# Computer Networks – Important 10Mark Questions

1. Explain the following: (a) Wireless LAN (b) Sensor networks

**a) Wireless Local Area Network (WLAN):**

A Wireless Local Area Network (WLAN) is a type of computer network that uses wireless data connections between network nodes. In other words, it is a wireless network that provides connectivity between devices such as computers, laptops, smartphones, and other mobile devices without the use of cables or wires.

WLANs are typically used to connect devices to the internet, to share files and resources such as printers and storage devices, and to enable communication between devices. They are widely used in homes, offices, airports, cafes, and other public spaces.

**Benefits of WLAN:**

1. **Internet connectivity while on the move:** The major benefit of a WLAN is that it allows people to be connected even if they are moving. The ability to use the internet for work and play while on the move has changed a lot of things for the better.
2. **Cost effective:** Another advantage of using WLAN is that it is cost effective. Installing cables quickly becomes extremely expensive when you have to cater to a large number of users and factor in the maintenance cost.
3. **Less hassle for IT and maintenance staff:** WLANs also make it easier for IT maintenance and support staff who don't have to individually check for broken connections all the time. Not to mention that WLANs are easier to install and require less dealing with cables and wires during installation.
4. **Flexibility for organizations:** WLANs also help organizations adjust their number of users or devices that need to be connected to the internet.
5. **Useful in disasters and when physical infrastructure is damaged:** WLANs can also prove incredibly useful when there is a natural disaster as it reduces the need for physical infrastructure to provide internet connectivity, granted that the range will be limited.

**Components of WLAN:**

1. **Access Point (AP):** An access point is a wireless networking hardware device that allows wireless devices to connect to a wired network. It acts as a central hub for wireless communication and enables devices to connect to the network and communicate with each other.
2. **Wireless Network Interface Card (NIC):** A wireless NIC is a hardware device that enables wireless communication between a device and the network. It is typically built into devices like laptops, tablets, and smartphones, and allows these devices to connect to a wireless network.
3. **Antennas:** Antennas are used to transmit and receive wireless signals between devices and the access point. They come in various shapes and sizes, and their design is critical to the performance of a wireless network.
4. **Wireless LAN Controller (WLC):** A WLC is a device that manages multiple access points and controls the configuration of the wireless network. It helps in load balancing, security, and mobility management of wireless devices.
5. **Network cables:** Although wireless LANs are wireless, they still require some wired components, such as network cables to connect the access points to the wired network.
6. **Network Security:** Wireless LANs are vulnerable to security threats, so it's important to implement security measures such as WPA2 (Wi-Fi Protected Access II) encryption, firewalls, and intrusion detection systems to protect the network and the devices connected to it.

**Applications of Wireless LAN:**

1. **Home Networking:** Wireless LAN technology is widely used in homes for networking various devices such as laptops, smartphones, tablets, smart TVs, gaming consoles, etc. It allows for seamless connectivity and sharing of data among different devices.
2. **Business Networking:** Wireless LAN is extensively used in businesses, especially in offices, factories, and warehouses. It allows for easy sharing of data among employees and also facilitates communication through VoIP and video conferencing.

3. **Public Wi-Fi:** Wireless LAN technology is used to provide free or paid internet connectivity in public places such as airports, cafes, restaurants, malls, and hotels. It allows people to access the internet on their mobile devices without the need for cables or wires.
4. **Healthcare:** In the healthcare industry, wireless LAN is used for connecting medical devices such as heart monitors, blood pressure monitors, and infusion pumps. It allows for easy monitoring of patient health, reducing the need for physical monitoring.
5. **Education**: Wireless LAN is used in educational institutions to provide internet access to students and staff. It also facilitates e-learning and online collaboration.
6. **Industrial Automation:** Wireless LAN technology is used in industrial automation to monitor and control various processes. It allows for real-time monitoring of production lines, reducing downtime, and improving productivity.
7. **Retail:** In the retail industry, wireless LAN technology is used to manage inventory, track sales, and improve customer experience. It allows for seamless communication among employees, facilitating faster customer service.

**b) Sensor networks:**

Sensor networks are networks of interconnected sensors that can communicate with each other and with a central data processing system. These networks are used to collect data from physical environments and transmit it to a centralized location for analysis.

It is a type of network that consists of a large number of small, autonomous devices called sensors, which are capable of sensing and collecting data from the environment. These sensors are typically equipped with various types of sensors, such as temperature, humidity, light, pressure, motion, and sound sensors, and they can communicate with each other to form a network that can transmit data to a central location for analysis.

**Characteristics of Sensor Networks:**

1. **Scalability:** It can be easily scaled up or down depending on the size and complexity of the application. New sensors can be added or removed without affecting the performance of the network.
2. **Self-Organization:** These are self-organizing, meaning that they can configure themselves automatically without the need for human intervention. The sensors can form a mesh network, in which each node can communicate with its neighbours to establish routes for data transmission.
3. **Energy Efficiency:** Sensors are typically battery-powered, so energy efficiency is critical to ensure the longevity of the network. Techniques such as duty cycling, sleep modes, and adaptive routing can be used to conserve energy and prolong the battery life of the sensors.
4. **Data Processing:** It generate a massive amount of data, which can be overwhelming to process and analyse. Data aggregation, compression, and filtering techniques can be used to reduce the amount of data and improve the efficiency of data processing.
5. **Security:** These are vulnerable to security threats, such as unauthorized access, data tampering, and denial of service attacks. Encryption, authentication, and access control mechanisms can be used to protect the network and the data transmitted over it.

**Components of Sensor Networks:**

1. **Sensors:** These are the main components of a sensor network, and they are responsible for sensing and collecting data from the environment. They are usually small, low-power devices that can be placed in various locations to capture data from different sources.
2. **Processing units:** These are the components that are responsible for processing the data collected by the sensors. They can be located either on the sensors themselves or on a separate device that is connected to the sensor network.
3. **Communication modules:** These are the components that enable the sensors to communicate with each other and with other devices in the network. They can be wired or wireless, and they are responsible for transmitting the data collected by the sensors to a central location for analysis.
4. **Power source:** Since the sensors in a sensor network are usually small and low-power devices, they typically rely on batteries for power. However, some sensor networks may also include energy-harvesting components, such as solar panels or kinetic energy harvesters, that can generate power from the environment.

Applications of sensor networks are diverse and include environmental monitoring, precision agriculture, structural health monitoring, smart cities, and industrial automation. Sensor networks have the potential to revolutionize many fields by providing real-time data and insights that were previously impossible to obtain.

They enable real-time data collection and analysis, which can help improve efficiency, reduce costs, and enhance decision-making. However, sensor networks also present challenges, such as power management, network scalability, and data security.

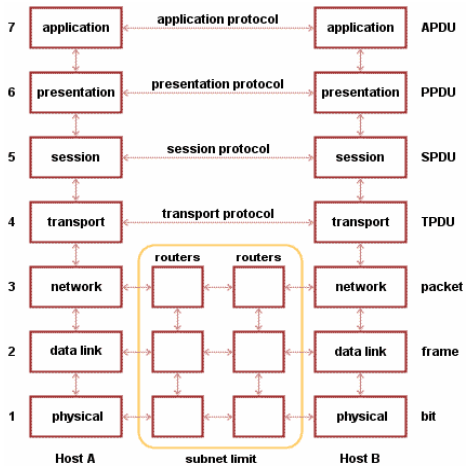
2. Describe the OSI reference model with neat sketch.

**Open Systems Interconnection (OSI) Reference Model:**

The Open Systems Interconnection (OSI) model defines a networking framework to implement protocols in layers, with control passed from one layer to the next. It is primarily used today as a teaching tool. It conceptually divides computer network architecture into **7 layers** in a logical progression.

The lower layers deal with electrical signals, chunks of binary data, and routing of these data across networks. Higher levels cover network requests and responses, representation of data, and network protocols, as seen from a user's point of view.

The OSI model was originally conceived as a standard architecture for building network systems, and many popular network technologies today reflect the layered design of OSI.




**Seven layers of OSI Model:**

1. **Physical Layer:**

   At Layer 1, the Physical layer of the OSI model is responsible for the ultimate transmission of digital data bits from the Physical layer of the sending (source) device over network communications media to the Physical layer of the receiving (destination) device.

   At the Physical layer, data is transmitted using the type of signaling supported by the physical medium: electric voltages, radio frequencies, or pulses of infrared or ordinary light.

2. **Data Link Layer:**

   When obtaining data from the Physical layer, the Data Link layer checks for physical transmission errors and packages bits into data frames. The Data Link layer also manages physical addressing schemes such as MAC addresses for Ethernet networks, controlling access of network devices to the physical medium.

   Because the Data Link layer is the most complex layer in the OSI model, it is often divided into two parts: the Media Access Control sub-layer and the Logical Link Control sub-layer.

3. **Network Layer:**

   The Network layer adds the concept of routing above the Data Link layer. When data arrives at the Network layer, the source and destination addresses contained inside each frame are examined to determine if the data has reached its final destination. If the data has reached the final destination, layer 3

formats the data into packets delivered to the Transport layer. Otherwise, the Network layer updates the destination address and pushes the frame down to the lower layers.

To support routing, the Network layer maintains logical addresses such as IP addresses for devices on the network. The Network layer also manages the mapping between these logical addresses and physical addresses.

4. **Transport Layer:**

   The Transport Layer delivers data across network connections. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are the most common examples of Transport Layer 4 network protocols. Different transport protocols may support a range of optional capabilities, including error recovery, flow control, and support for re-transmission.

5. **Session Layer:**

   The Session Layer manages the sequence and flow of events that initiate and tear down network connections. At layer 5, it is built to support multiple types of connections that can be created dynamically and run over individual networks.

6. **Presentation Layer:**

   The Presentation layer has the simplest function of any piece of the OSI model. At layer 6, it handles syntax processing of message data such as format conversions and encryption/decryption needed to support the Application layer above it.

7. **Application Layer**

   The Application layer supplies network services to end-user applications. Network services are protocols that work with the user's data. For example, in a web browser application, the Application layer protocol HTTP packages the data needed to send and receive web page content. This layer 7 provides data to (and obtains data from) the Presentation layer.

3. Discuss on communication satellites.

**Communication Satellites:**

Communication satellites are artificial satellites placed in orbit around the Earth to facilitate communication between distant points on the surface of the planet. They are used to relay communication signals between two or more points on Earth. They are typically placed in geostationary orbit, which means that they orbit the Earth at the same rate that the Earth rotates, allowing them to maintain a fixed position relative to the Earth's surface.

**Types of Communication Satellites and its Uses:**

1. **Geostationary satellites:** These are a type of communication satellite that orbits the Earth at an altitude of approximately 36,000 kilometres above the equator. The defining characteristic of a geostationary satellite is that it appears to remain stationary relative to a point on the Earth's surface, due to its orbit matching the rotation of the Earth. This allows a geostationary satellite to provide continuous coverage of a specific region, making it ideal for applications that require constant communication links.

   Uses: Television broadcasting, satellite telephony, satellite internet, whether monitoring and military applications.

2. **Low Earth Orbit (LEO) satellites:** These are satellites that orbit the Earth at an altitude of less than 2,000 kilometres. They are closer to the Earth than geostationary satellites and require a network of satellites to provide continuous coverage.

   LEO satellites have become an important part of modern communication and remote sensing systems, and their use is expected to increase in the coming years.

   Uses: satellite phone and data services, remote sensing, scientific research, space exploration.

3. **Highly Elliptical Orbit (HEO) satellites:** These are satellites that have an elliptical orbit with a high point of apogee (farthest point from the Earth) and a low point of perigee (closest point to the Earth). HEO satellites have several unique features that make them suitable for certain applications.

HEO satellites are used for applications where continuous coverage of a specific region is required, or where a unique vantage point is needed for observation or communication.

Uses: communication, navigation, military surveillance, scientific research.

**Key Features of Communication Satellites:**

1. They orbit the Earth at a fixed altitude and are equipped with transponders that receive and transmit signals. These signals can include voice, data, video, and other forms of information.
2. They are used for a variety of purposes, including television broadcasting, telephone communications, internet connectivity, and military communications.
3. Communication satellites are equipped with transponders, which receive and amplify signals from Earth-based transmitters and then retransmit them back to Earth.
4. They operate in different frequency bands, including the C-band, Ku-band, and Ka-band. The frequency band used depends on the specific application and regulatory requirements.
5. Some communication satellites are equipped with multiple spot beams, which allow them to provide coverage to different regions on Earth.
6. Communication satellites face several challenges, including signal interference, space debris, and solar flares. To mitigate these challenges, they are equipped with technologies such as adaptive modulation and error correction codes

4. Describe the elementary data link protocols.

**Elementary Data Link Protocol (EDLP):**

It is a simple protocol that is used to transfer data between two nodes in a communication network. EDLP is a type of data link layer protocol that ensures the reliable transfer of data between two nodes by detecting and correcting errors that may occur during transmission.

EDLP is a simple and reliable protocol that can be used for a variety of applications, including point-to-point communication, local area networks (LANs), and wide area networks (WANs). Its simplicity and reliability make it a popular choice for many communication networks.

**Key features of EDLP:**

1. **Framing:** EDLP uses framing to break up the data into smaller frames that can be transmitted over the network. Each frame contains a header and a trailer, which includes control information such as sequence numbers and error detection codes.
2. **Flow Control:** EDLP includes mechanisms for flow control, which ensure that data is transmitted at a rate that can be handled by the receiver. Flow control mechanisms may include techniques such as buffering, windowing, or rate control.
3. **Error Control:** EDLP uses error detection and correction mechanisms to ensure the reliability of data transmission. These mechanisms may include techniques such as checksums, cyclic redundancy checks (CRC), or error-correcting codes.
4. **Acknowledgements:** EDLP includes mechanisms for acknowledging receipt of data frames. These acknowledgements help to ensure that data is transmitted reliably between nodes.
5. **Retransmission:** EDLP includes mechanisms for retransmitting lost or corrupted data frames. These mechanisms may include techniques such as automatic repeat request (ARQ), selective repeat or go-back-N.

**Types of Elementary Data Link Protocol:**

1. **Stop-and-wait protocol:** This is a simple protocol in which the sender sends a frame and waits for an acknowledgment from the receiver before sending the next frame. It is a reliable protocol that ensures that all frames are delivered correctly, but it is not very efficient because it involves a lot of waiting.
2. **Sliding window protocol:** This protocol allows the sender to transmit multiple frames before receiving an acknowledgment from the receiver. The sender maintains a window of frames that can be sent without waiting for an acknowledgment. The receiver acknowledges the frames it has received, and the sender adjusts the size of the window accordingly. This protocol is more efficient than the stop-and-wait protocol, but it is more complex to implement.

3. **Selective repeat protocol:** This protocol is similar to the sliding window protocol, but it allows the receiver to selectively request retransmission of only those frames that were not received correctly. This reduces the number of retransmissions and makes the protocol more efficient.
4. **Go-back-N protocol:** This protocol is similar to the sliding window protocol, but it requires the sender to retransmit all unacknowledged frames if it receives a negative acknowledgment (NACK) from the receiver. This makes the protocol less efficient than the selective repeat protocol.
5. **High-level data link control (HDLC):** HDLC is a protocol that provides both connection-oriented and connectionless services. It is a bit-oriented protocol that uses flags to delimit frames and provides error detection and correction using cyclic redundancy check (CRC). HDLC supports a variety of transmission modes, including asynchronous and synchronous transmission.
6. **Point-to-Point Protocol (PPP):** PPP is a data link protocol used to establish a direct connection between two network nodes. It is often used to connect a computer to the Internet using a modem. PPP provides authentication, encryption, and compression services, as well as error detection and correction.

6. Explain the design issues of transport layer.

The transport layer is the fourth layer in the OSI model and is responsible for providing reliable end-to-end data transfer between applications on different hosts. It achieves this by breaking data into packets, adding necessary headers and trailers, and managing the flow of data between hosts. However, there are several design issues that must be addressed in the transport layer to ensure optimal performance and reliability.
Here are some of the design issues in the transport layer:

1. **Connection-oriented vs. connectionless service:** One of the primary design decisions in the transport layer is whether to provide a connection-oriented or connectionless service. In a connection-oriented service, a virtual circuit is established between the sender and receiver before data transfer begins. This provides reliable, ordered data transfer but can result in higher latency and overhead. In a connectionless service, each packet is sent independently and can take different paths to the destination. This provides lower latency and overhead but can result in out-of-order delivery and packet loss.
2. **Error control:** The transport layer must provide error control mechanisms to detect and correct errors that occur during data transfer. This is typically achieved through the use of error detection codes, such as checksums or cyclic redundancy checks (CRC), and retransmission of lost or damaged packets.
3. **Flow control:** The transport layer must manage the flow of data between the sender and receiver to prevent congestion and ensure optimal performance. This is typically achieved through the use of sliding window protocols, which allow the sender to transmit a fixed number of packets before waiting for acknowledgments from the receiver.
4. **Congestion control:** The transport layer must also manage congestion in the network to prevent packet loss and ensure fair sharing of network resources. This is typically achieved through the use of congestion control mechanisms, such as slow start and congestion avoidance, which adjust the sending rate based on network conditions.
5. **Quality of service (QoS):** The transport layer must also support QoS requirements, such as guaranteed bandwidth, low latency, and high reliability, for different types of applications. This is typically achieved through the use of traffic shaping and prioritization mechanisms, which allocate network resources based on the application's QoS requirements.
6. **Reliability:** One of the main goals of the transport layer is to ensure reliable communication between two end devices. This involves detecting and correcting errors that may occur during transmission, as well as ensuring that all data is delivered in the correct order. To achieve this, various error detection and correction techniques are used, such as checksums, sequence numbers, and acknowledgments.
7. **Multiplexing and demultiplexing:** The transport layer must also be able to multiplex data from multiple applications onto a single network connection, as well as demultiplex data received on the network connection and deliver it to the correct application. This is typically achieved using port numbers, which allow the transport layer to identify the application associated with each packet.
8. **Addressing and routing:** The transport layer may also be responsible for addressing and routing packets within a network. For example, the User Datagram Protocol (UDP) uses port numbers to address packets to

specific applications, while the Transmission Control Protocol (TCP) uses a combination of IP addresses and port numbers to identify the destination host and application.

9. **Security**: The transport layer needs to support the use of encryption and authentication mechanisms to ensure the confidentiality and integrity of data transmitted between hosts.
10. **Session establishment and termination:** The transport layer needs to provide mechanisms for establishing and terminating communication sessions between hosts.
11. **Protocol design:** The transport layer protocol needs to be designed to be efficient, scalable, and extensible to support future requirements and advancements in network technology.

6. Explain the methods for error detection and correction.

**Error Detection:**

Error detection is a process that allows detecting and correcting errors that occur during the transmission of digital data. There are several methods for error detection that can be used in various applications.

Here are some of the commonly used methods for error detection:

1. **Parity check:** In this method, a single bit is added to the data to make the total number of bits either even or odd. The receiver then checks the parity bit and determines whether the number of 1's in the data is even or odd. If the number of 1's is not the same as the parity bit, an error is detected.
2. **Checksum:** In this method, a sum of all the data bytes is calculated and transmitted along with the data. The receiver then calculates the checksum and compares it with the transmitted value. If the calculated value is different from the transmitted value, an error is detected.
3. **Cyclic redundancy check (CRC):** In this method, a polynomial code is generated and appended to the data. The receiver then calculates the polynomial code and checks if it matches the received value. If the calculated value is different from the received value, an error is detected.
4. **Hamming code:** In this method, additional bits are added to the data to allow detecting and correcting single-bit errors. The number of additional bits depends on the number of data bits and the desired level of error correction. Hamming codes are commonly used in computer memory systems to correct errors that occur during data storage and retrieval.
5. **Forward error correction (FEC):** In this method, additional redundant bits are added to the data to allow the receiver to correct errors that occur during transmission. FEC codes are commonly used in wireless communication systems to provide reliable communication over noisy channels.
6. **Reed-Solomon code:** In this method, a polynomial code is generated and added to the data. The receiver then uses the polynomial code to correct errors that occur during transmission. Reed-Solomon codes are commonly used in digital communication systems, such as satellite communication and digital television broadcasting.

The choice of error detection method depends on the specific requirements of the communication system, including the desired level of error detection and correction, the complexity of the algorithm, and the processing power available at the sender and receiver ends.

**Error Correction:**

Error correction is the process of identifying and correcting errors that may occur during data transmission, storage, or processing. Here are some common methods for error correction:

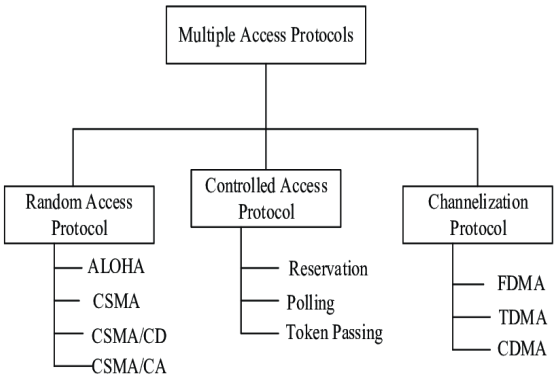
1. **Automatic Repeat Request (ARQ):** ARQ is a simple error correction technique that involves retransmitting the data that was received with errors. The receiver detects errors by using error detection techniques like checksum, CRC, or parity check. If an error is detected, the receiver sends a request to the sender to retransmit the data.
2. **Forward Error Correction (FEC):** FEC is a more sophisticated error correction technique that involves adding redundant bits to the transmitted data to enable the receiver to correct errors without requesting retransmission of data. Reed-Solomon codes and Convolutional codes are commonly used in FEC.
3. **Hamming Code:** Hamming codes are a type of error-correcting code that can detect and correct single-bit errors in data. They work by adding redundant bits to the transmitted data to allow the receiver to detect and correct errors.
4. **Reed-Solomon Code:** Reed-Solomon codes are another type of error-correcting code that can detect and correct multiple errors in data. They are commonly used in digital communication systems, such as satellite and mobile communication systems.

5. **Turbo Code:** Turbo codes are a type of error-correcting code that use multiple decoding iterations to improve error correction performance. They are commonly used in modern communication systems, such as 3G and 4G cellular networks.
6. **Convolutional Code:** Convolutional codes are a class of error-correcting codes that use the concept of state machines. These codes are more complex than Hamming and Reed-Solomon codes but can provide better error correction performance.

The choice of error correction method depends on the specific requirements of the communication system, including the desired level of error correction, the complexity of the algorithm, and the processing power available at the sender and receiver ends. A combination of error detection and error correction techniques can be used to provide a high level of data reliability in communication systems

7. Discuss on Multiple access protocols.

**Multiple access protocols:**




**RANDOM ACCESS:**

Random access protocols are used to allow multiple users to share a common communication channel without any coordination or scheduling. In random access protocols, each user transmits data whenever they have data to send, without any prior reservation or permission from the system.

**Types of Random Access Protocol:**

1. **ALOHA:** ALOHA is the simplest form of random access protocol, in which users transmit data whenever they have data to send. If two or more users transmit data at the same time, their signals collide and the data is lost. The sender then waits for a random amount of time before retransmitting the data. ALOHA is not very efficient, as a large number of collisions can occur, resulting in significant delays and loss of data.
2. **Slotted ALOHA:** Slotted ALOHA is an improvement over the basic ALOHA protocol. In Slotted ALOHA, the time is divided into discrete slots, and users are only allowed to transmit at the beginning of each slot. This reduces the chances of collision, as multiple users are less likely to transmit data at the exact same time. However, Slotted ALOHA still suffers from inefficiency, as some slots may be empty while others may have multiple users attempting to transmit at the same time.
3. **Carrier Sense Multiple Access (CSMA):** CSMA is a protocol in which each user listens to the channel to detect if it is idle before attempting to transmit data. If the channel is busy, the user waits for a random amount of time before attempting to transmit again. CSMA reduces collisions and improves efficiency, but it does not prevent collisions entirely, as multiple users may detect an idle channel at the same time and attempt to transmit simultaneously.
4. **Carrier Sense Multiple Access with Collision Detection (CSMA**/CD): CSMA/CD is a protocol that is used in Ethernet LANs. It is similar to CSMA, but includes a collision detection mechanism. If a collision is detected, the users stop transmitting and wait for a random amount of time before attempting to transmit again. CSMA/CD reduces the probability of collisions and improves efficiency, but it requires more complex hardware than basic CSMA.
5. **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA):** CSMA/CA is a protocol used in wireless LANs. It is similar to CSMA, but includes a collision avoidance mechanism. In CSMA/CA, each user requests permission to transmit from the access point (AP) before attempting to transmit. The AP grants permission to one user at a time, based on priority and availability. CSMA/CA improves efficiency and reduces collisions, but it can be affected by interference and signal propagation issues.

**Controlled Access Protocol:**

Controlled access protocols are used to allow multiple users to share a common communication channel, but with some form of coordination or scheduling to avoid collisions and ensure efficient use of the channel. In controlled access protocols, each user is assigned a time slot or a priority level to transmit their data, which is determined by the system based on various criteria such as urgency, importance, or fairness.

**Types of Controlled Access Protocol:**

1. **Reservation-based protocols:** Reservation-based protocols require users to reserve a time slot before transmitting data. This ensures that each user has a dedicated time slot for transmission, and eliminates the possibility of collisions. However, reservation-based protocols may be inefficient if some users reserve time slots but do not use them, leading to wasted bandwidth.
2. **Polling-based protocols:** Polling-based protocols require a central coordinator to poll each user in turn and request data transmission. This ensures that each user has an equal opportunity to transmit data and avoids collisions. However, polling-based protocols may be inefficient if some users have a lot of data to transmit, leading to delays for other users.
3. **Token-based protocols:** Token-based protocols use a token that is passed between users to allow them to transmit data. Only the user with the token is allowed to transmit data, while other users wait for their turn. This ensures fair access to the channel and avoids collisions, but may be inefficient if some users hold onto the token for a long time, leading to delays for other users.
4. **Demand-based protocols:** Demand-based protocols require users to send a request to transmit data before actually transmitting. The system then grants permission to transmit based on various criteria such as priority and availability. This ensures efficient use of the channel and avoids collisions, but may be inefficient if some users have a lot of data to transmit or if there are many requests for transmission.

**Channelization protocols:**

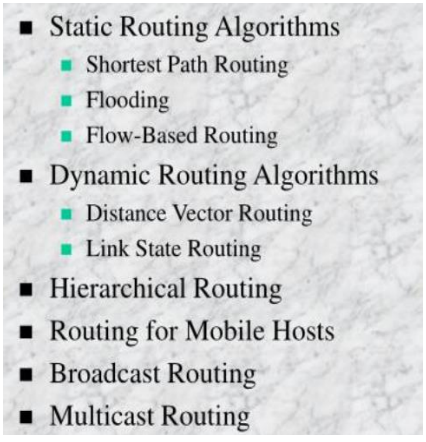
Channelization protocols are used to divide a communication channel into multiple sub-channels, allowing multiple users to share the channel without interfering with each other. Channelization protocols can be either time-division or frequency-division based.

**Types of Channelization protocols:**

1. **Time-division multiple access (TDMA):** TDMA is a channelization protocol in which the channel is divided into time slots, and each user is assigned a unique time slot to transmit data. Only one user is allowed to transmit data in a given time slot, and the time slots are assigned in a round-robin fashion.
2. **Frequency-division multiple access (FDMA):** FDMA is a channelization protocol in which the channel is divided into multiple frequency bands, and each user is assigned a unique frequency band to transmit data. Users transmit at different frequencies, and the frequencies are assigned in a round-robin fashion.
3. **Code-division multiple access (CDMA):** CDMA is a channelization protocol in which multiple users transmit data simultaneously on the same frequency band, using unique codes to differentiate between the transmissions. Each user is assigned a unique code, and the receiver uses the code to decode the transmitted data.

8. Describe any two routing algorithms in Network layer.

**Types of Routing Algorithm:**




**Hierarchical Routing:**

Hierarchical routing is a routing algorithm used in communication networks that organizes the network into a hierarchical structure. The goal of hierarchical routing is to reduce the number of routing table entries and the overhead associated with routing information exchange.

In hierarchical routing, the network is divided into multiple levels or domains, with each level containing a set of routers. The highest level is called the backbone or core level, which contains the largest and most powerful routers. Lower levels are called access levels and contain smaller and less powerful routers. Each level is responsible for routing traffic within its own domain, and traffic between domains is forwarded through the backbone level.

Hierarchical routing algorithm reduces the amount of routing information that needs to be stored and exchanged, thus reducing the overhead and complexity of routing. It also provides scalability and robustness to the network, as the hierarchical structure allows the network to handle a large number of nodes and tolerate failures in individual nodes or links.

The routing information is divided into two types: inter-domain routing information and intra-domain routing information. Inter-domain routing information is exchanged only between routers at the boundary of different domains, while intra-domain routing information is exchanged only within a domain.

The routing protocol used in hierarchical routing is typically a distance-vector protocol, such as the Routing Information Protocol (RIP) or the Open Shortest Path First (OSPF) protocol. The protocol is used to exchange routing information between routers within a domain and between routers at the boundary of different domains.

The advantages of hierarchical routing are that it reduces the size of routing tables and minimizes the overhead associated with routing information exchange. It also improves network scalability, as the network can be easily expanded by adding more domains or levels.

The disadvantages of hierarchical routing are that it can increase the complexity of the network, as multiple levels or domains need to be managed. It can also lead to longer path lengths, as traffic needs to be routed through the backbone level to reach other domains. In addition, hierarchical routing may not be suitable for networks with dynamic topology changes, as it may require frequent reconfiguration of the network structure.

Hierarchical routing is a widely used and effective routing algorithm in communication networks that allows for efficient routing information exchange and improves network scalability.

**MultiCast Routing:**

Multicast routing algorithms are used in communication systems to efficiently deliver data from a single source to multiple destinations. There are several multicast routing algorithms, each with its own advantages and disadvantages. Multicast routing algorithms are used in network layer of communication systems to efficiently deliver data to multiple receivers.

In general, multicast routing algorithms can be divided into two categories: source-based and shared tree.

1. **Source-based multicast:** In source-based multicast, the source node sends data to a multicast group address, and the data is forwarded to all members of the group. The routers along the path maintain information about the source and its members and use this information to forward the data to the appropriate destinations. The most commonly used source-based multicast routing algorithm is Protocol Independent Multicast Sparse Mode (PIM-SM). PIM-SM is a distributed protocol that uses an efficient sparse mode to deliver data from the source to the receivers.
2. **Shared tree multicast**: In shared tree multicast, a shared distribution tree is constructed that connects the source node to all members of the multicast group. Data is forwarded along the tree, and routers along the path maintain information about the tree and its members. The most commonly used shared tree multicast routing algorithm is Protocol Independent Multicast Dense Mode (PIM-DM). PIM-DM builds a dense distribution tree that includes all routers in the network, and data is flooded along the tree until it reaches all members of the multicast group.

There are several multicast routing algorithms, including:

1. **Distance Vector Multicast Routing Protocol (DVMRP):** DVMRP is a multicast routing protocol that uses the same distance-vector algorithm as used in the Routing Information Protocol (RIP) for unicast routing. It maintains a multicast distribution tree by flooding the multicast packets to all neighbors and pruning unwanted branches.
2. **Protocol Independent Multicast (PIM):** PIM is a family of multicast routing protocols that supports both dense and sparse modes of multicast delivery. In dense mode, the multicast packets are flooded throughout the network until they reach all receivers, while in sparse mode, the multicast packets are sent only to specific branches of the network tree.

3. **Multicast Open Shortest Path First (MOSPF):** MOSPF is a multicast routing protocol that extends the Open Shortest Path First (OSPF) unicast routing protocol to support multicast delivery. It builds a multicast distribution tree by calculating the shortest path from the source to the receivers and using it as the forwarding path.
4. **Bidirectional Multicast Routing Protocol (BDRP):** BDRP is a multicast routing protocol that supports bidirectional multicast communication. It builds a shared tree between the source and receivers, and a reverse path tree from the receivers to the source. It uses the shared tree for the majority of the traffic and the reverse path tree for reverse traffic.
5. **Distance Multicast Routing Protocol (DMRP):** DMRP is a multicast routing protocol that uses the same distance-vector algorithm as used in RIP for unicast routing. It builds a multicast distribution tree by flooding multicast packets and pruning unwanted branches.

9. Explain transport layer connection establishment and termination.

**Transport layer connection establishment:**

The transport layer in the OSI model provides end-to-end communication between processes running on different hosts. Connection establishment is a key function of the transport layer, allowing processes to establish a reliable communication channel before transmitting data.

Transport layer connection establishment is a process by which two end systems establish a connection before they can exchange data. This process is essential in providing reliable communication between the end systems.

The most common protocol used for transport layer connection establishment is the Transmission Control Protocol (TCP). TCP is a connection-oriented protocol that uses a three-way handshake to establish a connection between two end systems.

The three-way handshake consists of the following steps:

1. **SYN:** The initiating system sends a SYN (synchronize) packet to the receiving system, indicating that it wants to establish a connection. The SYN packet contains a randomly generated sequence number.
2. **SYN-ACK:** Upon receiving the SYN packet, the receiving system sends a SYN-ACK (synchronize-acknowledge) packet back to the initiating system. The SYN-ACK packet contains an acknowledgment number, which is the sequence number of the received SYN packet plus one, and a randomly generated sequence number.
3. **ACK:** Finally, the initiating system sends an ACK (acknowledge) packet back to the receiving system, acknowledging the receipt of the SYN-ACK packet. The ACK packet contains an acknowledgment number, which is the sequence number of the received SYN-ACK packet plus one.

At this point, the connection is established, and both systems can start exchanging data. If any of the packets are lost or not received, the process is repeated until the connection is established.

The connection establishment process is crucial in ensuring that both end systems are ready to receive and transmit data. It also helps in verifying the identity of the remote system, ensuring that the communication is secure.

**Transport layer connection Termination:**

In the transport layer, the most common protocol that provides connection-oriented service is the Transmission Control Protocol (TCP).

The connection termination process in TCP involves the following steps:

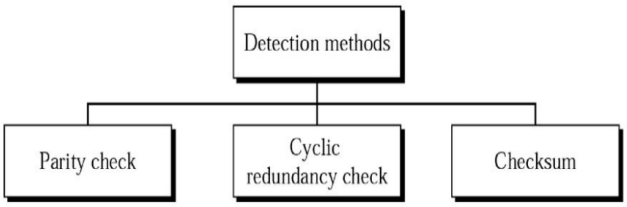
1. **FIN:** When a process decides to close the connection, it sends a FIN (finish) segment to the other end to indicate that it has no more data to send. The FIN segment includes a sequence number that indicates the last byte of data that the sender has sent.
2. **ACK:** Upon receiving the FIN segment, the other end sends an ACK (acknowledgment) segment to acknowledge receipt of the FIN segment. The ACK segment includes an acknowledgment number that is one more than the last sequence number received.
3. **FIN:** The other end may also decide to close the connection and send a FIN segment to the original sender. The same FIN-ACK process is then repeated in the opposite direction.
4. **TIME-WAIT:** After both ends have sent a FIN segment and received an ACK segment, they enter the TIME-WAIT state for a period of time to ensure that all packets have been transmitted and received. During this period, the end points wait for any retransmitted packets or delayed packets to arrive.
5. **CLOSED:** Once the TIME-WAIT period has expired, the connection is fully terminated, and both ends move to the CLOSED state.

10. Explain Error detecting codes with examples.

**Error Detecting codes:**

Error detecting codes are used in digital communication to detect transmission errors in the received data. These codes add redundancy to the data by adding extra bits, called parity bits or check bits, to the original data bits. When the receiver receives the data, it performs a check on the data bits and parity bits to see if there are any errors.

**Error Detection Methods:**




**Parity Check Code**:

Parity Check Code is a simple error detecting code that is widely used in digital communication. The code adds a single parity bit to the data to make the total number of 1's in the data plus parity bits either even or odd. If the receiver detects an odd number of errors in the received data, it knows that an error has occurred.

There are two types of parity check codes: even parity and odd parity. In even parity, the parity bit is set to 0 or 1 to make the total number of 1's even. In odd parity, the parity bit is set to 0 or 1 to make the total number of 1's odd. For example, suppose we want to send the binary data 1101. In even parity, we add a parity bit to make the total number of 1's even, resulting in 01101. In odd parity, we add a parity bit to make the total number of 1's odd, resulting in 11101.

To check for errors, the receiver performs the same parity check as the sender. If the total number of 1's in the received data plus parity bit is even (in even parity) or odd (in odd parity), the receiver assumes that no errors have occurred. If the total number of 1's is odd (in even parity) or even (in odd parity), the receiver assumes that an error has occurred.

**Cyclic Redundancy Check (CRC):**

Cyclic Redundancy Check (CRC) is a type of error detecting code that is commonly used in digital communication networks and storage devices to detect accidental changes or errors in transmitted or stored data.

The CRC code is generated using a polynomial division of the data, where the data is considered as a polynomial and the polynomial division is performed using a pre-defined divisor polynomial. The remainder obtained after the polynomial division is appended to the original data to create the CRC code.

At the receiving end, the same polynomial division is performed using the received data and the same divisor polynomial. If the remainder is zero, it is assumed that no errors occurred during transmission. If the remainder is non-zero, an error is assumed to have occurred.

CRC is widely used in various communication protocols such as Ethernet, Wi-Fi, Bluetooth, and in storage devices such as hard disk drives, USB drives, and memory cards. There are several types of CRC codes, with different polynomial divisors and bit lengths, depending on the application requirements.

**Checksum:**

Checksum is a simple error detecting code that is used to detect errors in data transmission. It involves adding up the values of all the bytes in the data packet, taking the complement of the sum, and appending it to the packet as a checksum.

Here is an example of how checksum works:

Suppose we want to transmit the data packet "01100001 01100010 01100011" (which represents the ASCII characters "abc"). We can calculate the checksum as follows:

1. Add up the values of all the bytes in the data packet (in binary):
   01100001 + 01100010 + 01100011 = 100100110
2. Take the complement of the sum (invert all the bits):
   011011001
3. Append the complement to the data packet as a checksum:
   01100001 01100010 01100011 011011001

Now, when the receiver receives the data packet, it can calculate the checksum using the same method and compare it to the checksum that was transmitted. If the checksums match, it is assumed that the data was transmitted correctly. If they do not match, an error is assumed to have occurred during transmission.

12. Explain channel allocation problem in medium access control sublayer.

**Medium Access Control(MAC) sublayer:**

The Medium Access Control (MAC) sublayer is a layer in the Data Link Layer of the OSI model that is responsible for controlling access to the physical transmission medium in a network. It is primarily concerned with the allocation and sharing of the available bandwidth among multiple users or devices that are connected to the same network segment.

The MAC sublayer provides a set of rules and protocols that govern how data frames are transmitted onto the physical medium and how collisions are resolved when multiple devices try to transmit data simultaneously.

**Channel Allocation Techniques in MAC Sublayer:**

There are various techniques for channel allocation in the MAC sublayer, including:

1. **Static/Fixed channel allocation:** In this technique, each node is allocated a fixed communication channel that it can use exclusively. This is suitable for applications where the number of nodes is small and fixed, and the traffic is predictable. However, this approach can lead to inefficient use of the communication channel when some nodes have no traffic to transmit.
2. **Dynamic channel allocation:** In this technique, the communication channel is dynamically allocated among the nodes based on their traffic demands. This can be further classified into:
    a. **Demand-assigned multiple access (DAMA):** In this technique, nodes request access to the communication channel when they have data to transmit, and the channel is allocated to them based on their requests. This approach is suitable for applications with variable traffic demands, but it can lead to collisions and high delay if many nodes request access simultaneously.
    b. **Reservation-based multiple access (RBMA):** In this technique, nodes reserve a portion of the communication channel in advance for their data transmission, and the channel is allocated to them at the reserved time. This approach reduces the chances of collisions and improves the efficiency of the communication channel, but it requires a centralized reservation mechanism and suffers from low utilization if nodes reserve more bandwidth than they actually need.
3. **Contention-based channel allocation:** In this technique, nodes compete for access to the communication channel by randomly accessing the channel and detecting collisions. This can be further classified into:
    a. **Carrier Sense Multiple Access (CSMA):** In this technique, nodes listen to the communication channel before transmitting data to ensure that no other nodes are transmitting at the same time. This reduces the chances of collisions, but it can lead to inefficient use of the communication channel if nodes wait too long before transmitting.
    b. **Carrier Sense Multiple Access with Collision Detection (CSMA/CD):** In this technique, nodes listen to the communication channel while transmitting data and stop transmission if they detect a collision. This approach reduces the chances of collisions and improves the efficiency of the communication channel, but it requires nodes to have the ability to detect collisions.

13. What are the two types of cryptographic principles? Explain.

**Redundancy**

The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message.

Cryptographic principle 1: Messages must contain some redundancy. In other words, upon decrypting a message, the recipient must be able to tell whether it is valid by simply inspecting the message and perhaps performing a simple computation. This redundancy is needed to prevent active intruders from sending garbage and tricking the receiver into decrypting the garbage and acting on the ‘‘plaintext.’’ However, this same edundancy makes it much easier for passive intruders to break the system, so there is some tension here.

Furthermore, the redundancy should never be in the form of n 0s at the start or end of a message, since running such messages through some cryptographic algorithms gives more predictable results, making the cryptanalysts’ job easier. A CRC polynomial is much better than a run of 0s since the receiver can easily verify it, but it generates more work for the cryptanalyst. Even better is to use a cryptographic hash, a concept we will explore later. For the moment, think of it as a better CRC. Getting back to quantum cryptography for a moment, we can also see how redundancy plays a role there. Due to Trudy’s interception of the photons, some bits in

Bob's one-time pad will be wrong. Bob needs some redundancy in the incoming messages to determine that rrors are present. One very crude form of redundancy is repeating the message two times. If the two copies are not identical, Bob knows that either the fiber is very noisy or someone is tampering with the transmission. Of course, sending everything twice is overkill; a Hamming or Reed-Solomon code is a more efficient way to do error detection and correction. But it should be clear that some redundancy is needed to distinguish a valid message from an invalid message, especially in the face of an active intruder.

**Freshness:**

The second cryptographic principle is that measures must be taken to ensure that each message received can be verified as being fresh, that is, sent very recently. This measure is needed to prevent active intruders from playing back old messages. If no such measures were taken, our ex-employee could tap TCP's phone line and just keep repeating previously sent valid messages.

Thus, Cryptographic principle 2: Some method is needed to foil replay attacks One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds and compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

13. List out the elements of transport protocol and explain.

**Elements of Transport protocol:**

Transport protocols are responsible for providing reliable data delivery services between end systems. The following are the key elements of transport protocols:

1. **Service types:** Transport protocols offer different types of services to meet the varying needs of applications. The most common services include connection-oriented, reliable delivery and connectionless, best-effort delivery.
2. **Addressing:** Transport protocols use port numbers to identify the application endpoints on the hosts. Port numbers are 16-bit numbers that allow the transport layer to differentiate between multiple applications running on the same host.
3. **Multiplexing/demultiplexing:** Multiplexing refers to the process of combining multiple data streams into a single connection. Demultiplexing is the reverse process of separating the multiple data streams and delivering them to the appropriate applications on the receiving end.
4. **Error control:** Transport protocols use error control mechanisms to detect and recover from errors in data transmission. The most common error control mechanisms are error detection codes, such as checksums, and error correction codes, such as forward error correction (FEC).
5. **Segmentation:** The transport protocol divides the data into smaller units, called segments or packets, for efficient transmission over the network. The segments are then reassembled at the receiver's end to form the original data. The size of the segments can be fixed or variable and is determined by various factors such as the maximum segment size (MSS) supported by the network and the buffer size at the receiver's end.
6. **Error recovery:** The transport protocol provides mechanisms for error detection and recovery to ensure reliable data transmission. This is typically achieved through the use of checksums, sequence numbers, and acknowledgments. When a segment is received, the receiver calculates its checksum and compares it with the expected value. If the checksums do not match, the segment is considered corrupt, and the receiver requests the sender to retransmit the segment.
7. **Flow control:** Flow control is a mechanism that regulates the rate of data transmission to prevent the receiver's buffer from overflowing. The transport protocol uses a sliding window mechanism to control the flow of data. The sender can only send a fixed number of segments, called the window size, before waiting for acknowledgments from the receiver. The receiver can also control the flow of data by specifying the size of its receive buffer.
8. **Congestion control:** Congestion control is a mechanism that prevents network congestion by regulating the rate of data transmission. The transport protocol uses various algorithms, such as TCP congestion control, to adjust the rate of data transmission based on the network conditions. When the network is congested, the

sender reduces the rate of data transmission to prevent further congestion and retransmits lost segments after a certain timeout period.

9. **Connection management:** The transport protocol establishes and terminates a connection between the sender and the receiver. Connection management involves three-way handshake, in which the sender and receiver exchange messages to agree on the initial sequence numbers, window sizes, and other parameters before data transmission can begin. The connection is terminated through a four-way handshake, in which both parties exchange messages to confirm the end of data transmission.

15. Explain the working of Handshake protocol.

The handshake protocol is a mechanism used in computer networks to establish a connection between two devices or applications. It is a key component of various protocols, including Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Internet Protocol Security (IPsec). The handshake protocol enables secure communication between two parties by establishing a shared secret key, which is used for encrypting and decrypting data transmitted between them.

The handshake protocol involves a series of steps, as outlined below:

1. **Initialization:** The process begins with an initialization phase, in which the two parties exchange information about the protocols and algorithms they support, as well as any other relevant parameters such as session IDs and nonce values.
2. **Key exchange:** The parties then perform a key exchange, in which they each generate a secret key based on the exchanged information. This key is used for encrypting and decrypting data transmitted between them.
3. **Authentication:** Once the keys have been exchanged, the parties authenticate each other to ensure that they are who they claim to be. This may involve presenting digital certificates, verifying passwords, or using other authentication mechanisms.
4. **Session key derivation:** Using the shared secret key, the parties derive a session key that is used for encrypting and decrypting data transmitted between them during the session.
5. **Cipher suite negotiation:** The parties negotiate a cipher suite, which is a set of cryptographic algorithms used to protect the data transmitted between them. The cipher suite includes algorithms for key exchange, encryption, message authentication, and integrity checking.
6. **Finished message:** Finally, the parties exchange finished messages to confirm that the handshake process has been completed successfully. The finished messages contain a hash of all the previous handshake messages, ensuring that the entire handshake process has not been tampered with or compromised.

Once the handshake protocol is complete, the two parties can begin securely transmitting data between them using the agreed-upon cipher suite and session key. The handshake protocol is typically performed only once per session, and subsequent data transmissions use the established session key and cipher suite for secure communication.

The handshake protocol is a critical component of secure communication in computer networks, enabling two parties to establish a secure connection by exchanging information, generating a shared secret key, authenticating each other, negotiating a cipher suite, and exchanging finished messages to confirm the handshake process's success.

16. Explain about RSA algorithm

RSA is a public-key cryptosystem that is widely used for secure communication over computer networks. It was invented by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977, and is named after their initials. RSA is based on the mathematical properties of prime numbers and is considered one of the most secure cryptographic algorithms available today.

The RSA algorithm works as follows:

1. **Key Generation:** The first step in using RSA is to generate a public-private key pair. The public key is used for encrypting messages, while the private key is used for decrypting them. The key pair is generated as follows:
    i. Choose two large prime numbers p and q.
    ii. Compute their product n = p * q.

iii. Compute Euler's totient function of n, φ(n) = (p - 1) * (q - 1).
iv. Choose a small odd integer e such that 1 < e < φ(n) and gcd(e, φ(n)) = 1.
v. Compute d, the modular multiplicative inverse of e modulo φ(n), i.e., d = e^-1 (mod φ(n)).
vi. The public key is (n, e), while the private key is (n, d).

The values of p and q are kept secret, while the other parameters are made public.

2. **Encryption:** To encrypt a message m using the public key (n, e), the sender computes the ciphertext c as follows:

   c = m^e (mod n)

   Here, ^ denotes exponentiation, and mod n means taking the remainder after division by n. The sender then transmits the ciphertext c to the receiver.
3. **Decryption:** To decrypt the ciphertext c using the private key (n, d), the receiver computes the plaintext m as follows:

   m = c^d (mod n)

   Here, ^ denotes exponentiation, and mod n means taking the remainder after division by n. The receiver then obtains the plaintext m.

The security of RSA is based on the difficulty of factoring large integers into their prime factors. Given the public key (n, e), an attacker would need to factor n into its prime factors p and q to obtain the private key (n, d). However, factoring large integers is believed to be a computationally difficult problem, especially for sufficiently large values of p and q.

RSA is used in a wide range of applications, including secure communication over the Internet, digital signatures, and secure authentication. It is also used in various security protocols, such as Transport Layer Security (TLS), Secure Shell (SSH), and Pretty Good Privacy (PGP).

RSA has some limitations, however. The key size required for security increases with advances in computing power, and RSA is vulnerable to attacks based on quantum computing. To address these issues, various post-quantum cryptography algorithms are being developed, which are believed to be resistant to quantum attacks.

The RSA algorithm is a widely used public-key cryptosystem that is based on the mathematical properties of prime numbers. It enables secure communication over computer networks by generating a public-private key pair, encrypting messages using the public key, and decrypting them using the private key. RSA is a critical component of various security protocols and applications, and its security is based on the difficulty of factoring large integers into their prime factors.