WINTER – 2022 EXAMINATION

Subject Name: Computer Networking and Data Comm. **Subject Code:** 22634

Model Answer

Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills.
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.
8) As per the policy decision of Maharashtra State Government, teaching in English/Marathi and Bilingual (English + Marathi) medium is introduced at first year of AICTE diploma Programme from academic year 2021-2022. Hence if the students in first year (first and second semesters) write answers in Marathi or bilingual language (English +Marathi), the Examiner shall consider the same and assess the answer based on matching of concepts with model answer.

Q. No.	Sub Q. N.	Answers	Marking Scheme
1	(A)	**Attempt any FIVE of the following:**	10- Total Marks
	(a)	**Define Bit rate and Baud rate**	2M
	Ans:	bit rate : It is defined as the number of bits transmitted per second. baud rate : It is defined as the number of signal units per second.	1 M each

	(b)	**Classify networks on the basis of transmission technologies.**	**2M**
	Ans:	Classification of networks on the basis of transmission technologies 1. Broadcast Network **2.** Point-to-Point Network	**1M Each**
	(c)	**State the function of transport layer in TCP/IP protocol suite**	**2M**
	Ans:	**Function of transport layer in TCP/ IP protocol suite** 1. Process to process delivery 2. End-to-end Connection between hosts 3. Multiplexing and Demultiplexing 4. Congestion Control 5. Data integrity and Error correction **6.** Flow control	**Any two valid function 1M each**
	(d)	**Name the layer of the OSI model that is responsible for moving of data in and out of physical link in network. State its functions.**	**2M**
	Ans:	**Physical layer** is responsible for moving of data in and out of physical link in network. Function of Physical layer 1. It defines the physical characteristics and functions of the physical devices and interfaces so that transmission can occur. 2. It defines the procedure of encoding of the bits. 3. It states the data transmission rate and the duration of a bit. 4. It defines the topology. 5. It also states the direction of transmission	**Name of layer 1M** **Any one valid function 1M**
	e)	**State the application of infrared waves**	**2M**

	Ans:	**Application of infrared waves** **1.** Remote Control 2. Optical Fibres 3. Thermal Imaging Cameras 4. Infrared Cookers 5. Electric Heaters **6.** Infrared Lamps	**Any 2 application 1M each**
	f)	**State the application of firewall.**	**2M**
	Ans:	**Application of firewall** • A fire wall is a network security device,either hardware or software-based,which monitors all incoming and out going traffic and based on a defined set of security rules it accepts ,rejects or drops that specific traffic. • A fire wall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet • A fire wall is a part of computer system or network that is designed to block unauthorized access while permitting authorized communication • A firewall is placed at the entry/exit point of the network	**Any one Valid application point 2M each**
	g)	**State the need for IPv6.**	**2M**
	Ans:	**Need for IPv6** The Internet has experienced a phenomenal increase of devices accessing the Internet. Because of this increase, IPv4 addresses are running out.Traditional model of classful addressing does not allow the address space to be used to its maximum potential.The solution is IPv6 which can accommodate the increased demand by providing a much larger address space IPv6 has 128-bit address space or 4 times more address bits compared to IPv4's 32-bit address space. This large address space will provide enough address space for many decades to come.	**2M**

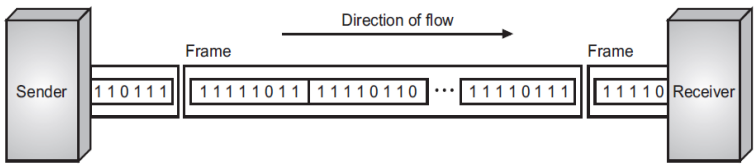
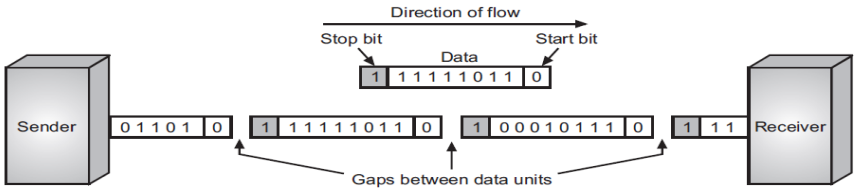
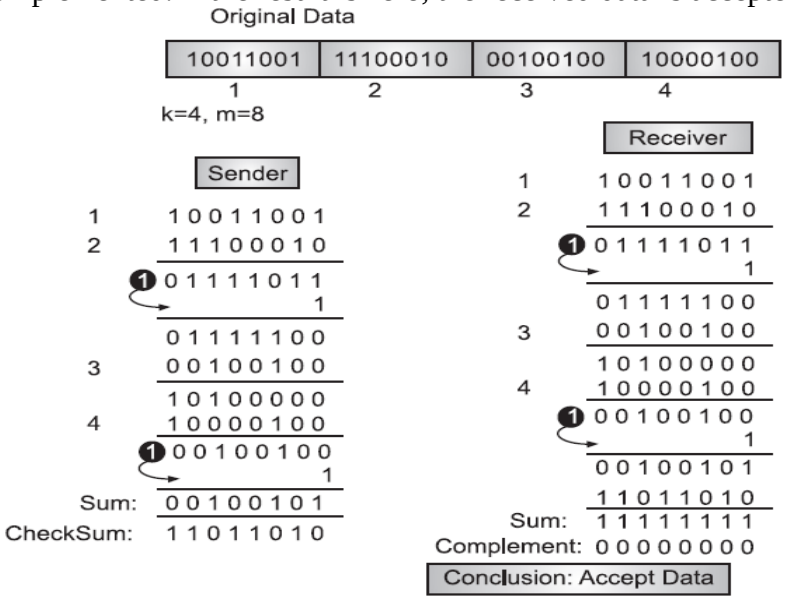
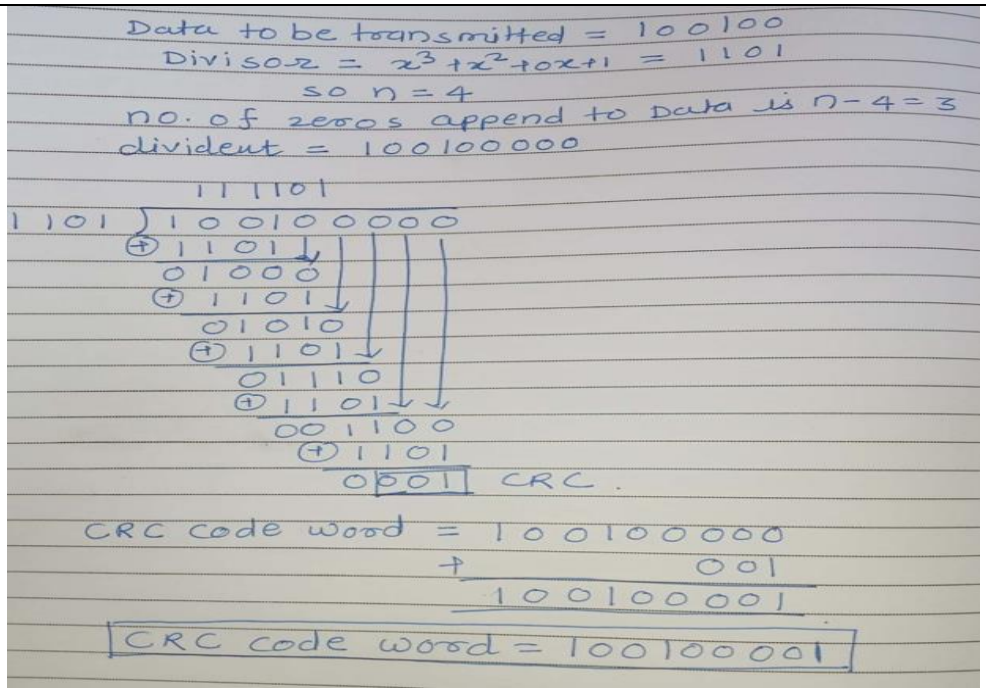
Q. No.	Sub Q. N.	Answers	Marking Scheme
2		**Attempt any THREE of the following:**	**12- Total Marks**
	a)	**Name the components of data communication system . State the function of each component.**	**4M**
	Ans:	Following are the building blocks (components) of Data Communication System: 1. **Message**:The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video. 2. **Sender**:The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on. 3. **Receiver**: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, etc 4. **Transmission medium**: the transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fibre-optic cable, and radio waves. 5. **Protocol:** A protocol is a set of rules that governs data communication.	**2M Explanation**
	b)	**Explain the terms Synchronous, and Asynchronous transmission of data with a neat diagram**	**4M**
	Ans:	**Synchronous Data Transmission:** 	**2M each for Synchronous & Asynchronous**

		Fig. : Synchronous Data Transmission • Synchronous data transmission is a data transfer method in which is a continuous stream of data signals accompanied by timing signals. • Synchronous transmission needs synchronization between transmitter and receiver in order to allow communication between the two. The transmitter and receiver share a common clock pulse so as to have synchronization in communication. This means data will be transmitted between the transmitter and receiver only after a constant time interval. • It allows the transmission of data in the form of frames or blocks. Thus, a huge data amount can be transmitted between transmitter and receiver once the clock pulse is sent **Asynchronous Data Transmission:**  Fig.:Asynchronous Data Transmission • Asynchronous transmission is a type of serial transmission that follows a non-synchronized form of communication. Thus start and stop bits are required in order to intimate the receiver about the beginning and end of the data stream. • It does not use a clock to synchronize data between the source and destination. • This transmission method sends one character time. In this method, before the transmission process begins, each character sends the start bit. After sending the character, it also sends the stop bit Thus it is also known as start stop transmission	**Data Transmission with Diagram**
	c)	**State the functions performed by the Network layer and application layer in a TCP/I protocol.**	**4M**
	Ans:	**Functions of Network Layer:** **(i) Subnet Traffic Control:** Network layer routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills	**2M each for Functio**

		up. **(ii) Logical-physical Address Mapping:** It translates logical addresses, or names, into physical addresses. **(iii) Subnet Usage Accounting:** It has accounting functions to keep track of frames forwarded by subnet intermediate systems. **(iv) Internetworking:** One of the main responsibilities of network layer is to provide internetworking between different networks. It provides logical connection between different types of network. It is because of this layer, we can combine various different networks to form a bigger network. **(v) Logical Addressing:** Large number of different networks can be combined together to from bigger networks or internetwork. In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. Such an address distinguishes each device uniquely and universally. **(vi) Routing:** When independent networks or links are combined together to create internet works, multiple routes are possible from source machine to destination machine. The network layer protocols determine which route or path is best from source to destination. This function of network layer is known as routing. Routes frames among networks. **(vii) Packetizing:** The network layer receives the data from the upper layers and creates its own packets by encapsulating these packets. The process is known as packetizing. This packetizing in done by Internet Protocol (IP) that defines its own packet format. **(viii) Fragmentation:** Fragmentation means dividing the larger packets into small fragments. The maximum size for a transportable packet in defined by physical layer protocol. For this, network layer divides the large packets into fragments so that they can be easily sent on the physical medium. If it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and reassembly at the destination station. **Functions Application Layer:** **(i) Network Virtual Terminal:** It allows a user to log on to a remote host. **(ii) File Transfer, Access and Management (FTAM):** This application allows a user to access files in remote computer (to make changes or read data), to retrieve files from a remote computer, and to manage or control files in a remote computer.	**ns of Networ k Layer & Applica tion Layer**

		(iii) Mail Service: This application provides the basis for e-mail forwarding and storage. **(iv) Remote Logins:** This layer allows logging into a host which is remote. **(v) Network Abstraction:** Provides an abstraction of the underlying network to an end user and an application. **(vi) Directory Services:** This application provides distributed database sources and access for global information about various objects and services.	
	d)	**Explain checksum error detection mechanism with a suitable example.**	**4M**
	Ans:	**Checksum:** 1.Checksum is an error-detecting technique in data communication that can be applied to a message of any length. In the Internet, this technique is mostly used at the network and transport layer rather than the data link layer. 2.In checksum error detection scheme, the data is divided into k segments each of m bits. In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum. 3.The checksum segment is sent along with the data segments. At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented. If the result is zero, the received data is accepted; otherwise discarded.  	**2M Explanation and 2M Example**

Q. No.	Sub Q. N.	Answers	Marking Scheme
	a)	**Name the layer of the OSI model that perform the following functions** **i) Bitrate control** **ii) Framing** **iii) Logical Addressing** **iv) Encryption / Decryption**	**4M**
	Ans:	i) Bitrate control : Physical layer ii) Framing : data link layer iii) Logical Addressing : network layer **iv)** Encryption / Decryption : presentation layer	**1M For each correct answer**
	b)	**Calculate the CRC for the frame of data to be transmitted in 100100 and the generator polynomial is $x^3+ x^2 + 1$. Generate the Codeword for the transmitted frame.**	**4M**
			**Correct divisor 1M & Correct calculation of CRC code word is 3M**

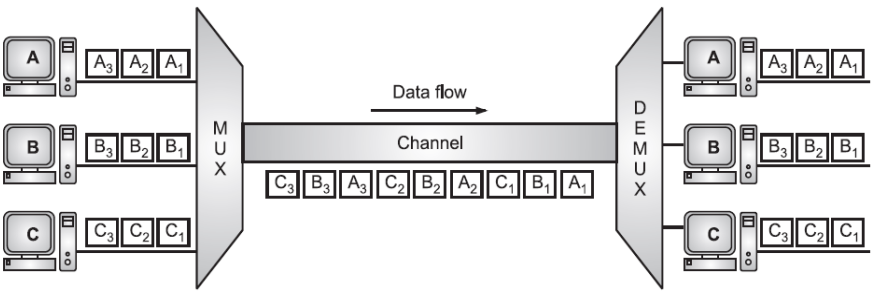
	c)	**On which layer of the O.S.I. model do the following devices work.** **i) Bridge** **ii) Routes** **iii) Gateway** **iv) Hub**	**4M**
	Ans:	i) Bridge: A bridge operates at the data link layer. ii) Routes : The router is mainly a Network Layer device. iii) Gateway : it can operate at any network layer iv) Hub : A hub operates at the physical layer	**1M For each**
	d)	**Compare classless and classful addressing. State the disadvantages of classful addressing.**	**4M**
	Ans:	Difference between Classful Addressing and Classless Addressing	**Any 3 valid differences 3M** **1M for any one valid disadvantage**

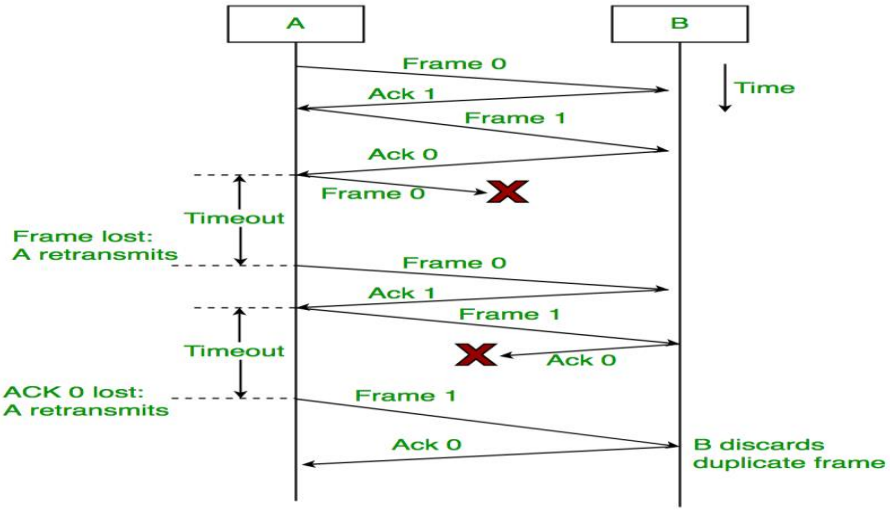
Sr. No.	**Parameter**	**Classful Addressing**	**Classless Addressing**
1.	**Basics**	In Classful addressing IP addresses are allocated according to the classes- A to E.	Classless addressing came to replace the classful addressing and to handle the issue of rapid exhaustion of IP addresses.
2.	**Practical**	It is less practical.	It is more practical.
3.	**Network ID and Host ID**	The changes in the Network ID and Host ID depend on the class.	There is no such restriction of class in classless addressing.

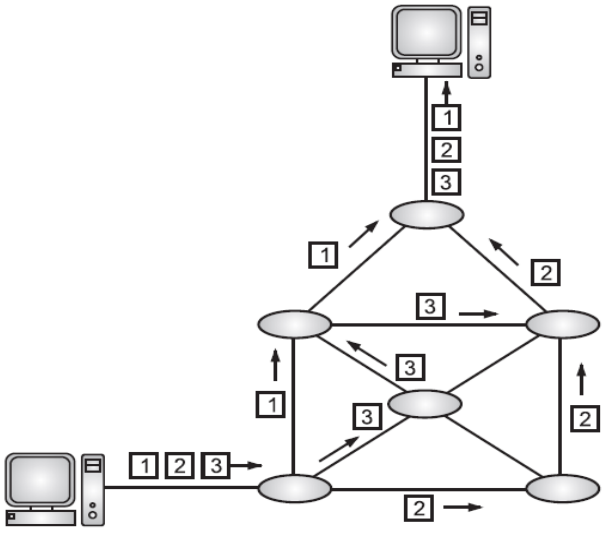
4.	**VLSM**	It does not support the Variable Length Subnet Mask (VLSM).	It supports the Variable Length Subnet Mask (VLSM).
5.	**Bandwidth**	Classful addressing requires more bandwidth. As a result, it becomes slower and more expensive as compared to classless addressing.	It requires less bandwidth. Thus, fast an less expensive as compared to classful addressing.
6.	**CIDR**	It does not support Classless Inter-Domain Routing (CIDR).	It supports Classless Inter-Domain Routing (CIDR).
7.	**Updates**	Regular or periodic updates	Triggered Updates
8.	**Troubleshooting and Problem detection**	Troubleshooting and problem detection are easy than classless addressing because of the division of network, host and subnet parts in the address.	It is not as easy compare to classful addressing.
9.	**Division of Address**	• Network • Host • Subnet	• Host • Subnet

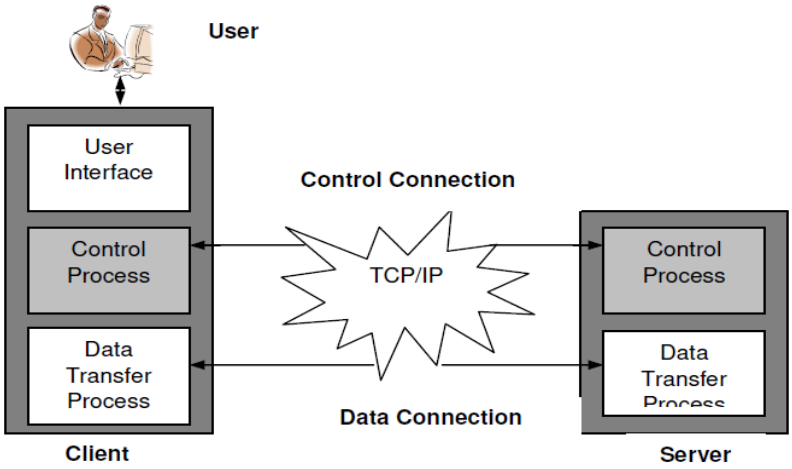
Disadvantage of Classful Addressing:

1. Class A with a mask of 255.0.0.0 can support 128 Network, 16,777,216 addresses per network and a total of 2,147,483,648 addresses.
2. Class B with a mask of 255.255.0.0 can support 16,384 Network, 65,536 addresses per network and a total of 1,073,741,824 addresses.
3. Class C with a mask of 255.255.255.0 can support 2,097,152 Network, 256 addresses per network and a total of 536,870,912 addresses.

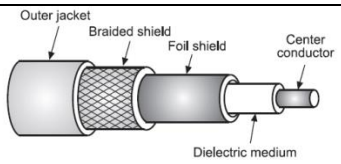
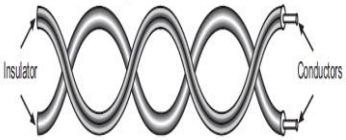
Q. No.	Sub Q. N.	Answers	Marking Scheme
4		**Attempt any THREE of the following:**	**12- Total Marks**
	(a)	**Explain the principle of working of TDM with suitable diagram**	**4M**
		Time Division Multiplexing (TDM): 1.In Time-division multiplexing all signals operate with same frequency at different times. 2.TDM is the digital multiplexing technique. In TDM, the channel/link is not divided on the basis of frequency but on the basis of time. Total time available in the channel is divided between several users. 3.Each user is allotted a particular a time interval called time slot or time slice during which the data is transmitted by that user. Thus each sending device takes control of entire bandwidth of the channel for fixed amount of time. In TDM the data rate capacity of the transmission medium should be greater than the data rate required by sending or receiving devices. 4. In TDM all the signals to be transmitted are not transmitted simultaneously. Instead, they are transmitted one-by-one. Thus, each signal will be transmitted for a very short time. One cycle or frame is said to be complete when all the signals are transmitted once on the transmission channel. 5.The TDM system can be used to multiplex analog or digital signals, however it is more suitable for the digital signal multiplexing. The TDM signal in the form of frames is transmitted on the common communication medium.  **Fig.: Time Division Multiplexing (TDM)**	**2M Diagram and 2M Explanation**

	(b)	**Explain stop and wait protocol used in flow control.**	**4M**
	Ans:	1. One bit sliding window uses Stop and Wait protocol for delivery of data frames. 2.The sender and receiver's windows size is 1 and the frames are alternately numbered 3.One bit sliding window uses Stop and Wait protocol .4.Sender transmit a frame with sequence number and waits for acknowledgment from the receiver. 5.Receiver send back an acknowledgement with sequence number. 6.If sequence number of acknowledgement matches with sequence number of frame. 7.Sender transmit the next frame. 8.Else sender re-transmit the previous frame. 9.Its bidirectional protocol.(full duplex communication)  **Normal Operation:**In normal operation thesender sends a frame and waits for acknowledgement from receiver .The acknowledgement should be received before the timer for the frame expires.The sequence number of acknowledgement should match the sequence number of next frame to be transmitted.If it matches the next frame is transmitted otherwise previous frame is transmitted **Lost or Damaged frame :.**When the receiver receives a damaged frame it discards it which means the frame is lost .The receiver remains silent about the lost frame .After the timer expires for that frame the sender retransmits the same frame . **Lost or Delayed acknowledgement:**In case of lost or delayed acknowledgement after the timer for the frame expires the sender retransmits the frame .The receiver takes care of discarding duplicate copy	**2M Diagram & 2M Explanation**

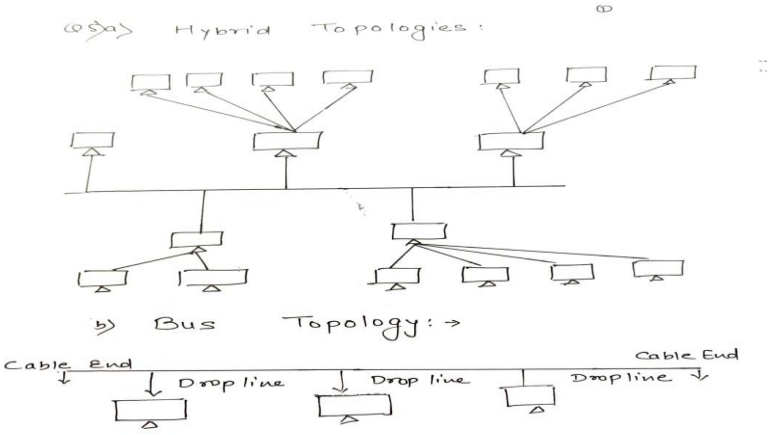
	(c)	**With neat diagram explain the concept of datagram approach of switching.**	**4M**
	Ans:	**Datagram Packet Switching:** In a datagram network, each packet is treated independently of all others. Datagram switching is normally done at the network layer. Figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers. • In this example, all four packets (or datagrams) belong to the same message, may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. • This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. • In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application. • The datagram networks are sometimes referred to as connectionless networks. The term connectionless here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. • Datagrams can contain the full destination address rather than using some number • There is no set up phase required for the datagram circuits. This means that no resources are consumed. • If any fault or loss occurs on a communication line, the datagrams circuits are capable of compensating for it.  **Fig.: Datagram Packet Switching**	**2M Diagram &2M Explanation**

	(d)	**Explain the concept of FTP with neat diagram.**	**4M**
	Ans:	**FTP (File Transfer Protocol) :**FTP is a standard mechanism provided by the Internet for copying a file from one host to the other It uses the services of TCP **User Interface :**Most operating systems provide user interface to to access the services of FTP. The interface prompts user for appropriate input **Control Connection :**The well known port 21 is used for control connection . It is opened once and maintained during entire FTP session **Data Connection** :The well known port 20 is used for data connection .The connection can be opened and closed multiple times. The data connection in FTP means one of the following 1) A file can be copied from server to client under the supervision of RETR command 2) A file is transferred from client to server under the supervision of STOR command 3) A list of directory or filename is sent to the client under the supervision of LIST command For communication over data connection client must define the type of file , structure of data and transmission mode **Architecture of FTP:**  	**2M Concept & 2M Architecture and Diagram of FTP**
	(e)	**Compare coaxial cable and twisted pair cable on the basis of-** **i) Bandwidth** **ii) Electromagnetic interference** **iii) Construction** **iv) applications**	**4M**

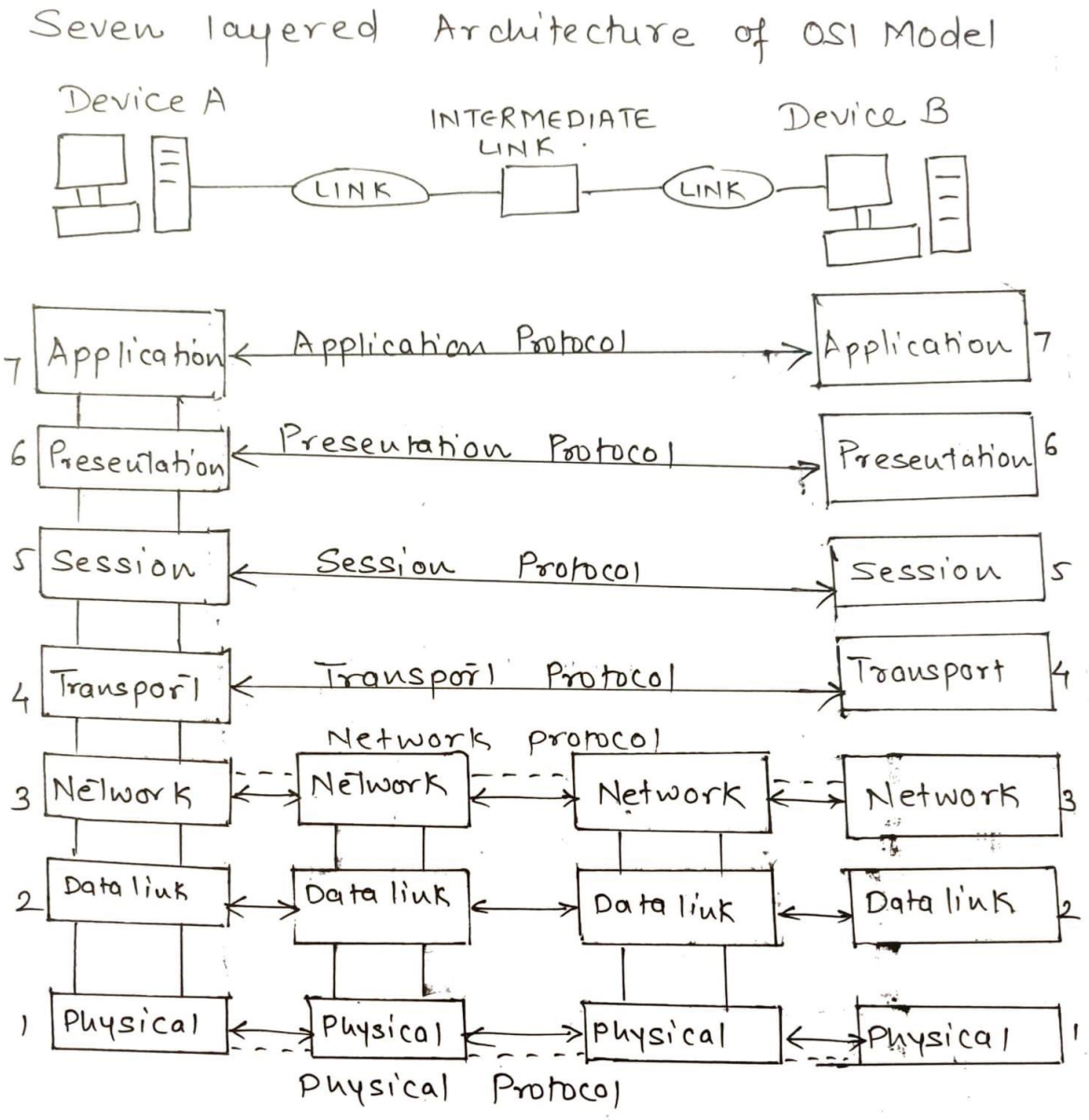
Ans:

Parametes	coaxial cable	Twisted pair cable
Bandwidth	Bandwidth is high which is 300 to 400 MHz.	Bandwidth is low which is 3 to 4 MHz.
Electromagnetic interference	Less affected by EMI and noise.	Affected by EMI and noise.
Construction		
applications	1. The use of coaxial cable started in analog telephone networks where a single coaxial network could carry 10,000 voice signals. 2. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. 3. Most common use is in cable TV. 4. Coaxial cabling is often used in heavy industrial environments where motors and generators produce a lot of electromagnetic interference (EMI), and where more expensive fiber-optic cabling is unnecessary because of the slow data rates needed.	1. TP cables are used in telephone lines to provide voice and data channels. 2. The line that connects subscribers to the central telephone office is most commonly UTP cable. 3. The DSL lines that are used by the telephone companies to provide high data rate connections also use high bandwidth capability UTP cable. 4. Local Area Network (LAN) also uses twisted-pair cable.

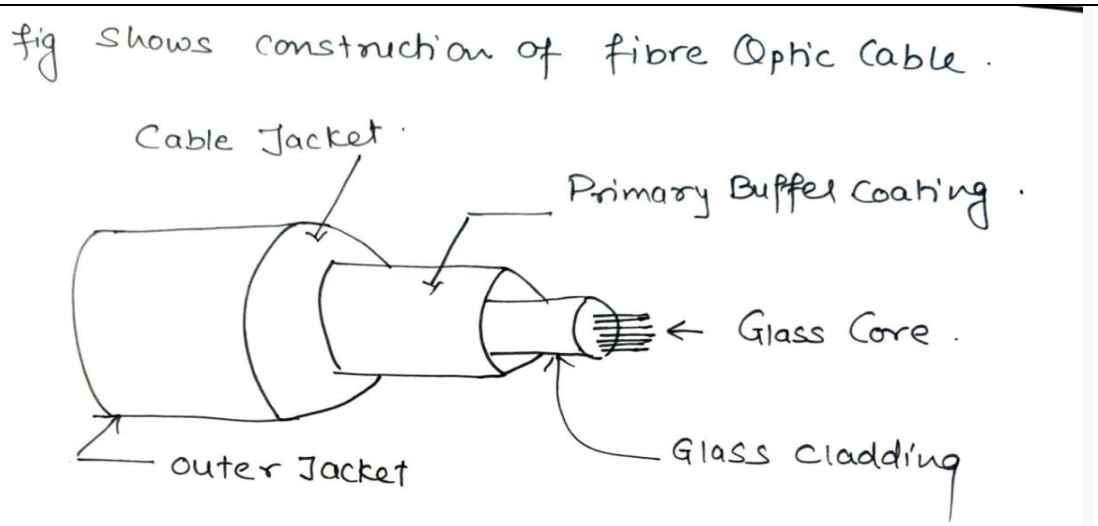
1M each for correct comparison point

Q. No.	Sub Q. N.	Answers	Marking Scheme
5.		**Attempt any TWO of the following:**	**12- Total Marks**
	a)	**Draw a diagram and describe the following topologies stating their applications.** **i) Hybrid** **ii) Bus**	**6M**
	Ans:	**Figure Illustrate the diagram for following topologies** **Hybrid Topology** • A hybrid topology is a kind of network topology that is a combination of two or more network topologies, such as Mesh topology, Bus topology**,** and Ring topology**.** • Its usage and choice are dependent on its deployments and requirements like the performance of the desired network, and the number of computers, their locations • This topology presents a blend of characteristics of all basic types. In this type, whole Computer Network is divided into Network Segments. Each Network Segments connects with Network Backbone  	**3M** **Diagram 1m** **explaination**

		Application of Hybrid Topology • Automated Industry • Banks • Multi National Offices • Educational Institute • Research Organization **Bus Topology** • Computers and peripherals are called nodes and are each connected to a single cable on which data can be sent. • A bus network topology has a terminator on each end. These are needed to ensure that the network functions correctly. **Bus Topology Application** • A bus topology is used to connect two floors using a single line. • A bus topology is used by an Ethernet network • In this type of network topology, one computer works like a server whereas the other works as a client. • The main function of the server is to exchange information between different client computers. • Bus topology network is used to add the printers, I/O devices in the offices or home.	**1M** **1M for any 2 application of each topology**
	b)	**Draw the seven layered architecture of the OSI model and explain.**	**6M**

	Ans:	 The working of the 7 Layers of the OSI Model are as following **Physical Layer:** It co-ordinates the functions required to transmit bit stream over physical medium. It Provides physical interface for transmission of information. . It Defines rules by which bits are passed from one system to another on a physical communication medium. It Covers all -mechanical, electrical, functional and procedural -aspects for physical	**2M for diagram** **4m for**

		communication. **Data Link Layer:** The data link layer is responsible for moving frames from one hop (node) to the next. It Breaks the outgoing data into frames and re-assemble the received frames. It Handle errors by implementing an acknowledgement and retransmission scheme. **Network Layer:** The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a important component used to route information where it needs to go between networks. **Transport Layer:** The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol. **Session Layer:** The session layer controls the conversations between different computers. A session or connection between devices is set up, managed, and terminated at layer 5. Session layer services also include authentication and reconnections. **Presentation Layer:** The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer. **Application Layer:** The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).	**Explai n-ation**
	c)	**Draw the labeled construction of Fibre optic cable. State four advantages compared to copper cables.**	**6M**
	Ans:	**Figure shows the labeled diagram for Fiber Optic Cable**	**2M for Diagra m**



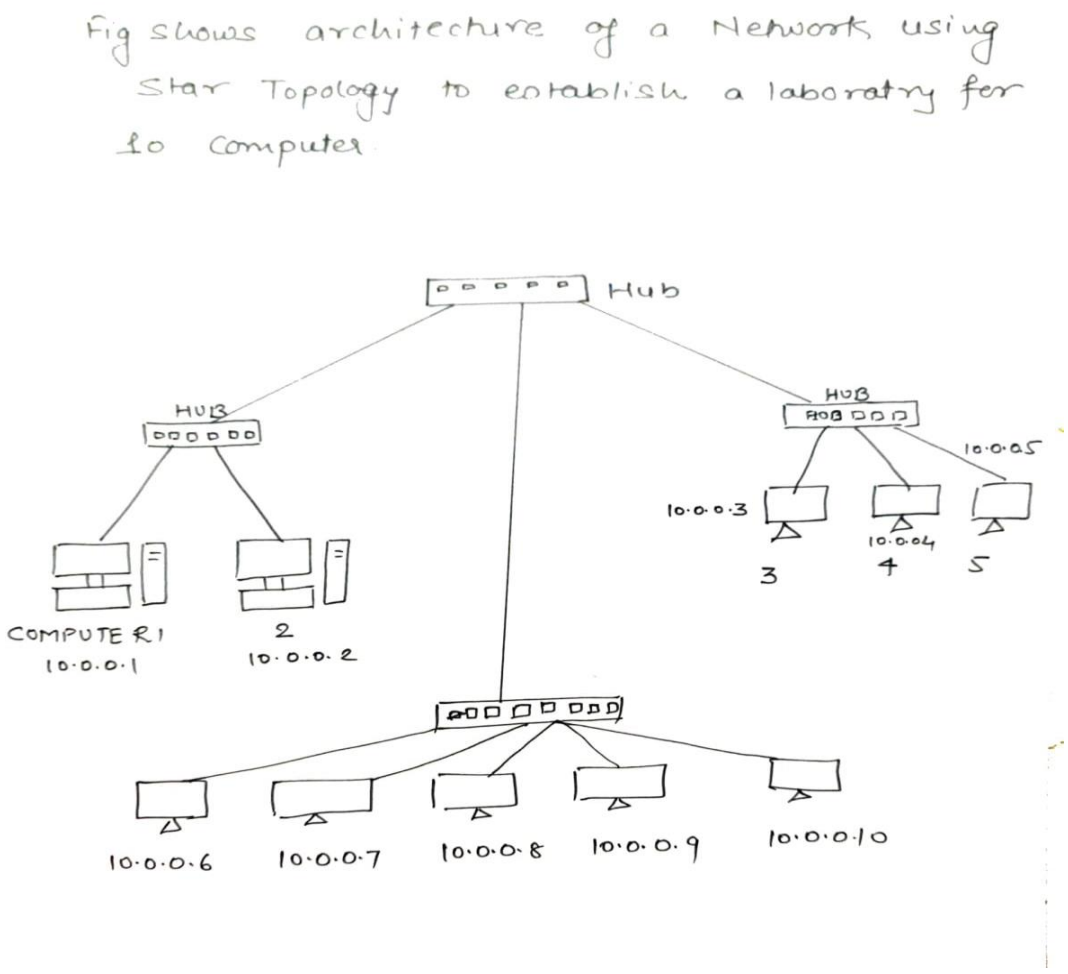
)

1M each for any 4 applications

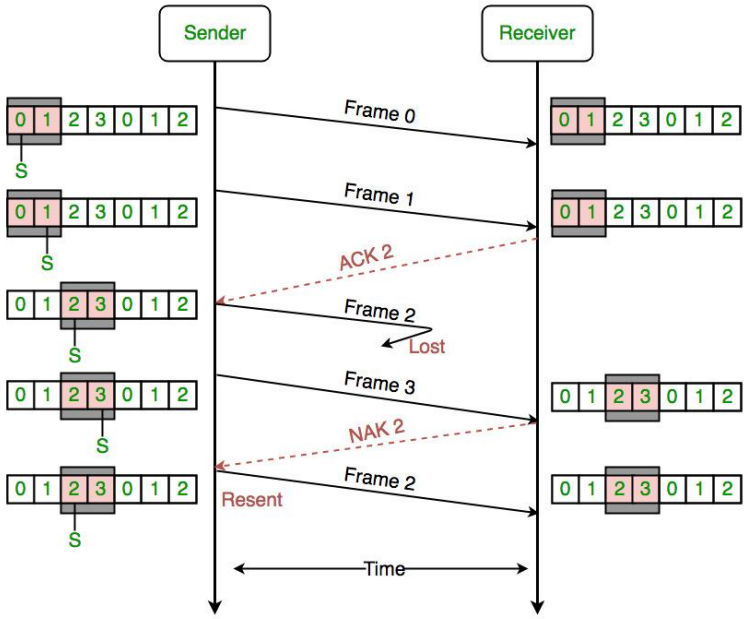
Advantages of fibre optic cable over copper cables

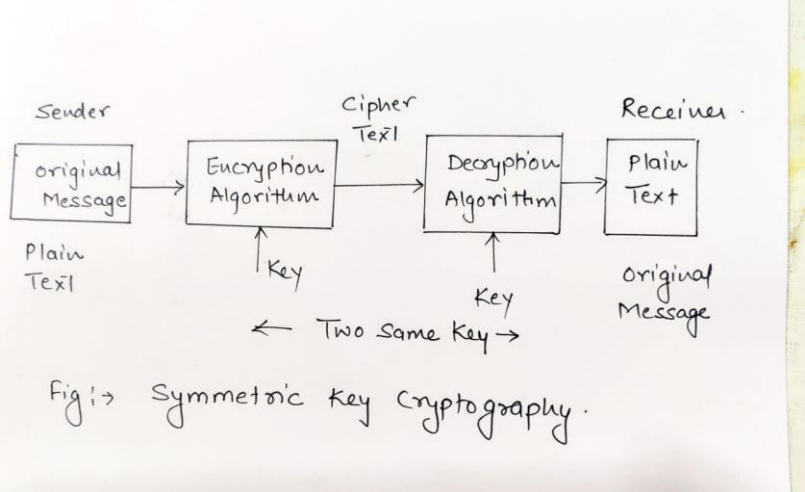
- These are not affected by electromagnetic interference, so noise and distortion is very less.
- Optical fiber cable are often made cheaper than equivalent lengths of copper wire.
- Used for both analog and digital signals
- Highly secured
- Provides high quality transmission of signals at very high speed (bandwidth 2 Gbps
- Smaller size and light weight
- Less power loss and allows data transmission for extended distances
- Bandwidth is high

Q. No.	Sub Q. N.	Answers	Marking Scheme
6.		**Attempt any TWO of the following :**	**12- Total Marks**
	a)	**Draw and describe architecture for a network using star topology to establish a**	**6M**

		laboratory with 10 computers	
	Ans:	The architecture for a network using star topology is as shown in the figure  • A star topology is a topology where every node in the network is connected to one central switch. Every device in the network is directly connected to the switch and indirectly connected to every other node. • The relationship between these elements is that the central network hub is a server and other devices are treated as clients. • The central node has the responsibility of managing data transmissions across the whole network and acts as a repeater. • With star topologies, computers are connected with a coaxial cable, twisted pair, or	**3M for Diagram** **3 M for description**

		optical fiber cable. • In terms of physical network structure, star topologies require fewer cables than other topology types. This makes them simple to set up and manage over the long-term. • The simplicity of the overall network design makes it much easier for administrators to run troubleshooting when dealing with network performance faults.	
	b)	**With suitable diagram explain selective repeat ARQ protocol**	**6M**
	Ans:	Selective Repeat ARQ •In this method the size of sender and receiver window is same •In selective repeat ARQ only damaged frames are resent •This method uses negative acknowledgement to report sequence number of damaged frame before timer expires •Selective repeat uses both positive and negative acknowledgement **Normal Operation** : Frames 0 and 1 are accepted when received because they are in the receiver window range.The sender's window shifts toward right and transmits frames 2 and 3 .The receiver accepts frame 3 as it is in receiver's window . The receiver sends NAK2 to show that frame 2 is lost .The sender then sends only frame 2 **Lost and delayed acknowledgement and NAK (Negative Acknowledgement)** If the window capacity is reached and acknowledgements are not received because of delay or loss within the time period the sender retransmits every frame in the window Similarly if NAK are lost or delayed the sender retransmits all the frames after last acknowledged frame	**3M for Diagram**

			**3M on explain ation**
	c)	**Draw the block diagram of Symmetric Key Cryptography and state the function of various components. Compare symmetric and Asymmetric Key Cryptography**	**6M**
	Ans:	**Figure illustrating the block diagram of Symmetric Key Cryptography** Symmetric key encryption also termed as shared -key ,single-key, secret-key in this type both the sender and receiver share same key which is used to both encrypt and decrypt messages There are five main components of a symmetric cryptography system: plaintext, encryption algorithm, secret key, ciphertext, and the decryption algorithm.	**2M for diagra mm** **2M for Explai nation** **2 M for any 2 valid points of**

		 Fig:- Symmetric Key Cryptography. **1. Plaintext** The term **plaintext** refers to the original message to be sent for encryption . Here the original message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The security depends on several factor. **2. Encryption Algorithm** The **encryption algorithm** takes the plaintext and converts it into an unreadable format. The encryption process s consists of an algorithm and a key. The key is a value independent of the plaintext. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be. **3. Key** Think of the key as a decoder ring: the secret of the scrambled text cannot be read without the key. The **key** holds the information on all the switches and substitutions made to the original plain text. In symmetric encryption, the key is actually bundled with the algorithm; in this sense, the decoder ring is not universal. The changes and substitutions depend on the key, and vice versa because the sender and recipient share the key. **4. Ciphertext** The **ciphertext** is the text that is now scrambled and ready to be sent. It may look like a random stream of data, and is unreadable. **5. Decryption Algorithm** In the **decryption algorithm**, the secret key is applied to the ciphertext. It converts it back to plaintext, basically performing the encryption in reverse. .. Upon reception, the cipher text can	**compa rison**

be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

Comparison of Symmetric and Asymmetric Key Cryptography is given as

Symmetric Key Encryption	Asymmetric Key Encryption
It is a simple form of encryption.	It is complicated from of encryption.
A single key is required for encryption and decryption.	Two separate keys are used to encrypt and decrypt.
Cypher text will carry smaller or the same size as of original text.	The size of cypher text can be large or the same.
Quicker process.	Slower process.
Preferred for large quantity encryption.	Preferred for small quantity encryption.
Confidentiality is the only benefit of this method.	Other than confidentiality, it provides authenticity and non-repudiation.
Resources are moderately utilised.	Resources and highly utilised.
Example: RC4, DES, 3DES, etc.	Example: Diffie-zhellman, El Gamal, ECC, RS, etc.