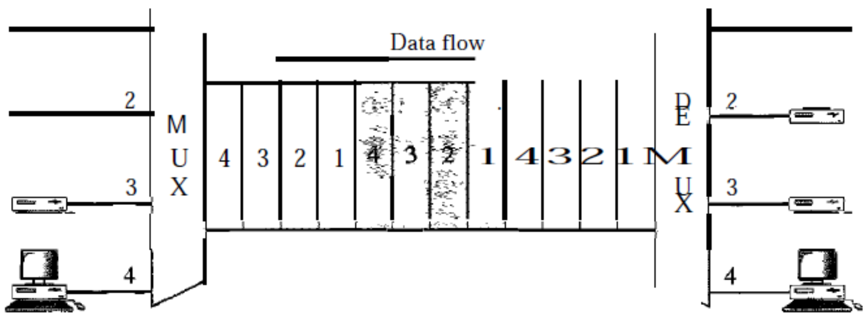
Demultiplexing Process

The demultiplexer uses a series of filters to decompose the multiplexed signal into its constituent component signals. The individual signals are then passed to a demodulator that separates them from their carriers and passes them to the output lines.



Time-Division Multiplexing

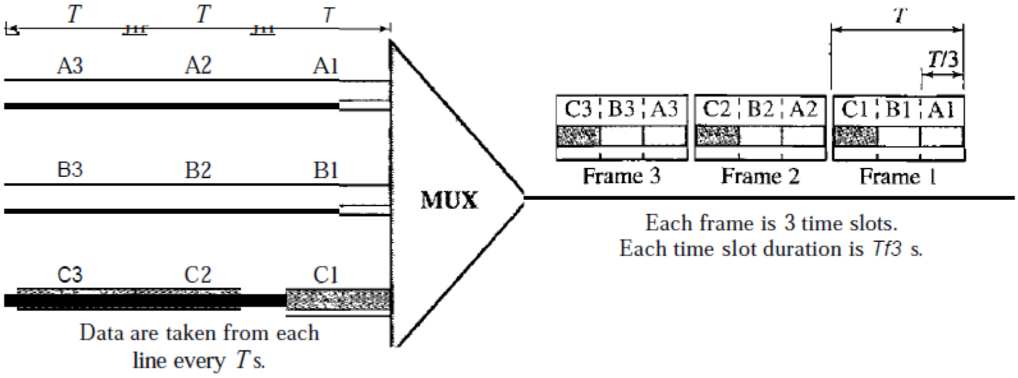
Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a link Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link.



TDM is, in principle, a digital multiplexing technique. Digital data from different sources are combined into one timeshared link. However, this does not mean that the sources cannot produce analog data; analog data can be sampled, changed to digital data, and then multiplexed by using TDM.

TDM is of two different schemes: synchronous and statistical. In synchronous TDM, each input connection has an allotment in the output even if it is not sending data.

In synchronous TDM, the data flow of each input connection is divided into units, where
each input occupies one input time slot. A unit can be 1 bit, one character, or one block of data. Each input unit becomes one output unit and occupies one output time slot. the duration of an output time slot is *n* times shorter than the duration of an input time slot. If an input time slot is *T* s, the output time slot is *T/n* s, where *n* is the number of connections.



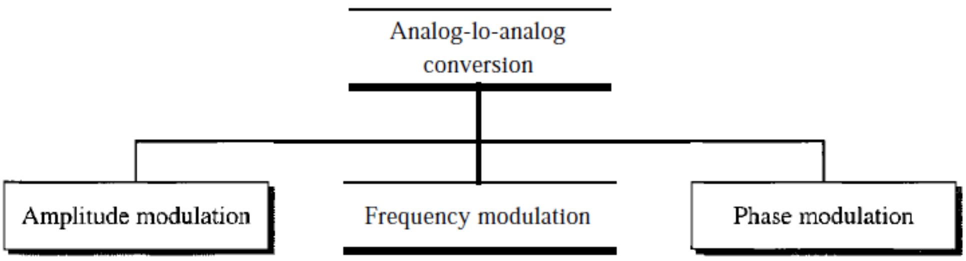
Statistical Time-Division Multiplexing

In statistical time-division multiplexing, slots are dynamically allocated to improve bandwidth efficiency. Only when an input line has a slot's worth of data to send is it given a slot in the output frame. In statistical multiplexing, the number of slots in each frame is less than the number of input lines. The multiplexer checks each input line in roundrobin fashion; it allocates a slot for an input line if the line has data to send; otherwise, it skips the line and checks the next line.

b. Frequency hopping spread spectrum. - 5mark

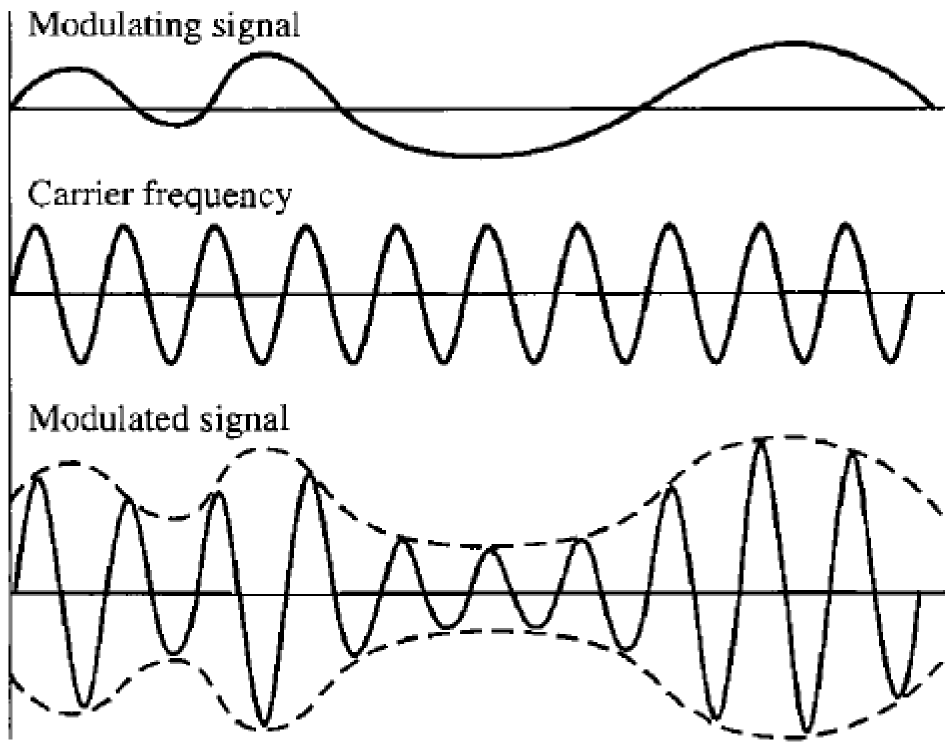
5. a. Listing of Various Scheme (AM, FM&PM) - 1mark
   1. AM Explanation with figure- 3mark
   2. FM Explanation with figure- 3mark
   3. FM Explanation with figure- 3mark

Analog-to-analog conversion can be accomplished in three ways: amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM).



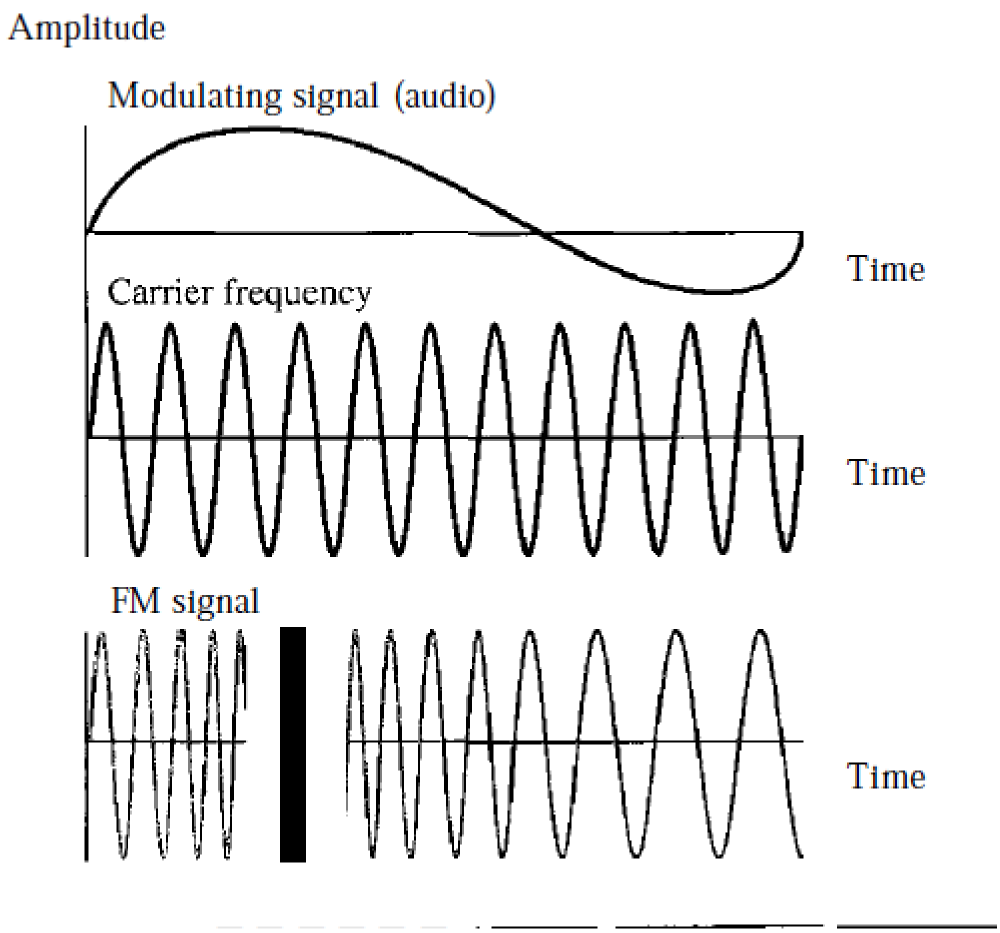
Amplitude Modulation

In AM transmission, the carrier signal is modulated so that its amplitude varies with the
changing amplitudes of the modulating signal. The frequency and phase of the carrier remain the same.



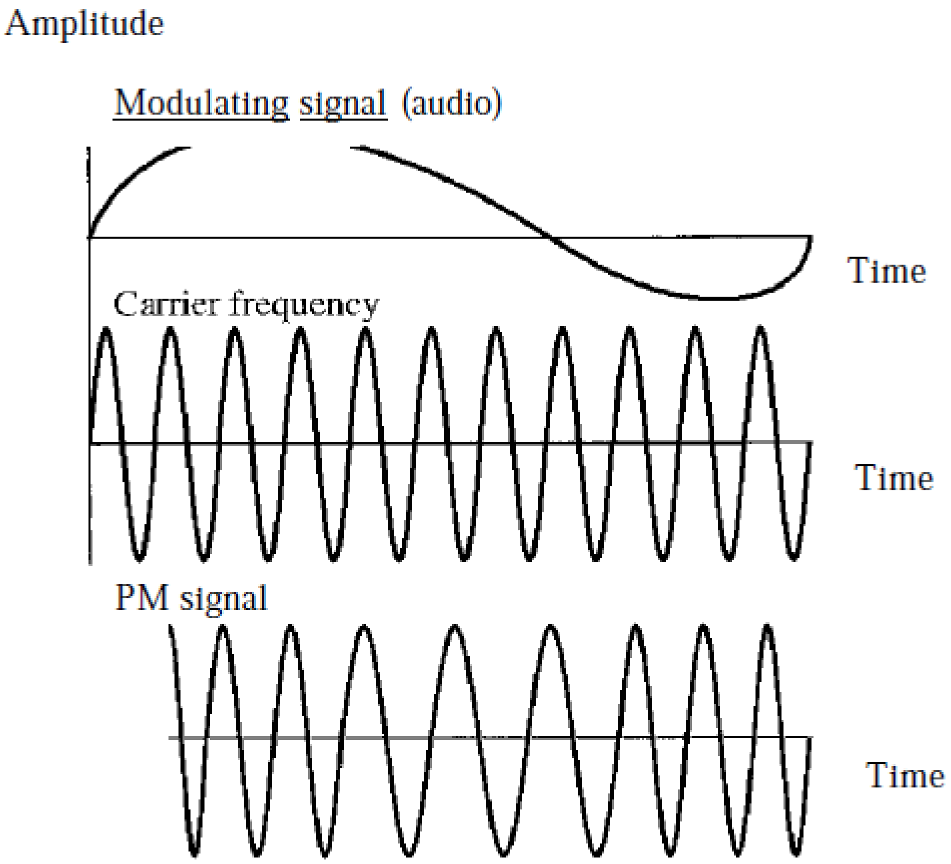
Frequency Modulation

In FM transmission, the frequency of the carrier signal is modulated to follow the changing voltage level (amplitude) of the modulating signal. The peak amplitude and phase of
the carrier signal remain constant.



Phase Modulation

In PM transmission, the phase of the carrier signal is modulated to follow the changing
voltage level (amplitude) of the modulating signal. The peak amplitude and frequency of the carrier signal remain constant



b. CDMA Explanation- 5mark

Code Division Multiple Access

CDMA for cellular systems can be described as follows.As with FDMA, each cell is allocated a frequency bandwidth, which is split into two parts, half for reverse (mobile unit to base station) and half for forward (base station to mobile unit). For full-duplex communication, a mobile unit uses both reverse and forward channels. Transmission is in the form of direct-sequence spread spectrum (DS-SS), which uses a chipping code to increase the data rate of the transmission, resulting in an increased signal bandwidth. Multiple access is provided by assigning orthogonal chipping codes (defined in Chapter 9) to multiple users, so that the receiver can recover the transmission of an individual unit from multiple transmissions. CDMA has a number of advantages for a cellular network:

• **Frequency diversity:** Because the transmission is spread out over a larger bandwidth, frequency-dependent transmission impairments, such as noise bursts and selective fading, have less effect on the signal.

• **Multipath resistance:** In addition to the ability of DS-SS to overcome multipath fading by frequency diversity, the chipping codes used for CDMA not only exhibit low cross correlation but also low autocorrelation.3 Therefore, a version of the signal that is delayed by more than one chip interval does not interfere with the dominant signal as much as in other multipath environments.

• **Privacy:** Because spread spectrum is obtained by the use of noiselike signals, where each user has a unique code, privacy is inherent.

• **Graceful degradation:** With FDMA or TDMA, a fixed number of users can access the system simultaneously. However, with CDMA, as more users access the system simultaneously, the noise level and hence the error rate increases; only gradually does the system degrade to the point of an unacceptable error rate. Two drawbacks of CDMA cellular should also be mentioned:
• **Self-jamming:** Unless all of the mobile users are perfectly synchronized, the arriving transmissions from multiple users will not be perfectly aligned on chip boundaries. Thus the spreading sequences of the different users are not orthogonal and there is some level of cross correlation. This is distinct from either TDMA or FDMA, in which for reasonable time or frequency guard bands respectively, the received signals are orthogonal or nearly so.
• **Near-far problem:** Signals closer to the receiver are received with less attenuation than signals farther away. Given the lack of complete orthogonality, the transmissions from the more remote mobile units may be more difficult to recover.

(5)

6. a.

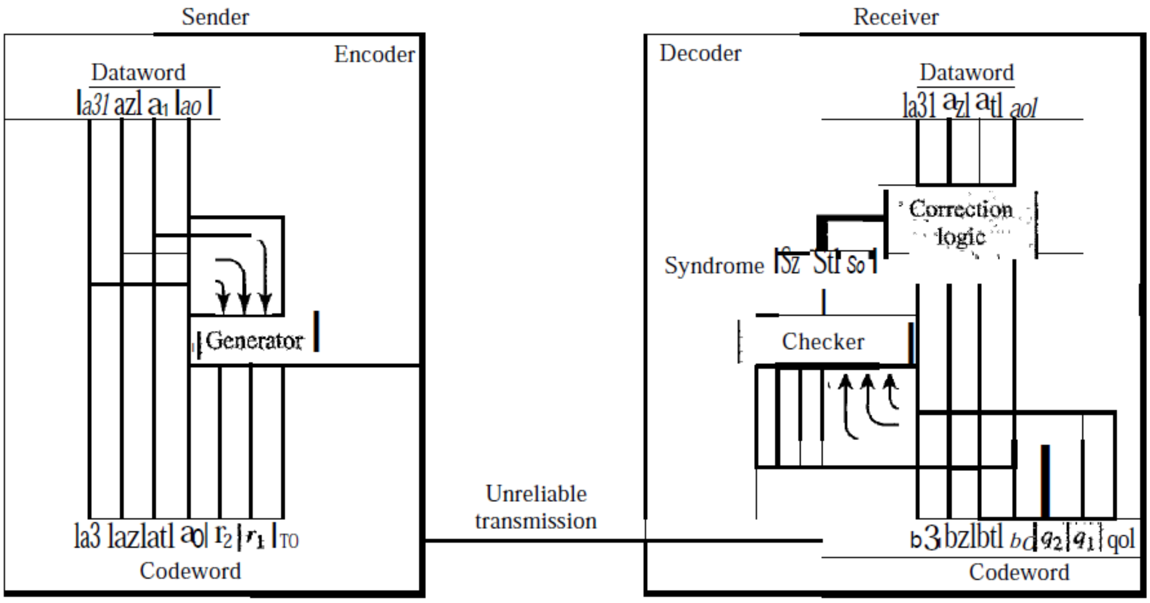
1. Parity Check (Linear Block Coding) - 3mark
2. CRC (Cyclic Code) - 4mark
3. Checksum - 3mark

LINEAR BLOCK CODES

In a linear block code, the exclusive OR (XOR) of any two valid codewords creates another valid codeword.

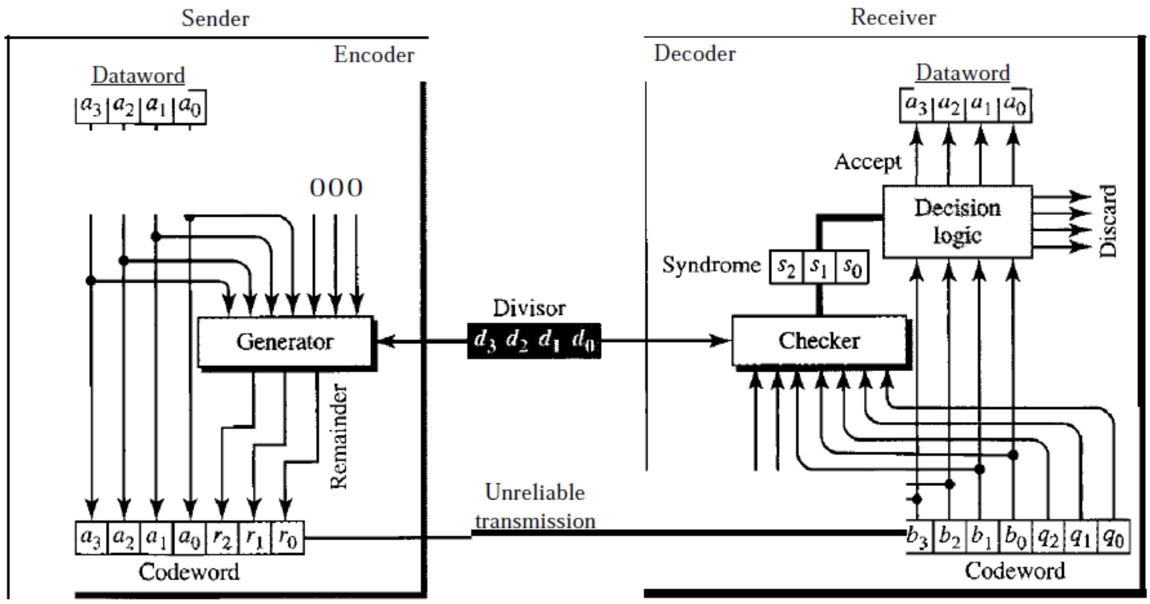
Simple Parity-Check Code

In this code, a *k-bit* dataword is changed to an n-bit codeword where $n = k + 1$. The extra bit, called the parity bit, is selected to make the total number of Is in the codeword even. If the number of 1s is even, the result is 0; if the number of 1s is odd, the result is 1. In both cases, the total number of 1s in the codeword is even. The encoder uses a generator that takes a copy of a 4-bit dataword *(ao,* aI' *a2'* and*a3)* and generates a parity bit *roo* The dataword bits and the parity bit create the 5-bit codeword. The parity bit that is added makes the number of Is in the codeword even. This is normally done by adding the 4 bits of the dataword (modulo-2); the result is the parity bit. In other words, If the number of 1s is even, the result is 0; if the number of 1s is odd, the result is 1. In both cases, the total number of 1s in the codeword is even. The sender sends the codeword which may be corrupted during transmission. The receiver receives a 5-bit word. The checker at the receiver does the same thing as the generator in the sender with one exception: The addition is done over all 5 bits. The result, which is called the syndrome, is just 1 bit. The syndrome is 0 when the number of Is in the received codeword is even; otherwise, it is 1.

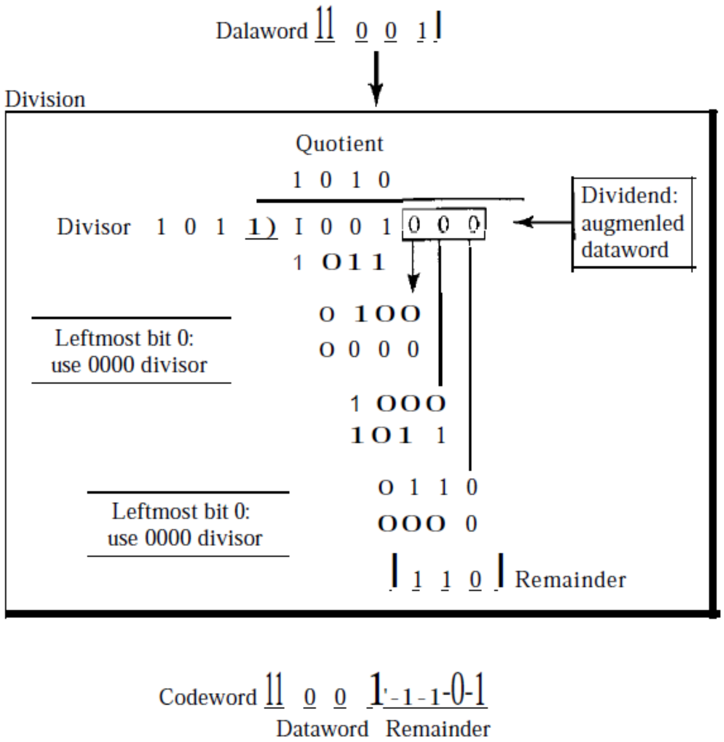


CYCLIC CODES

Cyclic Redundancy Check

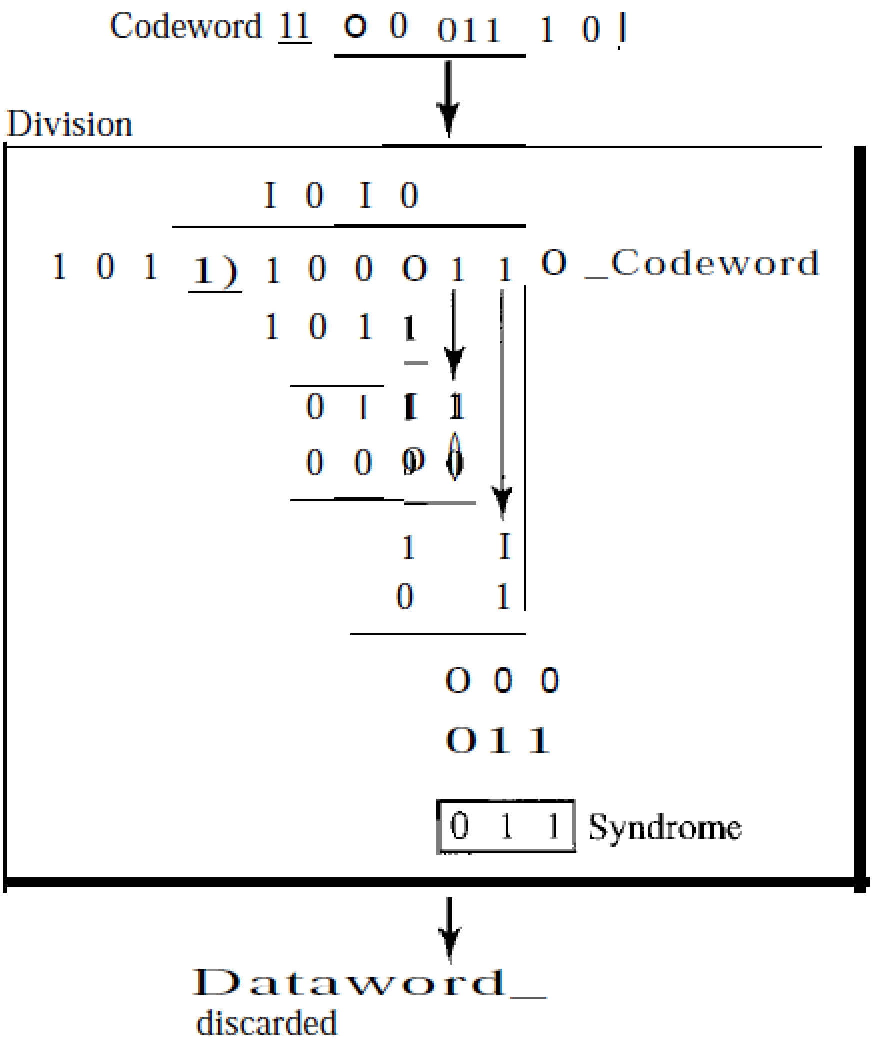


In the encoder, the dataword has *k* bits (4 here); the codeword has *n* bits (7 here). The size of the dataword is augmented by adding *n* - *k* (3 here) Os to the right-hand side of the word. The n-bit result is fed into the generator. The generator uses a divisor of size *n* - *k* + I (4 here), predefined and agreed upon. The generator divides the augmented dataword by the divisor (modulo-2 division). The quotient of the division is discarded; the remainder is appended to the dataword to create the codeword. The decoder receives the possibly corrupted codeword. A copy of all *n* bits is fed to the checker which is a replica of the generator. The remainder produced by the checker is a syndrome of *n* - *k* (3 here) bits, which is fed to the decision logic analyzer.



Decoder

The codeword can change during transmission. The decoder does the same division process as the encoder. The remainder of the division is the syndrome. If the syndrome is all Os, there is no error; the dataword is separated from the received codeword and accepted. Otherwise, everything is discarded.



CHECKSUM

Suppose our data is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers. For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12,0,6,36), where 36 is the sum of the original numbers. The receiver adds the five numbers and compares the result with the sum. If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum. Otherwise.

We can make the job of the receiver easier if we send the negative (complement) of the sum, called the *checksum*. In this case, we send (7, 11, 12,0,6, -36). The receiver can add all the numbers received (including the checksum). If the result is 0, it assumes no error; otherwise, there is an error.

b. Huffman coding+ Example - 5mark

PART C

Answer any two questions.

PART C

7. a. Compare packet switching and circuit switching. (10)

1 Mark for each differences, (1 x 10 = 10)

Circuit switching

Circuit switching requires that a circuit be set up end to end before communication begins. The result of the connection setup with circuit switching is the reservation of bandwidth all the way from the sender to the receiver. All packets follow this path and thus they cannot arrive out of order. Setting up a path in advance also opens up the possibility of reserving bandwidth in advance. If bandwidth is reserved, then when a packet arrives, it can be sent out immediately over the reserved bandwidth. If a circuit has been reserved for a particular user and there is no traffic to send, the bandwidth of that circuit is wasted. It cannot be used for other traffic. With circuit switching, the bits just flow through the wire continuously. The store-and-forward technique adds delay. Circuit switching is completely transparent. The sender and receiver can use any bit rate, format, or framing method they want to. The carrier does not know or care.

Packet switching

Packet switching does not require any advance setup. The first packet can just be sent as soon as it is available. With packet switching there is no path, so different packets can follow different paths, depending on network conditions at the time they are sent. They may arrive out of order. Packet switching is more fault tolerant than circuit switching. In fact, that is why it was invented. If a switch goes down, all of the circuits using it are terminated and no more traffic can be sent on any of them. With packet switching, packets can be routed around dead switches. With packet switching, no bandwidth is reserved, so packets may have to wait their turn to be forwarded. Packet switching does not waste bandwidth and thus is more efficient from a system-wide perspective. Packet switching does not waste bandwidth and thus is more efficient from a system-wide perspective. Packet switching uses store-and-forward transmission. A packet is accumulated in a router's memory, then sent on to the next router. With packet switching, the carrier determines the basic parameters.

Having bandwidth reserved in advance means that no congestion can occur when a packet shows up (unless more packets show up than expected). On the other hand, when an attempt is made to establish a circuit, the attempt can fail due to congestion. Thus, congestion can occur at different times with circuit switching (at setup time) and packet switching (when packets are sent).

Item	Circuit switched	Packet switched
Call setup	Required	Not needed
Dedicated physical path	Yes	No
Each packet follows the same route	Yes	No
Packets arrive in order	Yes	No
Is a switch crash fatal	Yes	No
Bandwidth available	Fixed	Dynamic
Time of possible congestion	At setup time	On every packet
Potentially wasted bandwidth	Yes	No
Store-and-forward transmission	No	Yes
Transparency	Yes	No
Charging	Per minute	Per packet

7. b. Explain GSM and GPRS technologies with neat sketches. (10)

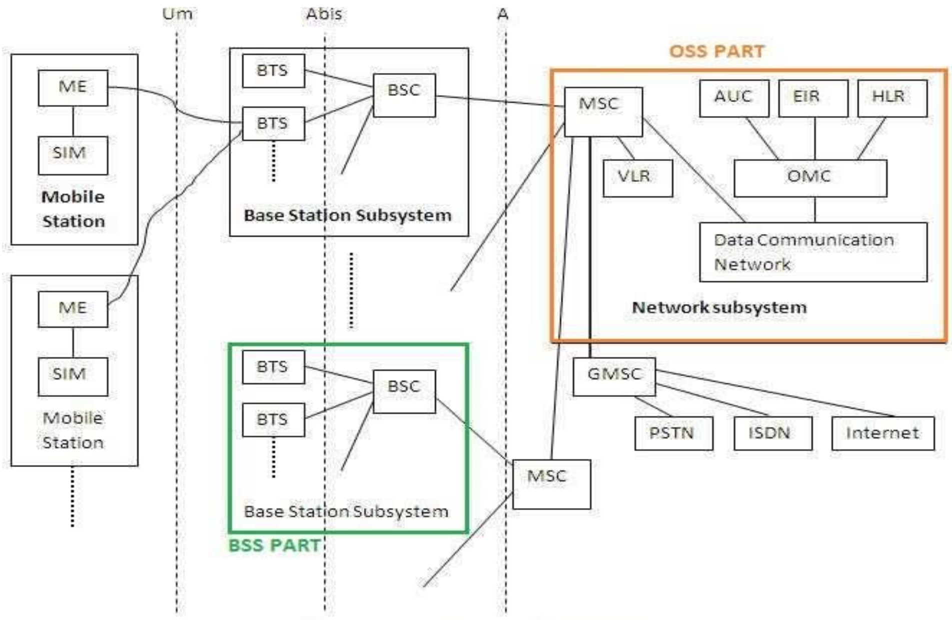
GSM – description: 3.5, Sketch: 1.5   GPRS – description: 3.5, Sketch: 1.5

1. GSM

GSM is the short form of Global System for Mobile Communications. It is called 2G or Second Generation technology. It is developed to make use of same subscriber units or mobile phone terminals throughout the world. There are various GSM standards such as GSM900, EGSM900, GSM1800 and GSM 1900; they mainly differ based on RF carrier frequency band and bandwidth.

GSM Network Architecture

GSM network is consists of Mobile station, Base station subsystem and Network and operation subsystem. Following figure depicts complete GSM system network architecture.



GSM Network Architecture

Mobile Station- This Mobile station is GSM mobile phone equipment which houses DSP, RF chip and SIM (subscriber Identity Module). This SIM is enough to carry to avail the service of GSM network. SIM contains subscriber related all the information, network with which subscriber is subscribed with and encryption related information.

Base station Subsystem- Base station subsystem houses Base Transceiver station-BTS and Base station controller-BSC. This subsystem take care of radio control related functions and provides GSM air interface for GSM mobile phones to connect with GSM network. To provide GSM service, region/city on earth is divided into various cells. The cell size is usually about 100m to about 35 km. BTS coverage is limited to this cell. Like this many BTSs cover entire region. All this BTSs are interfaced with one BSC in various ways mesh, star etc. This BSC takes care of radio frequency assignments to the mobile phones, takes care of handoff within BSS i.e. between one BTS and the other BTS.

Network Subsystem (NSS) - This subsystem provides interface between cellular system and circuit switched telephone network i.e. PSTN. It performs switching and operation & maintenance related functions. NSS takes care of call processing functions such as call setup, switching, tear down and also hand over between BSCs. NSS takes care of security and authentication related functions. There are various network elements in this subsystem. These are basically database elements.

HLR-Home Location Register, it stores permanent and temporary subscriber related information.

VLR- Visitor Location Register, it stores visitor subscriber related information about its facilities, the network it is subscribed to, and its home location and so on.

AUC- Authentication center, used to authenticate activities in the system. It holds encryption (A5 key) and authentication keys (A3 key) in both HLR and VLR.

EIR- Equipment Identification Register, it helps in security as it keeps track of equipment type available in Mobile Station or Terminal.

GSM Interfaces

Air interface between Mobile station and BTS

Abis interface between BTS and BSC

A interface between BSC and MSC

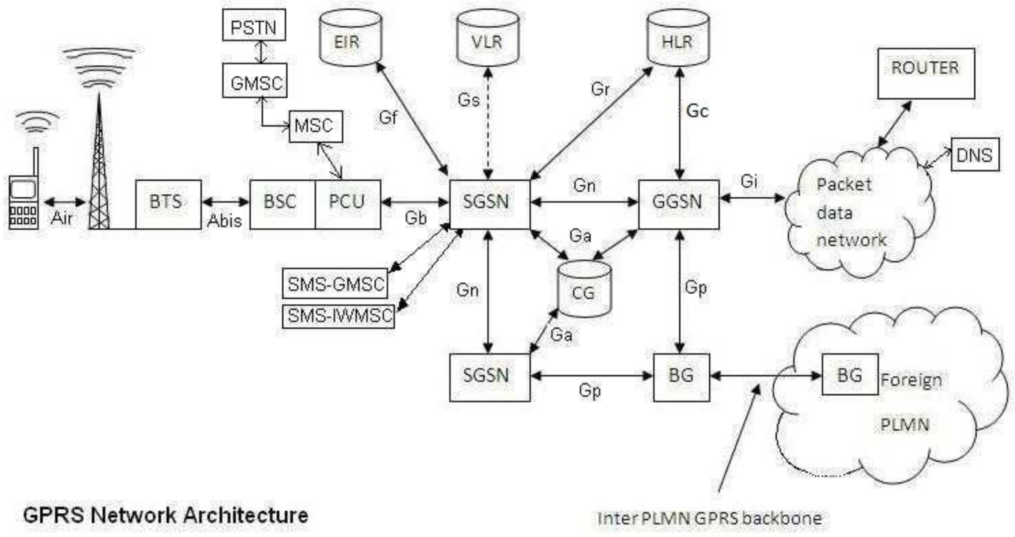
SS7 interface between MSC and PSTN

2. GPRS

GPRS is the short form of General Packet Radio Service. It is used in tandem with GSM network and mainly used for data connections through packet switched network. It is mainly used to browse/access internet in mobile devices. GPRS is GSM based packet switched technology. It requires MS (mobile subscriber) or user to support GPRS, network operator to support GPRS and services for the user to be enabled to use GPRS features. In GSM, Mobile subscriber is allocated one time slot while in GPRS it is possible to have a multislot allocated to users. Two major changes have been incorporated in GSM network to provide GPRS functionality. One is Channel coding unit is upgraded at BTS and the other is Packet Control Unit added suitably at BSC or between BSC-MSC, as mentioned below.

GPRS network Architecture

Entire GPRS network can be divided for understanding into following basic GPRS network elements.



GPRS Network Architecture

Packet Control Unit (PCU)- This PCU is the core unit to segregate between GSM and GPRS traffic. It separates the circuit switched and packet switched traffic from the user and sends them to the GSM and GPRS networks respectively which are shown in the figure above. In GPRS PCU has following two paths.

1. PCU-MSC-GMSC-PSTN
2. PCU-SGSN-GGSN-Internet (packet data network)

Serving GPRS Support Node (SGSN)- It is similar to MSC of GSM network. SGSN functions are outlined below.

- Data compression which helps minimise the size of transmitted data units.
- Authentication of GPRS subscribers.
- Routing of data to the corresponding GGSN when a connection to an external network is needed.
- Mobility management as the subscriber moves from one PLMN area to the another PLMN, and possibly one SGSN to another SGSN.
- Traffic statistics collections.

Gateway GPRS Support Node (GGSN)- GGSN is the gateway to external networks such as PDN (packet data network) or IP network. It does two main functions. It is similar to GMSC of GSM network .

- Routes mobile destined packet coming from external IP networks to the relevant SGSN within the GPRS network

- Routes packets originated from a user to the respective external IP network

Border Gateway (BG)- It is a kind of router which interfaces different operators GPRS networks. The connection between two border gateways is called GPRS tunnel. It is more secure to transfer data between two operators using their own PLMN networks through a direct connection rather than via the public Internet which is less secure.

Charging Gateway (CG)- GPRS users have to be charged for the use of the network, this is taken care by Charging gateway. Charging is done based on Quality of Service or plan user has opted either prepaid or post paid. This charging data generated by all the SGSNs and GGSNs in the network is referred to as Charging Data Records (CDRs). The Charging Gateway (CG) collects all of these CDRs, processes the same and passes it on to the Billing System.

DNS server- Connected at ISP location or at IP network. It converts domain name to IP addresses required to establish internet connection and to deliver web pages on user's terminal screen.

Intra PLMN- An IP based network inter-connecting all the above mentioned GPRS network elements in one PLMN area.

Inter PLMN- Connection between two different PLMN areas.

8. a. Explain error handling using Hamming codes with necessary example. (10)

Hamming Code – description: 7, Example: 3

Hamming codes are a family of linear error-correcting codes that generalize the Hamming (7,4)-code, and were invented by Richard Hamming. Hamming codes can detect up to two-bit errors or correct one-bit errors without detection of uncorrected errors. Hamming codes are perfect codes, that is, they achieve the highest possible rate for codes with their block length and minimum distance of three.

Calculating the Hamming Code

The key to the Hamming Code is the use of extra parity bits to allow the identification of a single error. Create the code word as follows:

1. Mark all bit positions that are powers of two as parity bits. (positions 1, 2, 4, 8, 16, 32, 64, etc.)
2. All other bit positions are for the data to be encoded. (positions 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, etc.)

3. Each parity bit calculates the parity for some of the bits in the code word. The position of the parity bit determines the sequence of bits that it alternately checks and skips.
   Position 1: check 1 bit, skip 1 bit, check 1 bit, skip 1 bit, etc. (1,3,5,7,9,11,13,15,...)
   Position 2: check 2 bits, skip 2 bits, check 2 bits, skip 2 bits, etc. (2,3,6,7,10,11,14,15,...)
   Position 4: check 4 bits, skip 4 bits, check 4 bits, skip 4 bits, etc. (4,5,6,7,12,13,14,15,20,21,22,23,...)
   Position 8: check 8 bits, skip 8 bits, check 8 bits, skip 8 bits, etc. (8-15,24-31,40-47,...)
   Position 16: check 16 bits, skip 16 bits, check 16 bits, skip 16 bits, etc. (16-31,48-63,80-95,...)
   Position 32: check 32 bits, skip 32 bits, check 32 bits, skip 32 bits, etc. (32-63,96-127,160-191,...)
   etc.
4. Set a parity bit to 1 if the total number of ones in the positions it checks is odd. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

Example:

A byte of data: 10011010

Create the data word, leaving spaces for the parity bits: _ _ 1 _ 0 0 1 _ 1 0 1 0

Calculate the parity for each parity bit (a ? represents the bit position being set):

- Position 1 checks bits 1,3,5,7,9,11:
  ? _ **1** _ **0** 0 **1** _ **1** 0 **1** 0. Even parity so set position 1 to a 0: **0** _ **1** _ **0** 0 **1** _ **1** 0 **1** 0
- Position 2 checks bits 2,3,6,7,10,11:
  0 **? 1** _ 0 **0 1** _ 1 **0 1** 0. Odd parity so set position 2 to a 1: 0 **1 1** _ 0 **0 1** _ 1 **0 1** 0
- Position 4 checks bits 4,5,6,7,12:
  0 1 1 **? 0 0 1** _ 1 0 1 **0**. Odd parity so set position 4 to a 1: 0 1 1 **1 0 0 1** _ 1 0 1 **0**
- Position 8 checks bits 8,9,10,11,12:
  0 1 1 1 0 0 1 **? 1 0 1 0**. Even parity so set position 8 to a 0: 0 1 1 1 0 0 1 **0 1 0 1 0**
- Code word: 011100101010.

Detection and correction of a bad bit

The above example created a code word of 011100101010. Suppose the word that was received was 011100101110 instead. Then the receiver could calculate which bit was wrong and correct it. The method is to verify each check bit. Write down all the incorrect parity bits. Doing so, you will discover that parity bits 2 and 8 are incorrect. Hence bit position 10 is the location of the bad bit. In general, check each parity bit, and add the positions that are wrong, this will give the location of the bad bit.

8. b. Describe about CRC encoding and decoding. (10)

CRC – description: 7, Example: 3

Cyclic redundancy check (CRC) codes

– A type of linear block codes

• Generally, not cyclic, but derived from cyclic codes

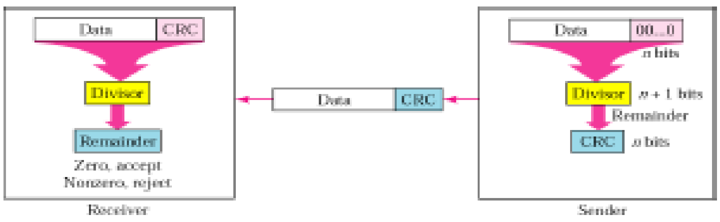
– A systematic error detecting code

• A group of error control bits (which is the remainder of a polynomial division of a message polynomial by a generator polynomial) is appended to the end of the message block

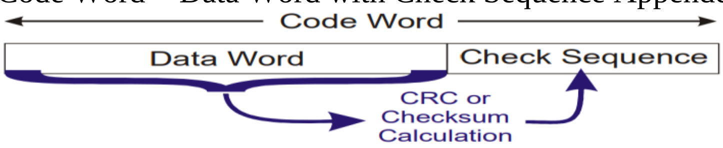
• With considerable burst-error detection capability

– The receiver generally has the ability to send retransmission requests back to the data source through a feedback channel.

CRC Generator and Checker

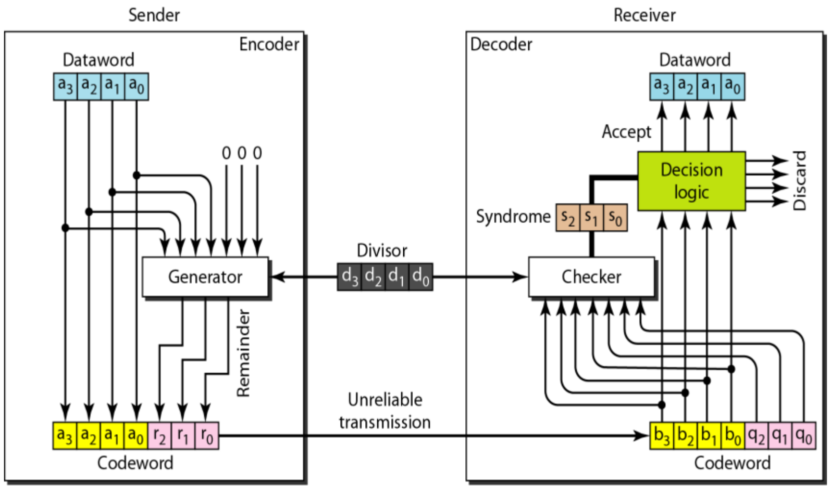


- Compute check sequence when data is transmitted or stored
  - Data Word: the data you want to protect (can be any size; often Mbytes)
  - Check Sequence: the result of the CRC or checksum calculation
  - Code Word = Data Word with Check Sequence Appended



- To check data integrity:
  - Retrieve or receive Code Word
  - Compute CRC or checksum on the received Data Word
  - If computed value equals Check Sequence then no data corruption found

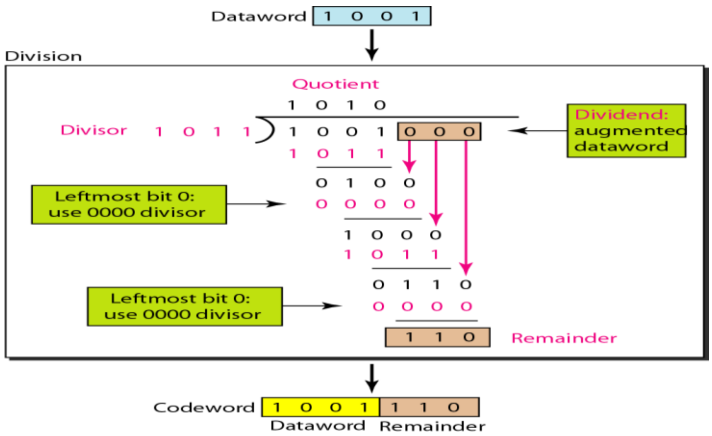
CRC encoder and decoder



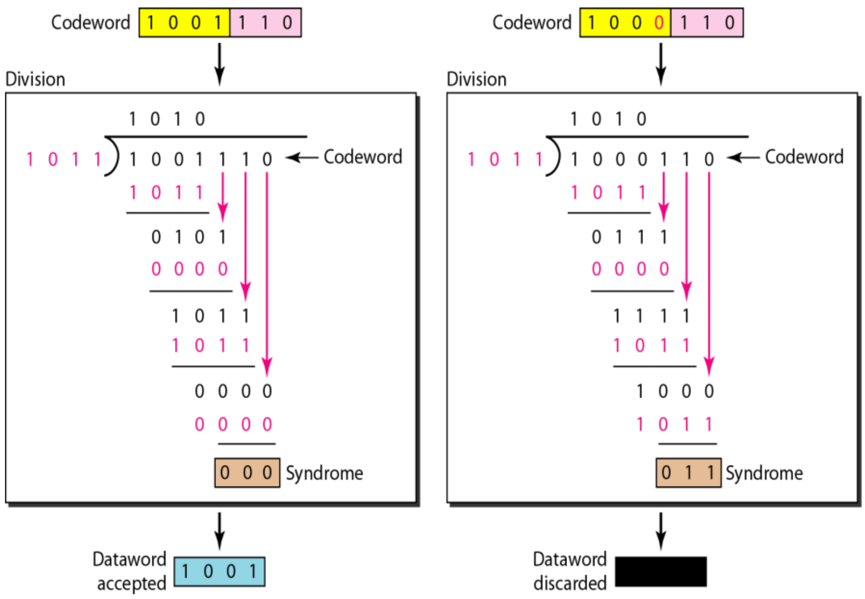
The dataword has k bits (4 here); the codeword has n bits (7 here); The generator uses a divisor of size n - k + 1 (4 here).

EXAMPLE

Compute check sequence



To check data integrity



9. a. Explain in detail about Wi-Fi and WiMax. (10)

WiFi – description: 4 WiMax – description: 4 WiFi and Wi Max Comparison - 2

Wi-Fi or **WiFi** is a technology for wireless local area networking with devices based on the IEEE 802.11 standards. Devices that can use Wi-Fi technology include personal computers, video-game consoles, smartphones, digital cameras, tablet computers, smart TVs, digital audio players and modern printers. Wi-Fi compatible devices can connect to the Internet via a WLAN and a wireless access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometres achieved by using multiple overlapping access points. Wi-Fi most commonly uses the 2.4 gigahertz (12 cm) Ultra High Frequency and 5 gigahertz (6 cm) Super High Frequency ISM radio bands. Having no physical connections, it is more vulnerable to attack than wired connections, such as Ethernet.

WiMAX (**Worldwide Interoperability for Microwave Access**) is a family of wireless communication standards based on the IEEE 802.16 set of standards, which provide multiple physical layer (PHY) and Media Access Control (MAC) options. The name "WiMAX" was created by the **WiMAX Forum** to promote conformity and interoperability of the standard, including the definition of predefined system profiles for commercial vendors. The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL". IEEE 802.16m or WirelessMAN-Advanced was a candidate for the 4G, in competition with the LTE Advanced standard. WiMAX was initially designed to provide 30 to 40 megabit-per-second data rates, with the 2011 update providing up to 1 Gbit/s[3] for fixed stations.

Comparison

WiMAX is similar to the wireless standard known as Wi-Fi, but on a much larger scale and at faster speeds. We can compare it with Wi-Fi based on the following factors.

1. IEEE Standards

Wi-Fi is based on IEEE 802.11 standard whereas WiMAX is based on IEEE 802.16. However, both are IEEE standards.

2. Range

Wi-Fi typically provides local network access for a few hundred feet with the speed of up to 54 Mbps, a single WiMAX antenna is expected to have a range of up to 40 miles with the speed of 70 Mbps or more. As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks.

3. Scalability

Wi-Fi is intended for LAN applications, users scale from one to tens with one subscriber for each CPE (Consumer premises equipment) device. Fixed channel sizes (20MHz).

WiMAX is designed to efficiently support from one to hundreds of Consumer premises equipments (CPE)s, with unlimited subscribers behind each CPE. Flexible channel sizes from 1.5MHz to 20MHz.

4. Bit rate

Wi-Fi works at 2.7 bps/Hz and can peak up to 54 Mbps in 20 MHz channel.

WiMAX works at 5 bps/Hz and can peak up to 100 Mbps in a 20 MHz channel.

5. Quality of Service

Wi-Fi does not guarantee any QoS but WiMax will provide your several level of QoS.

As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks. Wi-Fi does not provide ubiquitous broadband while WiMAX does.

Comparison Table

Feature	**WiMax (802.16a)**	**Wi-Fi (802.11b)**	**Wi-Fi (802.11a/g)**
Primary Application	Broadband Wireless Access	Wireless LAN	Wireless LAN
Frequency Band	Licensed/Unlicensed 2 G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	Adjustable 1.25 M to 20 MHz	25 MHz	20 MHz

Half/Full Duplex	Full	Half	Half
Radio Technology	OFDM (256-channels)	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth Efficiency	<=5 bps/Hz	<=0.44 bps/Hz	<=2.7 bps/Hz
Modulation	BPSK, QPSK, 16-, 64-, 256-QAM	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	Convolutional Code Reed-Solomon	None	Convolutional Code
Encryption	Mandatory- 3DES Optional- AES	Optional- RC4 (AES in 802.11i)	Optional- RC4 (AES in 802.11i)
Mobility	Mobile WiMax (802.16e)	In development	In development
Mesh	Yes	Vendor Proprietary	Vendor Proprietary
Access Protocol	Request/Grant	CSMA/CA	CSMA/CA

9. b. What are BCH codes and RS codes? Explain. (10)

BCH – description: 5 RS codes – description: 5

BCH codes or **Bose–Chaudhuri–Hocquenghem codes**

- A class of cyclic error-correcting codes that are constructed using polynomials over a finite field(also called *Galois field*).
- BCH codes were invented in 1959 by French mathematician Alexis Hocquenghem, and independently in 1960 by Raj Bose and D. K. Ray-Chaudhuri. The name *Bose–Chaudhuri–Hocquenghem* (and the acronym *BCH*) arises from the initials of the inventors' surnames.
- One of the key features of BCH codes is that during code design, there is a precise control over the number of symbol errors correctable by the code. It is possible to design binary BCH codes that can correct multiple bit errors.

- Another advantage of BCH codes is the ease with which they can be decoded, namely, via an algebraic method known as syndrome decoding. This simplifies the design of the decoder for these codes, using small low-power electronic hardware.
- BCH codes are used in applications such as satellite communications, compact disc players, DVDs, disk drives, solid-state drives and two-dimensional bar codes.

Reed–Solomon codes

- A group of error-correcting codes that were introduced by Irving S. Reed and Gustave Solomon.
- In coding theory, the Reed–Solomon code belongs to the class of non-binary cyclic error-correcting codes.
- The Reed–Solomon code is based on univariate polynomials over finite fields.
- It is able to detect and correct multiple symbol errors.
- By adding t check symbols to the data, a Reed–Solomon code can detect any combination of up to t erroneous symbols, or correct up to $\lfloor t/2 \rfloor$ symbols.
- As an erasure code, it can correct up to t known erasures, or it can detect and correct combinations of errors and erasures.
- Reed–Solomon codes are also suitable as multiple-burst bit-error correcting codes, since a sequence of $b + 1$ consecutive bit errors can affect at most two symbols of size b. The choice of t is up to the designer of the code, and may be selected within wide limits.
- They have many applications, the most prominent of which include consumer technologies such as CDs, DVDs, Blu-ray Discs, QR Codes, data transmission technologies such as DSL and WiMAX, broadcast systems such as DVB and ATSC, and storage systems such as RAID 6.
- They are also used in satellite communication.

****