SUB CNS END

Q1 a) Connection establishment and data transfer in AODV and DSDV [9 Marks]

i) AODV (Ad hoc On-demand Distance Vector Routing):

- **Type**: Reactive routing protocol.
- **Connection Establishment:**
  - A source node broadcasts a **Route Request (RREQ)** when it needs a route.
  - Intermediate nodes forward RREQ and record the reverse route to the source.
  - When the destination or a node with a fresh route receives RREQ, it replies with **Route Reply (RREP)**.
  - RREP travels back to the source using the reverse path.
- **Data Transfer:**
  - Once the route is established, data packets are forwarded through the discovered path.
  - If the path breaks, a **Route Error (RERR)** is sent to the source, and a new route discovery starts.

Diagram Explanation (draw this):

Source → RREQ → → Intermediate Nodes → Destination

← ← ← RREP ← ← ←

---

ii) DSDV (Destination-Sequenced Distance Vector):

- **Type**: Proactive routing protocol.
- **Connection Establishment:**
  - Every node maintains a routing table with the next hop and number of hops to all destinations.
  - Routing tables are periodically updated and exchanged between nodes.
- **Data Transfer:**

    - Since routes are always maintained and available, data is forwarded immediately using the routing table.

Diagram Explanation (draw a node table like below):

Node A Routing Table:

Dest	Next Hop	Hops	Seq. No.
B	B	1	12
C	B	2	10

Q1 b) Layered Architecture for Sensor Network [9 Marks]

Sensor Network Layered Architecture:

Typically consists of **5 layers**:

1. **Physical Layer:**
    - Deals with frequency selection, carrier frequency generation, modulation.
    - Handles transmission and reception of raw data.
2. **Data Link Layer:**
    - Responsible for multiplexing of data streams, data frame detection, error control, and MAC (Medium Access Control).
    - Ensures reliable point-to-point and point-to-multipoint connections.
3. **Network Layer:**
    - Manages routing of data from sensor nodes to the base station.
    - Handles issues like data aggregation and energy-efficient routing.
4. **Transport Layer:**
    - Provides reliable message delivery and congestion control.
    - May be lightweight depending on application needs.
5. **Application Layer:**
    - Defines application-specific functions.
    - Provides query processing, data aggregation, and data visualization.

Diagram Explanation (draw a 5-layer stack like OSI):

```
+----------------------+
| Application Layer    |
+---------------------+
| Transport Layer      |
+---------------------+
| Network Layer        |
+---------------------+
| Data Link Layer      |
+---------------------+
| Physical Layer       |
+---------------------+
```

Q2 a) Differentiate between Infrastructure Network and Infrastructure-less Network [6 Marks]

Feature	**Infrastructure Network**	**Infrastructure-less Network (Ad-hoc)**
Definition	Uses centralized devices (like access points or base stations) for communication.	Devices communicate directly without centralized control.
Control	Centralized control via access point.	Distributed control among all devices.
Scalability	More scalable due to centralized management.	Less scalable, complex with more devices.
Setup Time	Takes time to set up due to required hardware.	Quick and easy to set up.
Reliability	Generally more reliable and secure.	Less reliable, prone to interference.
Example	Wi-Fi with router.	Bluetooth or mobile hotspot sharing.

Q2 b) Hidden Station and Exposed Station Problem in WLAN [6 Marks]

Hidden Station Problem:

- Occurs when two nodes are **out of range** of each other but **both can communicate with a common access point**.
- These nodes **can't detect each other's signals**, so they might transmit at the same time → **collision** at the access point.

Example:

A → AP ← C   (A and C cannot hear each other)

- Both A and C transmit to AP, causing a collision.

Exposed Station Problem:

- Occurs when a node **refrains from transmitting** because it **overhears a transmission**, even though its transmission would not cause a collision.

Example:

A → B   C → D

- C hears A's transmission to B, so it **thinks the medium is busy**, but C to D would not interfere. So, **C unnecessarily delays**.

Q2 c) Explain Distributed Denial of Service (DDoS) Attacks [6 Marks]

Definition:

A **DDoS attack** is an attempt to make an online service unavailable by **overwhelming it with traffic** from multiple sources.

How It Works:

- The attacker controls multiple systems (called **botnets**) infected with malware.
- These systems simultaneously send massive traffic or requests to the target server/network.

Objectives:

- Disrupt services (websites, servers, apps).
- Cause financial loss or reputational damage.
- Sometimes used as a distraction for other attacks.

Example:

Thousands of computers flooding a bank’s website with fake requests, making it **inaccessible to real users**.

Here is the **complete answer for Q3 (a and b)** from your exam paper, written in a clear **exam-style** format:

Q3 a) What is network attack? Write short notes on the following with suitable example [8 Marks]

Network Attack:

A **network attack** is any unauthorized action aimed at accessing, altering, or destroying data on a computer network. These attacks can be either **active** or **passive**.

i) Active Attack:

- Involves modification or disruption of the data or system.
- The attacker tries to alter data packets or affect operations.
- These attacks can be **detected**.

Examples:

- **Man-in-the-Middle (MITM)**: Attacker intercepts and alters communication between two parties.
- **Denial of Service (DoS)**: Making a network resource unavailable.

ii) Passive Attack:

- Involves **monitoring or listening** to communication without altering it.
- The main goal is to **gather information**.
- These attacks are **difficult to detect**.

Examples:

- **Eavesdropping**: Intercepting data like passwords or confidential messages.
- **Traffic Analysis**: Studying the flow of packets to gain insights.

Q3 b) What is Cipher Feedback Mode (CFM)? Explain the process with suitable diagram [9 Marks]

Cipher Feedback Mode (CFB):

CFB is a **block cipher mode** that allows **block ciphers to act like stream ciphers**. It enables encryption of small amounts of data such as bytes or bits.

Process:

1. **Initialization Vector (IV)** is encrypted with the block cipher.
2. The output is **XORed with the plaintext** to produce ciphertext.
3. The ciphertext block is then used as the **next input** to the encryption function.

Steps (Assume block size = 8 bits):

1. Encrypt IV using block cipher → Output1

2. Ciphertext1 = Output1 XOR Plaintext1

3. Encrypt Ciphertext1 → Output2

4. Ciphertext2 = Output2 XOR Plaintext2

... and so on

Diagram (Describe or draw):

Plaintext1 → XOR ← Encrypt ← IV

↓

Ciphertext1

Plaintext2 → XOR ← Encrypt ← Ciphertext1

↓

Ciphertext2

Key Features:

- Suitable for encrypting data streams.
- Errors in one block affect only the next few blocks.
- Requires synchronization between sender and receiver.

Here is the **complete answer for Q4 (a, b, c)** from your exam paper, formatted in a clear **exam-style** manner:

Q4 a) What is Electronic Code Book (ECB)? Explain the process with suitable diagram [5 Marks]

Electronic Code Book (ECB) Mode:

ECB is the **simplest mode of block cipher encryption**, where each block of plaintext is **independently encrypted** using the same key.

Process:

- The plaintext is divided into **fixed-size blocks** (e.g., 64 or 128 bits).
- Each block is encrypted **separately** using the same encryption key.
- No chaining or feedback is used.

Diagram (describe or draw):

Plaintext Block1 → Encrypt(Key) → Ciphertext Block1

Plaintext Block2 → Encrypt(Key) → Ciphertext Block2

Plaintext Block3 → Encrypt(Key) → Ciphertext Block3

Features:

- Fast and simple to implement.
- **Weakness**: Identical plaintext blocks yield identical ciphertext → not secure for repetitive data (e.g., images or patterns).

Q4 b) Describe the following network security threats [6 Marks]

i) Unauthorized Access:

- Refers to accessing computer systems, networks, or data **without permission**.
- Attackers may steal, alter, or delete sensitive information.
- Can occur due to **weak passwords**, **misconfigured systems**, or **exploited vulnerabilities**.

Example: A hacker logging into a server without authorization using stolen credentials.

---

ii) Distributed Denial of Service (DDoS) Attacks:

- Involves flooding a target system (website/server) with massive amounts of traffic from **multiple sources** (botnets).

- The goal is to **overwhelm the server** and make it unavailable to legitimate users.

Example: Thousands of infected computers sending requests to a website, making it crash.

Q4 c) Differentiate between Active Attack and Passive Attack [6 Marks]

Feature	**Active Attack**	**Passive Attack**
Action	Modifies or disrupts data	Monitors or listens to data
Goal	Cause damage or alter communication	Gather information without detection
Detection	Easier to detect	Hard to detect
Examples	DoS, MITM, data modification	Eavesdropping, traffic analysis
Impact	Direct damage to system/data	Breach of confidentiality

---

Here is the **complete answer for Q5 (a and b)** from your exam paper **[Computer Networks and Security]**, written in a clear **exam-style format**:

Q5 a) Define and list various computer network security mechanisms. Also write short notes on the following terms [9 Marks]

Definition:

Network security mechanisms are methods or tools used to protect data and systems from unauthorized access, attacks, and data breaches in a networked environment.

Common Security Mechanisms:

1. **Encryption**
2. **Decryption**
3. **Authentication**
4. **Access Control**
5. **Firewalls**
6. **Intrusion Detection Systems (IDS)**
7. **Digital Signatures**

8. **Hash Functions**
9. **Antivirus and Anti-malware tools**

---

i) Encryption:

- **Definition**: The process of converting **plaintext into ciphertext** using an encryption algorithm and a key to prevent unauthorized access.
- **Purpose**: Ensures confidentiality of the data during storage or transmission.
- **Example**: AES (Advanced Encryption Standard), RSA.

---

ii) Decryption:

- **Definition**: The reverse process of encryption, where **ciphertext is converted back into plaintext** using a decryption algorithm and key.
- **Purpose**: Allows authorized users to retrieve the original data.
- **Example**: Using a private key to decrypt a message encrypted with a public key.

Q5 b) Define and explain digital signature. What are the applications of digital signature? [9 Marks]

Definition of Digital Signature:

A **digital signature** is a cryptographic technique used to **verify the authenticity and integrity** of a digital message or document. It is the digital equivalent of a handwritten signature or stamped seal.

How It Works:

1. The sender hashes the message using a **hash function**.
2. The hash is then **encrypted with the sender's private key**.
3. This encrypted hash is the **digital signature**.
4. The receiver decrypts it using the sender's **public key** and compares the hash.

Diagram (to be drawn):

Sender:

Message → Hash → Encrypt (Private Key) → Digital Signature

Receiver:

Message → Hash → Decrypt (Sender’s Public Key) → Verify Hash

Applications of Digital Signatures:

1. **Email Authentication** – To confirm sender identity.
2. **Software Distribution** – To ensure software hasn’t been tampered with.
3. **Online Transactions** – For secure financial dealings.
4. **e-Governance** – Digital certificates in Aadhaar, PAN, etc.
5. **Legal Documents** – eContracts and eFiling with legal authority.

Here is the **complete answer for Q6 (a and b)** from your exam paper, formatted in a clear **exam-style** format:

Q6 a) Define the following mathematical preliminaries and explain in brief [9 Marks]

i) Prime Numbers:

- A **prime number** is a natural number greater than 1 that has **only two positive divisors**: 1 and itself.
- It **cannot be divided evenly** by any number other than 1 and itself.
- **Examples**: 2, 3, 5, 7, 11, 13...

Importance in Cryptography:

- Prime numbers are fundamental in **public key algorithms** like RSA, where the security depends on the difficulty of **factoring large prime products**.

---

ii) Group:

- A **group** is a set of elements combined with an operation that satisfies **four properties**:
    1. **Closure**: a * b ∈ G for all a, b ∈ G
    2. **Associativity**: (a * b) * c = a * (b * c)

3. **Identity**: There exists an element e such that a * e = e * a = a
4. **Inverse**: For every a ∈ G, there exists an element a^{-1} such that a * a^{-1} = a^{-1} * a = e

Example: Integers under addition form a group.

Relevance: Groups are the foundation of **modular arithmetic** and **elliptic curve cryptography**.

Q6 b) What is Cryptography? Also explain the following terms: [9 Marks]

Definition of Cryptography:

Cryptography is the **science of securing communication** by converting data into an unreadable format (encryption), so that **only authorized parties can understand** it.

---

i) Public Key Encryption:

- Uses a pair of keys: a **public key** (shared with everyone) and a **private key** (kept secret).
- The sender encrypts data with the receiver's **public key**, and only the receiver can decrypt it using their **private key**.

Example: RSA algorithm.

Uses:

- Secure messaging
- Digital signatures
- Secure web transactions (HTTPS)

---

ii) Hash Function:

- A **hash function** takes input data and produces a **fixed-size string of characters**, which is typically a digest that uniquely represents the data.
- **One-way function**: Cannot retrieve original data from hash.
- **Deterministic**: Same input → same hash.

Properties:

- Collision-resistant

- Fast computation
- Pre-image resistance

Example: SHA-256, MD5

Applications:

- Password storage
- Data integrity verification
- Blockchain technology

Here is the **complete answer for Q7 (a and b)** from your **Computer Networks and Security** paper, formatted in a clear **exam-style** format:

Q7 a) What is Cyber Terrorism? What is an example of cyber terrorism? [8 Marks]

Definition of Cyber Terrorism:

Cyber terrorism is the use of **internet-based attacks to cause large-scale disruption, fear, or damage** to infrastructure, systems, or people. It is usually politically or ideologically motivated.

Characteristics:

- Targets critical systems like power grids, hospitals, transport, or government websites.
- May involve data theft, destruction, or service disruption.
- Aimed at causing panic, economic loss, or political instability.

Example of Cyber Terrorism:

A hacker group attacking a **nation's power grid** using malware to cause a **nationwide blackout**, disrupting emergency services and causing chaos — all for political or ideological purposes.

Another example: **Stuxnet worm**, which was used to damage Iran's nuclear facilities.

Q7 b) Define Crime and Cybercrime. State Cybercrimes classification. [9 Marks]

Crime:

A **crime** is any **illegal activity or act** that violates the law and is punishable by the government through fines, imprisonment, or both.

Cybercrime:

Cybercrime refers to **criminal activities conducted using computers, networks, or the internet**. It includes crimes that target computers or use them as tools to commit other offenses.

Classification of Cybercrimes:

1. **Cybercrimes Against Individuals:**
    - Cyberstalking
    - Identity theft
    - Harassment via email or social media
2. **Cybercrimes Against Property:**
    - Hacking
    - Intellectual property theft (e.g., software piracy)
    - Spreading malware (viruses, worms)
3. **Cybercrimes Against Government:**
    - Cyber terrorism
    - Hacking government websites
    - Spying or data theft (espionage)
4. **Cybercrimes Against Society:**
    - Distribution of child pornography
    - Spreading fake news or hate speech
    - Online drug or weapon trafficking

Here's an answer to Q8 based on the provided document:

Q8) a) Explain the term Phishing & SQL Injection.

b) What Is Cyberstalking explain with an example.

Answer:

a) Phishing & SQL Injection

- **Phishing:** Phishing is a type of cybercrime where attackers attempt to trick individuals into revealing sensitive information, such as usernames, passwords, and credit card[1] details, by disguising themselves as a trustworthy entity in an electronic communication[cite:[2] 16]. This is often done through emails that appear to be from legitimate organizations like banks, social media platforms, or government agencies. These emails usually contain malicious links that direct the user to a fake website designed to look like the real one, or they may contain attachments with malware.
- **SQL Injection:** SQL Injection is a code injection technique used to attack data-driven applications. It occurs when an attacker inserts malicious SQL (Structured Query Language) code into input fields on a website or application. If the application's software is vulnerable, this malicious code can then be executed by the database, allowing the attacker to bypass security measures, retrieve, modify, or delete sensitive data, or even gain control over the database server.

b) Cyberstalking

- **Cyberstalking:** Cyberstalking refers to the use of the internet or other electronic means to stalk or harass an individual, a group, or an organization[cite:[3] 16]. It involves repeated, unwelcome actions that cause a reasonable person to feel fear, annoyance, or emotional distress. Cyberstalking can manifest in various ways, including:
    - Sending unwanted and threatening emails or messages.
    - Harassing victims on social media platforms.
    - Monitoring a person's online activity without their consent.
    - Spreading false rumors or defamatory information online.
    - Impersonating the victim online to damage their reputation.
    - Ordering goods or services in the victim's name.
- **Example of Cyberstalking:** A common example of cyberstalking could be a former partner repeatedly sending unwanted, aggressive, or threatening messages via email and social media to their ex-partner after a breakup. This might include posting private information or embarrassing photos of the ex-partner online, creating fake social media profiles to follow and harass them, or even sending threats to their friends and family, causing the victim to fear for their safety and well-being.

PAPAER 2

Here's the answer to Q1 based on the provided document:

Q1) a) Explain MACAW protocol in details.

b) Explain with diagram Layered Architecture for Sensor Network.

Answer:

a) MACAW Protocol:

The MACAW (Multiple Access with Collision Avoidance for Wireless) protocol is an enhancement to the MACA protocol, designed to address some of its limitations in wireless networks. Key aspects of MACAW include:

- **Problem it addresses:** It aims to reduce the problem of hidden terminals and exposed terminals in wireless communication by using a mechanism that involves an exchange of control packets before actual data transmission.
- **Mechanism:** MACAW introduces a Request-to-Send (RTS), Clear-to-Send (CTS), Data (DATA), and Acknowledgment (ACK) exchange. However, it specifically enhances MACA by adding a Data-Sending (DS) and Request-for-Request-to-Send (RTS) mechanisms to improve fairness and efficiency in a multi-hop environment.
- **Carrier Sense:** Unlike some simpler protocols, MACAW uses carrier sense not only for determining if the channel is busy but also for adapting its behavior.
- **Congestion Control:** It also incorporates a mechanism for congestion control by adjusting the backoff timer based on network conditions, which helps in improving overall throughput in dense wireless networks.

b) Layered Architecture for Sensor Network:

A typical layered architecture for a sensor network is often depicted with five layers, though variations exist. This architecture facilitates the design, deployment, and management of sensor networks by breaking down complex functionalities into manageable modules. A common layered architecture includes:

- **Application Layer:** This is the top layer and is responsible for the specific task of the sensor network. It provides software for end-users to interact with the sensor data and the network. For example, in a habitat monitoring application, this layer would present temperature, humidity, or animal movement data to researchers.
- **Presentation Layer:** This layer is responsible for data formatting and translation to ensure that data can be correctly interpreted by applications and different

sensor nodes. It handles data compression, encryption, and other transformations.

- **Transport Layer:** This layer is responsible for reliable end-to-end data transfer between the sink node (base station) and the sensor nodes. It handles flow control, congestion control, and error recovery. Examples include TCP or UDP-like protocols adapted for sensor networks.
- **Network Layer:** The network layer is crucial for routing data packets from sensor nodes to the sink node. Given the resource constraints of sensor nodes and the dynamic nature of wireless sensor networks, routing protocols at this layer are often energy-aware and self-organizing. Examples include various routing protocols like AODV or DSDV adapted for sensor networks.
- **Data Link Layer:** This layer handles reliable point-to-point and point-to-multipoint communication. It manages media access control (MAC) and error control for the wireless links between sensor nodes. It often includes mechanisms for collision avoidance and power management.
- **Physical Layer:** This is the lowest layer and deals with the actual transmission and reception of raw bits over the wireless medium. It defines the hardware specifications, modulation techniques, frequency selection, and power management for radio communication between sensor nodes.

Diagram:

A diagram would typically show these layers stacked vertically, with arrows indicating the flow of data up and down the stack, and horizontal interactions between peer layers on different nodes. It would also show sensor nodes communicating wirelessly and eventually sending data to a sink node or base station.

Here's the answer to Q2 based on the provided document:

Q2) a) Explain different issues and Challenges protocol for Ad-hoc Wireless Network.

b) What are hidden station and exposed station problem in WLAN.

c) Explain with diagram Layered Architecture for Sensor Network.

Answer:

a) Issues and Challenges in Ad-hoc Wireless Network Protocols:

Designing protocols for Ad-hoc Wireless Networks (also known as Mobile Ad-hoc Networks or MANETs) presents several significant challenges due to their unique characteristics. Some of the key issues and challenges include:

- **Dynamic Topology:** The nodes in an ad-hoc network are mobile and can join or leave the network at any time. This frequent change in network topology makes it difficult to maintain stable routes and can lead to frequent route breaks, impacting data delivery.
- **Limited Resources:** Ad-hoc nodes often operate on battery power and have limited computational capabilities and memory. Protocols must be designed to be energy-efficient and lightweight to conserve these scarce resources.
- **Security Vulnerabilities:** The decentralized nature of ad-hoc networks, without a fixed infrastructure or central authority, makes them highly susceptible to various security threats, including eavesdropping, impersonation, and denial-of-service attacks.
- **Scalability:** As the number of nodes in an ad-hoc network increases, maintaining efficient routing and communication becomes challenging. Protocols need to be scalable to handle a large number of nodes without significant performance degradation.
- **Bandwidth Constraints:** Wireless links inherently have lower bandwidth compared to wired connections, and this limited bandwidth is shared among all nodes in the vicinity. Efficient bandwidth utilization is crucial for good performance.
- **Quality of Service (QoS):** Providing QoS guarantees (e.g., for real-time applications) in ad-hoc networks is difficult due to variable link quality, dynamic topology, and contention for shared wireless medium.
- **Interference:** Wireless communication is prone to interference from other wireless devices or environmental factors, which can lead to packet loss and reduced network performance.
- **Hidden and Exposed Terminal Problems:** These are specific challenges related to the shared wireless medium that can lead to inefficient channel utilization and collisions. (More details in part b).
- **Routing Overhead:** Maintaining routing information in a dynamic environment can generate significant overhead in terms of control messages, consuming bandwidth and energy.

b) Hidden Station and Exposed Station Problem in WLAN:

These are common problems in Wireless Local Area Networks (WLANs) that arise due to the nature of wireless communication and can lead to inefficient channel utilization and collisions.

- **Hidden Station Problem:**

    - **Description:** A hidden station (or hidden terminal) refers to a situation where two stations are out of range of each other, but both are within range of a third station (typically an access point). When one of the hidden stations transmits, the other hidden station cannot hear the transmission and thus assumes the channel is free. If both transmit simultaneously to the common receiver, a collision occurs at the receiver.
    - **Example:** Imagine three stations: A, B, and C. A can hear B, and C can hear B, but A and C cannot hear each other. If A starts transmitting to B, C cannot detect this transmission. If C then decides to transmit to B, a collision will occur at B, even though both A and C thought the channel was clear.
    - **Diagram:** (Imagine a diagram with three nodes A, B, C. B is in the middle. A has a communication range that covers B but not C. C has a communication range that covers B but not A. An arrow from A to B and C to B indicates communication. A dashed line between A and C indicates they cannot hear each other.)
- **Exposed Station Problem:**
    - **Description:** An exposed station (or exposed terminal) refers to a situation where a station is within the transmission range of another station, preventing it from transmitting, even though its transmission would not cause interference at the intended receiver.
    - **Example:** Consider four stations: A, B, C, and D arranged linearly. A can hear B, B can hear A and C, C can hear B and D, and D can hear C. If B is transmitting to A, C can hear B's transmission and might defer its own transmission to D, even though C's transmission to D would not interfere with B's transmission to A (as D is out of range of B). This leads to inefficient use of the spectrum.
    - **Diagram:** (Imagine a diagram with four nodes A, B, C, D in a line. A-B link, B-C link, C-D link. B's range covers A and C. C's range covers B and D. If B transmits to A, C detects B's transmission and mistakenly assumes it cannot transmit to D, even though D is not affected by B's transmission.)

c) Layered Architecture for Sensor Network:

A typical layered architecture for a sensor network is often depicted with five layers, though variations exist. This architecture facilitates the design, deployment, and management of sensor networks by breaking down complex functionalities into manageable modules. A common layered architecture includes:

- **Application Layer:** This is the top layer and is responsible for the specific task of the sensor network. It provides software for end-users to interact with the sensor data and the network. For example, in a habitat monitoring application, this layer would present temperature, humidity, or animal movement data to researchers.
- **Presentation Layer:** This layer is responsible for data formatting and translation to ensure that data can be correctly interpreted by applications and different sensor nodes. It handles data compression, encryption, and other transformations.
- **Transport Layer:** This layer is responsible for reliable end-to-end data transfer between the sink node (base station) and the sensor nodes. It handles flow control, congestion control, and error recovery. Examples include TCP or UDP-like protocols adapted for sensor networks.
- **Network Layer:** The network layer is crucial for routing data packets from sensor nodes to the sink node. Given the resource constraints of sensor nodes and the dynamic nature of wireless sensor networks, routing protocols at this layer are often energy-aware and self-organizing. Examples include various routing protocols like AODV or DSDV adapted for sensor networks.
- **Data Link Layer:** This layer handles reliable point-to-point and point-to-multipoint communication. It manages media access control (MAC) and error control for the wireless links between sensor nodes. It often includes mechanisms for collision avoidance and power management.
- **Physical Layer:** This is the lowest layer and deals with the actual transmission and reception of raw bits over the wireless medium. It defines the hardware specifications, modulation techniques, frequency selection, and power management for radio communication between sensor nodes.

Diagram:

(Imagine a diagram with five layers stacked vertically, from top to bottom: Application Layer, Transport Layer, Network Layer, Data Link Layer, and Physical Layer. Arrows would show data flow down through the layers at the source node, across the wireless medium at the physical layer, and then up through the layers at the destination node. This diagram would be similar to the OSI model but adapted for sensor networks.)

Here's the answer to Q3 based on the provided document:

Here's a breakdown of Q4, focusing on network security threats and information security principles, in a notes format:

Q4) a) Describe the following network security threats:

- **i) Unauthorized access:** This refers to gaining entry to a system or network without proper permission.
- **ii) Distributed Denial of Service (DDoS) attacks:** These attacks aim to disrupt a service by overwhelming it with a flood of traffic from multiple compromised sources.

Q4) b) Describe the following fundamental principles of Information security:

- **i) Integrity:** This principle ensures that information remains accurate, complete, and trustworthy, preventing unauthorized modification.
- **ii) Authentication:** This process verifies the identity of a user, device, or process attempting to access a system or resource.
- **iii) Authorization and Access Control:** Authorization determines what a verified user or entity is permitted to do, while access control mechanisms enforce these permissions, restricting access to resources based on defined rules.

Q4) c) What is Cipher Feedback Mode (CFM) and Electronic Codebook (ECB)?

- **Cipher Feedback Mode (CFM):** This is a block cipher mode of operation that processes data in smaller units (like a stream cipher) by using the output of the previous encryption or a portion of the plaintext as feedback for the next encryption block.
- **Electronic Codebook (ECB):** This is a simple block cipher mode where each block of plaintext is encrypted independently using the same key. Identical plaintext blocks will result in identical ciphertext blocks.

Here's an explanation of Q5, building on the notes format:

Q5) a) Data Encryption Standard (DES) Algorithm:

The Data Encryption Standard (DES) is a symmetric-key block cipher algorithm, meaning it uses the same key for both encryption and decryption. It was a widely used standard for many years, though it's now considered insecure for most applications due to its relatively short key length.

- **Block Cipher Operation:** DES operates on fixed-size blocks of plaintext, typically 64 bits at a time. It transforms this 64-bit plaintext into a 64-bit ciphertext using a 56-bit key.
- **Feistel Structure:** DES is based on the Feistel cipher structure. This structure allows the encryption and decryption processes to be very similar, using the same set of operations but in reverse order for decryption. The 64-bit input block is divided into two 32-bit halves. These halves are then processed through a series of rounds.

- **Number of Rounds:** DES employs 16 identical rounds of operations. Each round involves a substitution and permutation process.
- **Key Length:** While the input key is 64 bits, 8 of these bits are used for parity checking, resulting in an effective key length of 56 bits. This 56-bit key is then used to generate 16 subkeys, one for each round.
- **Initial and Final Permutations:** Before the main 16 rounds, the 64-bit plaintext undergoes an initial permutation (IP). After the 16 rounds, a final permutation (FP), which is the inverse of the IP, is applied to the output. These permutations do not enhance security but were originally thought to complicate cryptanalysis.
- **Round Function (f-function):** The core of each round is the f-function. In each round, one half of the block is combined with a subkey, and the result is then XORed with the other half. The f-function involves:
  - **Expansion P-box:** The 32-bit right half of the data block is expanded to 48 bits.
  - **XOR with Subkey:** The expanded 48 bits are XORed with a 48-bit subkey generated from the main key.
  - **S-boxes (Substitution Boxes):** The 48-bit result is then divided into eight 6-bit chunks, and each chunk is fed into a separate S-box. Each S-box performs a non-linear substitution, mapping 6 input bits to 4 output bits, resulting in a 32-bit output. This is where the non-linearity of DES comes from, making it resistant to linear cryptanalysis.
  - **Permutation P-box:** The 32-bit output from the S-boxes is then permuted by a P-box.
- **Key Schedule Generation:** The 56-bit effective key is used to generate 16 different 48-bit subkeys, one for each round. This involves shifts and permutations of the main key.
- **Diagram:** A suitable diagram would typically show the overall Feistel structure, with the 16 rounds, initial/final permutations, and then a more detailed view of a single round, illustrating the f-function components (expansion, key XOR, S-boxes, P-box).

Q5) b) Diffie-Hellman Algorithm:

The Diffie-Hellman (DH) algorithm is a widely used cryptographic protocol that allows two parties to establish a shared secret key over an insecure communication channel, even if an eavesdropper is listening. The key idea is that they don't actually transmit the shared secret key itself; instead, they exchange public information from which they can *derive* the same secret key independently.

- **Purpose:** To enable two parties (let's say Alice and Bob) to agree on a secret key that can then be used for symmetric-key encryption (like AES or even DES once the key is established) to secure their subsequent communications.
- **How it Works (Based on Exponentiation in a Finite Field):** The security of Diffie-Hellman relies on the computational difficulty of solving the discrete logarithm problem.
- **Publicly Agreed Parameters:**
    - **Prime Number (p):** Alice and Bob first publicly agree on a large prime number, p. This number is known to everyone, including potential eavesdroppers.
    - **Primitive Root Modulo (g) of p:** They also agree on an integer g that is a primitive root modulo p. This means that the powers of g modulo p will generate all numbers from 1 to $p-1$. Both p and g are public.
- **Private Keys:**
    - **Alice's Private Key (a):** Alice secretly chooses a large random integer, a, as her private key. This key is known only to Alice.
    - **Bob's Private Key (b):** Similarly, Bob secretly chooses a large random integer, b, as his private key. This key is known only to Bob.
- **Public Keys (Exchange):**
    - **Alice's Public Key (A):** Alice computes her public key as A=ga(modp). She then sends A to Bob over the insecure channel.
    - **Bob's Public Key (B):** Bob computes his public key as B=gb(modp). He then sends B to Alice over the insecure channel.
    - An eavesdropper can see p, g, A, and B. However, it's computationally infeasible for them to derive a from A or b from B (this is the discrete logarithm problem).
- **Shared Secret Calculation:**
    - **Alice's Calculation:** Alice receives Bob's public key B. She then computes the shared secret key S as S=Ba(modp). Substituting B=gb(modp), this becomes S=(gb)a(modp)=gba(modp).
    - **Bob's Calculation:** Bob receives Alice's public key A. He then computes the shared secret key S as S=Ab(modp). Substituting A=ga(modp), this becomes S=(ga)b(modp)=gab(modp).

- **Result:** Since gba=gab, both Alice and Bob arrive at the exact same shared secret key S, which no one else can easily determine. This shared secret S can then be used as the key for a symmetric-key encryption algorithm to encrypt their subsequent communication.
- **Man-in-the-Middle (MIM) Attack:** A crucial point about Diffie-Hellman is its susceptibility to a Man-in-the-Middle (MIM) attack. Without proper authentication (e.g., using digital signatures), an attacker can intercept the public key exchanges, establish separate shared secrets with both Alice and Bob, and then relay messages between them, decrypting and re-encrypting them as they pass through. Therefore, Diffie-Hellman is often used in conjunction with other protocols that provide authentication.

Here's a breakdown of Q6 in notes format:

Q6) a) Explain Private Key Management:

- **Definition:** Private key management refers to the secure handling of cryptographic private keys throughout their lifecycle.
- **Key aspects:** This includes generation, storage, distribution, backup, recovery, and destruction of private keys.
- **Importance:** Proper private key management is crucial for maintaining the confidentiality and integrity of encrypted data and digital signatures.
- **Challenges:** Protecting private keys from unauthorized access, compromise, and loss is a significant challenge.

Q6) b) Explain following terms:

- **i) PKIX Model:**
    - **Full form:** Public Key Infrastructure X.509 Model.
    - **Purpose:** It defines a framework for managing digital certificates and public keys.
    - **Components:** Typically includes Certificate Authorities (CAs), Registration Authorities (RAs), repositories, and archiving systems.
    - **Standardization:** Based on the X.509 standard for digital certificates.
- **ii) Digital Signature:**
    - **Definition:** A mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

    - **Functionality:** Provides assurance to the recipient that the message was created by a known sender (authentication) and that it has not been altered in transit (integrity).
    - **Mechanism:** Typically involves encrypting a hash of the message with the sender's private key.
- **iii) Digital Certificate:**
    - **Definition:** An electronic document used to prove the ownership of a public key.
    - **Content:** Contains information about the owner (e.g., name, organization), the public key itself, the issuer (Certificate Authority), and a validity period.
    - **Purpose:** Enables secure communication by allowing parties to verify each other's identities and public keys, preventing "man-in-the-middle" attacks.

Here's the answer to Q7 in notes format:

Q7) a) What is Cyber terrorism? What is an example of cyber terrorism?

- **Cyber terrorism:** This refers to the convergence of terrorism and cyberspace. It involves using computer networks and the internet to carry out terrorist acts or to facilitate traditional terrorist activities. The goal is often to cause widespread disruption, fear, or damage to critical infrastructure, government systems, or public services.
- **Example of Cyber Terrorism:** An example could be a terrorist group launching a coordinated cyberattack against a nation's power grid, aiming to cause widespread blackouts and panic, thereby disrupting essential services and creating a sense of insecurity among the populace. Another example might involve an extremist organization using the internet to recruit and radicalize individuals, spread propaganda, or coordinate physical attacks.

Q7) b) Define Crime and Cybercrime. State Cybercrimes classification.

- **Crime:** In a general sense, a crime is an act or omission that constitutes an offense punishable by law. It is a violation of a legal or moral code, causing harm to individuals or society.
- **Cybercrime:** This specifically refers to any criminal activity that involves a computer, computer network, or networked device. The computer can be the tool used to commit the crime, the target of the crime, or both.

- **Cybercrimes classification:** While classifications can vary, common categories include:
    - **Crimes against individuals:** These target individuals directly, such as cyberstalking, online harassment, identity theft, and phishing.
    - **Crimes against property:** These involve targeting digital assets or financial resources, including financial fraud, credit card fraud, intellectual property theft, and online extortion.
    - **Crimes against government/society:** These aim to disrupt public services, national security, or societal order, such as cyberterrorism, cyberwarfare, and attacks on critical infrastructure.
    - **Computer as a tool:** Crimes where the computer is used to facilitate traditional crimes, such as online drug trafficking, child pornography distribution, or money laundering.
    - **Computer as a target:** Crimes where the computer system itself is the target of the attack, such as hacking, malware distribution (viruses, worms, ransomware), and denial-of-service (DoS) attacks.

Q8Here's the information in notes format:

---

a) Cyberstalking

- **Definition:** Using the internet or electronic means to stalk or harass an individual, group, or organization.
- Involves a **pattern of threatening or malicious online behavior**.
- Causes victim to **fear for safety** or experience **significant emotional distress**.
- Unlike traditional stalking, **doesn't require physical proximity**.

Key Characteristics:

- **Repeated, unwanted contact:** Emails, social media, instant messages, online forums, manipulated phone calls.
- **Threatening/intimidating content:** Direct threats, humiliation, reputational damage, exposure of private info.
- **Monitoring/surveillance:** Tracking online activity, location, personal info.
- **Identity theft/Impersonation:** Fake profiles to interact, gather info, spread misinformation.

- **Doxing:** Publishing private/identifiable info online without consent.
- **Manipulation/Psychological abuse:** Goal is control, fear, anxiety, isolation.

Example:

- **Scenario:** Ben cyberstalks ex-partner Alex after a breakup.
- **Actions:**
    - Sends numerous unwanted, angry emails.
    - Creates fake social media accounts to send threatening messages/post derogatory comments.
    - Spreads rumors on online forums.
    - Creates fake profile impersonating Alex to send embarrassing messages to Alex's friends/colleagues.
    - Potentially tries to access Alex's accounts or track location.
- **Impact:** This continuous, escalating online harassment causes Alex fear and distress.

---

b) Phishing & SQL Injection

Phishing

- **Definition:** Cyberattack where attackers **masquerade as a trustworthy entity** in electronic communication.
- Aims to **trick individuals into revealing sensitive information** (usernames, passwords, credit card details, bank info).
- Appears to come from legitimate organizations (banks, social media, government, companies).

How it Works:

- **Deception:** Relies on **social engineering** to manipulate victims.
- **Urgency/Threats:** Messages create a sense of urgency, fear, or compelling offer.
- **Fake Websites/Forms:** Directs victims to look-alike fake websites to enter credentials.

- **Malicious Attachments/Links:** Contains attachments that install malware or links to infected sites.

Example:

- **Scenario:** You receive an email seemingly from "SecureBank."
- **Email Content:**
    - Subject: "Urgent: Your Account Has Been Locked - Action Required."
    - Body: "Dear Customer, due to unusual activity... click on the link below and verify your details immediately."
    - Link: http://securebank-verification.com/login (malicious, slightly different domain).
- **Outcome:** Clicking the link takes you to a fake login page. Entering your credentials gives them to the attacker, who can then access your real bank account.

SQL Injection (SQLi)

- **Definition:** A **web security vulnerability** allowing an attacker to interfere with an application's database queries.
- Occurs when an application builds SQL statements using **user-supplied input without proper validation/sanitization**.
- Attacker injects **malicious SQL code** into input fields.
- Tricks database into executing **unintended commands**.
- Leads to **data theft, manipulation, or database control**.

How it Works:

- **Vulnerable Input Fields:** Forms (login, search, contact) are common targets.
- **Lack of Input Validation:** Application fails to filter or escape special characters from user input.
- **Malicious Query Construction:** Attacker inserts SQL syntax into input, altering the original query.

Example (Login Bypass):

- **Vulnerable Query:** SELECT * FROM users WHERE username = ' [username_input] ' AND password = ' [password_input] '

- **Attacker Input:**
    - **Username:** ' OR '1'='1
    - **Password:** (anything, doesn't matter for this specific attack)
- **Resulting Query (after injection):** SELECT * FROM users WHERE username = '' OR '1'='1' -- AND password = ' [any_password] '
    - ' closes the username string.
    - OR '1'='1' is always true.
    - -- comments out the rest of the original query.
- **Outcome:** The query effectively becomes SELECT * FROM users WHERE username = '' OR '1'='1', which is always true. This allows the attacker to **bypass login authentication** without knowing valid credentials.

Certainly! Here's a detailed answer for **Q1(a)** and **Q1(b)** suitable for university-level exams like SPPU.

Q1(a) Layered Architecture & Clustered Architecture for Sensor Network [9 Marks]

1. Layered Architecture in Wireless Sensor Networks (WSN)

Layered architecture is similar to the OSI model and provides a structured approach for communication in sensor networks.

Diagram:

```
+--------------------------+

|     Application Layer   |

+--------------------------+

|     Transport Layer     |

+--------------------------+

|      Network Layer      |

+--------------------------+

|  Data Link (MAC) Layer  |

+--------------------------+

|     Physical Layer      |
+-------------------------+
```

Explanation of Layers:

- **Application Layer:** Responsible for traffic management and data formatting. Interfaces with the user applications.
- **Transport Layer:** Ensures reliable data transmission and congestion control.
- **Network Layer:** Manages routing and forwarding of packets.
- **Data Link Layer (MAC):** Responsible for medium access and error detection.
- **Physical Layer:** Handles transmission and reception of raw bit streams over a physical medium.

2. Clustered Architecture in Wireless Sensor Networks

In this architecture, the network is divided into clusters. Each cluster has a **Cluster Head (CH)** that manages communication within the cluster and forwards data to the base station.

Diagram:

```
         +------------------+
         |  Base Station   |
         +--------+---------+
              |
       +------------+-------------+
       |              |
    +----+----+        +----+----+
    | Cluster |        | Cluster |
    |  Head   |        | Head   |
    +----+----+        +----+----+
       |              |
   +------+------+      +-------+------+
   |    |    |       |    |    |
Sensor Sensor Sensor   Sensor  Sensor Sensor
```

Advantages:

- Reduces communication overhead.
- Enhances scalability.
- Saves energy by aggregating data at CHs.

Q1(b) Adhoc Network MAC Layer: Design Issues and Goals

MAC Layer in Adhoc Networks

The MAC (Medium Access Control) layer in ad hoc networks controls how devices access the shared wireless medium without centralized control.

Design Issues:

1. **Collision Avoidance:** Since nodes share the same medium, the protocol must avoid packet collisions.
2. **Hidden Terminal Problem:** Nodes out of each other's range may cause interference.
3. **Exposed Terminal Problem:** A node unnecessarily defers transmission.
4. **Energy Efficiency:** Nodes are battery-powered; MAC protocols must be energy-aware.
5. **Mobility Support:** Frequent topology changes due to node movement.
6. **Fairness:** All nodes should get equal opportunity to transmit data.
7. **Throughput Maximization:** Efficient channel utilization.

Design Goals:

1. **Efficient Medium Access:** Ensure smooth and collision-free data transfer.
2. **Energy Conservation:** Reduce idle listening and retransmissions.
3. **Scalability:** Should work efficiently with a large number of nodes.
4. **Low Latency:** Minimize delay in data transmission.
5. **Adaptability:** Should adjust to changing network conditions.
6. **QoS Support:** Support for real-time data and prioritization.

Let me know if you want diagrams in image format or explanations in simpler terms.

Here's a detailed answer for **Q2(a)** and **Q2(b)** with well-organized points suitable for exam answers:

Q2(a) Issues in Designing a Routing Protocol for Ad Hoc Wireless Networks [9 Marks]

Ad hoc wireless networks are dynamic and infrastructure-less. Designing efficient routing protocols for them is challenging due to the following issues:

1. Dynamic Topology

- Nodes move randomly, leading to frequent changes in network topology.
- Routes may break often, requiring frequent updates.

2. Limited Bandwidth

- Wireless links offer lower bandwidth compared to wired networks.
- Routing protocols must minimize control overhead.

3. Energy Constraints

- Nodes are battery-powered; routing should minimize energy consumption to prolong network life.

4. Scalability

- The protocol should perform well even as the number of nodes increases.

5. Security Threats

- Ad hoc networks are vulnerable to attacks like spoofing, eavesdropping, and denial of service (DoS).
- Routing must consider secure path establishment.

6. Multi-hop Communication

- Nodes rely on others to forward packets.
- Ensures that routing protocols handle multi-hop paths effectively.

7. Mobility Models

- The movement patterns of nodes affect link stability.
- Protocols must adapt quickly to new routes.

8. Broadcast Nature of Wireless Medium

- Routing must handle broadcast and interference effectively.
- Also raises the need for mechanisms like collision avoidance.

9. Quality of Service (QoS)

- Ad hoc applications (like video streaming) may require guaranteed bandwidth, delay, etc.
- Routing should support QoS parameters.

Q2(b) Issues and Challenges in Designing a Sensor Network [9 Marks]

Designing a wireless sensor network (WSN) involves several challenges due to its constraints and application-specific nature.

1. Energy Efficiency

- Sensors are battery-operated with limited power.
- Energy-efficient protocols and hardware are crucial.

2. Limited Computational Power

- Sensor nodes have low processing capability.
- Algorithms must be simple and lightweight.

3. Limited Memory and Storage

- Nodes have constrained memory.
- Data processing and storage must be optimized.

4. Scalability

- Networks may consist of hundreds or thousands of nodes.
- The architecture should support scaling without performance degradation.

5. Fault Tolerance

- Nodes can fail due to battery drain or damage.
- The system must continue functioning with alternative paths.

6. Data Aggregation and Fusion

- Combining data from multiple sensors reduces redundancy.
- Helps save energy and bandwidth.

7. Network Topology

- Often dynamic due to node failure or environmental conditions.
- Protocols must adapt to changes efficiently.

8. Security

- WSNs are prone to attacks (e.g., node capture, spoofing).
- Designing lightweight but secure protocols is a challenge.

9. Communication Constraints

- Limited bandwidth and high error rates in wireless communication.
- Protocols must be optimized for reliability and efficiency.

10. Deployment Environment

- Harsh environments (forests, disaster zones, etc.) can damage nodes.
- Nodes must be robust and self-configurable.

Let me know if you want short answers, MCQs, or diagrams to accompany these notes!

Here's a detailed answer for **Q3(a)** and **Q3(b)**, formatted for exam-style responses:

Q3(a) Importance & Need for Security and Explanation of Network Attacks [8 Marks]

Importance and Need for Security in Networks:

Security in computer networks ensures the **confidentiality, integrity, and availability** (CIA) of data and services.

Key Reasons for Security:

1. **Confidentiality:** Prevents unauthorized access to sensitive information.
2. **Integrity:** Ensures data is not modified or tampered with during transmission.
3. **Availability:** Ensures that network services are available when needed.
4. **Authentication:** Verifies the identity of users or devices.
5. **Non-repudiation:** Ensures that the sender cannot deny the transmission of a message.
6. **Protection Against Threats:** Safeguards against viruses, worms, hackers, and malicious activities.

Network Attacks:

Network attacks are actions taken to compromise the security of a network by exploiting vulnerabilities.

Types of Network Attacks:

1. **Passive Attacks:**
    - Eavesdropping on network traffic.
    - Example: **Traffic analysis**, **snooping**.
    - Goal: Gather information without altering the data.
2. **Active Attacks:**
    - Modify or disrupt communication.
    - Types:
        - **Masquerade Attack:** Attacker pretends to be a legitimate user.
        - **Replay Attack:** Capturing data and resending it later.
        - **Modification Attack:** Data is altered in transit.
        - **Denial of Service (DoS):** Makes services unavailable to legitimate users.

Q3(b) Explain Different Block Cipher Modes [8 Marks]

Block cipher modes define how encryption is applied to blocks of data. They help provide security for different scenarios in secure communications.

1. Electronic Codebook (ECB)

- Each block is encrypted independently.
- Simple but insecure for large data (identical plaintext = identical ciphertext).

Diagram:

Plaintext → [Encrypt] → Ciphertext

2. Cipher Block Chaining (CBC)

- Each block is XORed with the previous ciphertext block before encryption.
- Requires an Initialization Vector (IV) for the first block.

Advantage: More secure than ECB.

Diagram:

P1 ⊕ IV → Encrypt → C1

P2 ⊕ C1 → Encrypt → C2

...

3. Cipher Feedback (CFB)

- Converts block cipher into a self-synchronizing stream cipher.
- Uses IV and previous ciphertext for encryption.

Diagram:

IV → Encrypt → Output ⊕ P1 → C1

C1 → Encrypt → Output ⊕ P2 → C2

...

4. Output Feedback (OFB)

- Converts block cipher into a synchronous stream cipher.
- IV is repeatedly encrypted to generate keystream.

Advantage: Errors do not propagate.

Diagram:

IV → Encrypt → Output1 ⊕ P1 → C1

Output1 → Encrypt → Output2 ⊕ P2 → C2

...

5. Counter (CTR) Mode

- Encrypts a counter value for each block and XORs with plaintext.
- Highly parallelizable and efficient.

Diagram:

Counter1 → Encrypt → Output1 ⊕ P1 → C1

Counter2 → Encrypt → Output2 ⊕ P2 → C2

...

Let me know if you'd like hand-drawn-style diagrams or simplified summaries!

Here's a comprehensive answer for **Q4(a)** and **Q4(b)**, written in a format suitable for exam purposes:

Q4(a) Explain Distributed Denial of Service (DDoS) Attacks in Detail [8 Marks]

What is a DDoS Attack?

A **Distributed Denial of Service (DDoS)** attack is a **malicious attempt to disrupt** the normal functioning of a **targeted server, service, or network** by **flooding it with a massive amount of traffic** from multiple sources.

Key Features:

- Uses a **network of compromised systems** (called **botnet**) to launch attacks.
- The target is overwhelmed with fake traffic, making it **unavailable to legitimate users**.
- Harder to detect and block because traffic originates from many locations.

How it Works:

1. **Attacker** infects multiple computers or IoT devices with malware.
2. These devices become part of a **botnet** controlled by the attacker.
3. Botnet sends huge amounts of traffic (HTTP requests, pings, etc.) to the target system.
4. Target becomes **slow, crashes**, or becomes **unavailable**.

Types of DDoS Attacks:

1. **Volume-based Attacks:** Overwhelm bandwidth (e.g., UDP floods, ICMP floods).
2. **Protocol Attacks:** Exploit server resources (e.g., SYN floods, Ping of Death).
3. **Application Layer Attacks:** Target specific apps (e.g., HTTP floods).

Example:

- In **2016**, the **Dyn DNS provider** was hit by a major DDoS attack using the **Mirai botnet**, disrupting major sites like Twitter, Netflix, and Reddit.

Impact:

- **Service Downtime**
- **Loss of revenue**

- **Reputation damage**
- **Security breach risk**

Q4(b) Active and Passive Attacks with Examples [8 Marks]

1. Active Attacks

An **active attack** involves **modifying or disrupting** the system or data during transmission. It is **detectable** but causes **harm** to the system.

Types of Active Attacks:

- **Masquerade Attack:** Attacker pretends to be a legitimate user.
- **Replay Attack:** Data is captured and resent to create unauthorized effects.
- **Modification Attack:** Data is altered in transit.
- **Denial of Service (DoS):** Services are made unavailable to users.

Example:

- An attacker intercepts a message "Transfer ₹5000" and changes it to "Transfer ₹50,000".

---

2. Passive Attacks

A **passive attack** involves **eavesdropping or monitoring** transmissions. The goal is to gather information **without detection**.

Types of Passive Attacks:

- **Eavesdropping:** Listening to private communication.
- **Traffic Analysis:** Studying patterns of communication, even if data is encrypted.

Example:

- An attacker listens to login credentials being sent over an unencrypted Wi-Fi connection.

Comparison Table:

Feature	Active Attack	Passive Attack
Detection	Easier to detect	Hard to detect
Damage	Causes harm	No immediate damage
Examples	DoS, Modification	Eavesdropping, Monitoring
Intent	Disrupt/Alter data	Gather confidential info

Let me know if you'd like a diagram or real-world analogy to better understand these concepts!

a) Short Notes

i) Encryption

1. **Definition**: Process of converting plaintext into unreadable ciphertext using an algorithm and a key.
2. **Purpose**: Ensures confidentiality by preventing unauthorized access to sensitive data.
3. **Types of Encryption**:
   - *Symmetric-key*: Same key used for encryption/decryption (e.g. AES, DES).
   - *Asymmetric-key*: Public key encrypts, private key decrypts (e.g. RSA).
4. **Algorithms**:
   - *Block ciphers*: Operate on fixed-size blocks (AES: 128-bit blocks).
   - *Stream ciphers*: Encrypt bit-by-bit or byte-by-byte (RC4).
5. **Modes of Operation** (for block ciphers): ECB, CBC, CFB, OFB, CTR – affecting error propagation and parallelism.
6. **Key Management**: Secure generation, distribution, storage, and rotation of keys are critical.

ii) Decryption

1. **Definition**: Reverse process of encryption that converts ciphertext back to original plaintext using the corresponding key.
2. **Purpose**: Restores data to intelligible form for authorized users or systems.
3. **Symmetric vs. Asymmetric**:

    - *Symmetric*: Uses the same shared secret key.
    - *Asymmetric*: Uses private key corresponding to the public key used for encryption.
4. **Integrity Check**: Often combined with hashing or MAC (Message Authentication Code) to verify ciphertext hasn't been tampered with.
5. **Performance Considerations**: Decryption speed depends on algorithm complexity and key length.
6. **Error Handling**: Corrupted ciphertext may lead to decryption failure or garbled plaintext.

---

b) RSA Algorithm

1. **Overview**
    - Asymmetric cryptosystem named after Rivest, Shamir, and Adleman (1978).
    - Provides confidentiality, authentication, and digital signatures.
2. **Key Generation**

1. **Select two large primes**: pp and qq (hundreds of digits).

2. **Compute modulus**: n=p×qn = p \times q.

3. **Compute totient**: ϕ(n)=(p−1)(q−1)\phi(n) = (p-1)(q-1).

4. **Choose public exponent**: ee, such that 1<e<ϕ(n)1 < e < \phi(n) and gcd(e,ϕ(n))=1\gcd(e, \phi(n)) = 1 (commonly 65537).

5. **Compute private exponent**: d≡e−1mod ϕ(n) d \equiv e^{-1} \mod \phi(n).

6. **Keys**:
    - *Public key*: (e,n)(e, n)
    - *Private key*: (d,n)(d, n)

3. **Encryption**
    - *Plaintext* mm must satisfy 0≤m<n0 \le m < n.
    - Compute ciphertext:

c=memodn c = m^e \bmod n

4. **Decryption**

- Use private key:

m=cd mod n m = c^d \bmod n

- Recovers original mm.

5. **Digital Signature**
    - *Signing*: s=md mod ns = m^d \bmod n
    - *Verification*: check if se mod n=ms^e \bmod n = m
6. **Security Basis**
    - Hardness of *integer factorization* of nn.
    - If pp and qq cannot be efficiently factored, dd remains secret.
7. **Practical Considerations**
    - **Key Size**: Typically ≥2048 bits for adequate security.
    - **Padding Schemes**:
        - *PKCS#1 v1.5*, *OAEP* (Optimal Asymmetric Encryption Padding) to prevent deterministic encryption and chosen-ciphertext attacks.
    - **Performance**:
        - Slower than symmetric algorithms; often used to encrypt symmetric session keys rather than bulk data.
8. **Applications**
    - Secure web (TLS/SSL) certificate exchange.
    - Email encryption (e.g. PGP/GPG).
    - Digital signatures for code signing, document authenticity.
9. **Summary of Steps**

1. Generate large primes p,qp, q → compute n,ϕ(n)n, \phi(n).
2. Choose ee and compute dd.
3. Publish (e,n)(e, n); keep (d,n)(d, n) secret.
4. Encrypt with ee; decrypt with dd.
5. Use padding for security; reserve RSA for small messages/session keys.

Answer structured in concise points for clarity and exam preparation.

Here is a well-structured answer for **Q6(a)** and **Q6(b)**, suitable for academic exams:

Q6(a) What is Digital Signature? What are the Applications of Digital Signature? [9 Marks]

Definition:

A **digital signature** is a **mathematical technique** used to **validate the authenticity and integrity** of a message, software, or digital document. It is the **digital equivalent of a handwritten signature or a stamped seal**, but it is much more secure.

How it Works:

1. The sender **creates a message hash** (a fixed-size output).
2. The hash is **encrypted using the sender's private key**.
3. This encrypted hash is the **digital signature**.
4. The receiver **decrypts the signature** using the sender's **public key** and compares the hash to ensure the message was not altered.

Applications of Digital Signatures:

1. **Authentication:**
   - Ensures the message is from the genuine sender.
   - Used in secure emails and electronic transactions.
2. **Integrity:**
   - Confirms that the data has not been tampered with during transmission.
3. **Non-Repudiation:**
   - The sender cannot deny having sent the message.
   - Used in legal and financial documents.
4. **Secure Software Distribution:**
   - Validates that the software hasn't been modified since release.
5. **E-Governance:**
   - Used in online filing of forms, e-tendering, and digital identity verification.
6. **E-Commerce:**

    - Secures online payment and transactions.

Q6(b) Explain the Following Terms: [9 Marks]

---

i) Cryptography:

Cryptography is the science of **securing information** by transforming it into an unreadable format using mathematical techniques.

- It protects data **confidentiality, integrity, and authenticity**.
- Involves **encryption (scrambling)** and **decryption (unscrambling)** of messages.

Example: Converting “HELLO” into “URYYB” using a Caesar cipher.

---

ii) Symmetric Key Cryptography:

In **symmetric key cryptography**, the **same key** is used for both **encryption and decryption**.

- **Fast** and suitable for encrypting large amounts of data.
- Key must be **securely shared** between sender and receiver.

Example Algorithms:

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)

Example Use Case:

- Secure data storage, VPNs.

---

iii) Asymmetric Key Cryptography:

In **asymmetric key cryptography**, **two different keys** are used:

- A **public key** (used for encryption)
- A **private key** (used for decryption)
- More secure but **slower** than symmetric key systems.
- Public key can be shared openly, but private key is kept secret.

Example Algorithms:

- RSA (Rivest-Shamir-Adleman)
- ECC (Elliptic Curve Cryptography)

Example Use Case:

- Digital signatures, secure email, HTTPS/SSL.

Let me know if you'd like visual diagrams or quick revision points for these topics!

Q7) a) Write short notes on [9]

---

i) Malware

1. **Definition**:
    - Malware stands for *Malicious Software* – programs designed to harm, exploit, or disable computers, systems, or networks.
2. **Types**:
    - **Virus** – Attaches to files and spreads.
    - **Worm** – Self-replicates over networks.
    - **Trojan Horse** – Disguised as legitimate software.
    - **Spyware** – Steals sensitive information.
    - **Ransomware** – Encrypts data and demands payment.
3. **Effects**:
    - Data theft, corruption, system slowdowns, unauthorized access.
4. **Delivery Methods**:
    - Email attachments, malicious websites, software downloads, USB drives.
5. **Prevention**:
    - Use antivirus software, keep systems updated, avoid unknown links/files.

---

ii) Phishing

1. **Definition**:

- A cyberattack method that tricks users into revealing sensitive information like passwords or credit card numbers by pretending to be a trustworthy source.

2. **Common Techniques**:
   - Fake emails or websites resembling legitimate ones.
   - Urgent messages asking to "verify" or "reset" credentials.
3. **Types of Phishing**:
   - **Spear Phishing** – Targeted at specific individuals or organizations.
   - **Whaling** – Targeting high-profile users (executives).
   - **Smishing** – Phishing via SMS.
   - **Vishing** – Voice phishing via phone calls.
4. **Prevention**:
   - Verify sender addresses, don't click unknown links, use two-factor authentication (2FA).
5. **Goal**:
   - Credential theft, financial fraud, identity theft.

---

iii) MITM Attack (Man-in-the-Middle Attack)

1. **Definition**:
   - A type of cyberattack where the attacker secretly intercepts and possibly alters communication between two parties.
2. **How It Works**:
   - Attacker positions themselves between the victim and the server (e.g., during Wi-Fi communication) to eavesdrop or modify data.
3. **Techniques**:
   - Packet sniffing
   - Session hijacking
   - DNS spoofing
   - HTTPS stripping

4. **Consequences**:
    - Data theft, credential hijacking, financial fraud, injection of malicious code.
5. **Prevention**:
    - Use encrypted protocols (HTTPS, SSL/TLS), VPNs, secure Wi-Fi, strong authentication mechanisms.
6. **Example**:
    - Attacker intercepts online banking login credentials during a user's session.

Each topic is covered with definition, techniques, impact, and prevention to match a 9-mark question format.

Here’s a complete and exam-oriented answer for both options **Q7(b)** and **Q8)**. You can choose based on your preference or as required in your exam.

Q7(b) Cyber Security Policies and Challenges in Internet Governance [8 Marks]

Cyber Security Policies:

Cyber security policies are **guidelines and rules** created to protect systems, networks, and data from cyber threats.

Types of Cyber Security Policies:

1. **Acceptable Use Policy (AUP):**
    - Defines what users can and cannot do with company systems and internet.
    - Example: No downloading unauthorized software.
2. **Access Control Policy:**
    - Specifies who can access what data and systems.
    - Ensures users only access necessary resources.
3. **Data Protection Policy:**
    - Ensures sensitive data is encrypted and securely stored or transmitted.
4. **Incident Response Policy:**

- Procedures for responding to cyber incidents like hacking or data breaches.

5. **Network Security Policy:**
   - Rules for securing network traffic with firewalls, intrusion detection, VPNs.
6. **Email and Communication Policy:**
   - Guidelines for safe use of emails and social media to prevent phishing and spam.
7. **Remote Access Policy:**
   - Rules for employees connecting to internal systems from remote locations.

Challenges in Internet Governance:

Internet governance deals with the **development and application of shared principles and policies** for the internet.

Challenges:

1. **Lack of Global Regulation:**
   - Different countries have different laws, causing conflicts in cross-border cyber crimes.
2. **Privacy vs. Surveillance:**
   - Balancing individual privacy rights and government surveillance is complex.
3. **Cybersecurity Threats:**
   - Rising threats from hackers, cyber terrorists, and nation-state attacks.
4. **Freedom of Speech:**
   - Defining boundaries between free expression and hate speech or misinformation.
5. **Digital Divide:**
   - Ensuring fair access to internet resources for developing regions.
6. **Intellectual Property and Copyright Issues:**

  - Regulating content sharing without violating creators' rights.

OR

Q8(a) Explain Cyber Stalking, How to Identify and Detect It [4 Marks]

What is Cyber Stalking?

Cyber stalking is the **use of the internet, email, social media, or other digital tools to harass or threaten someone repeatedly**.

Characteristics:

- Sending threatening emails or messages.
- Spreading false information or rumors online.
- Monitoring someone's online activity or hacking into their accounts.
- Using GPS or spyware to track location.

How to Identify and Detect Cyber Stalking:

1. **Repeated Unwanted Contact:**
   - Receiving frequent messages even after asking the person to stop.
2. **Monitoring Your Online Presence:**
   - The stalker frequently reacts or comments immediately on all your posts.
3. **Threats or Blackmail:**
   - Receiving online threats, blackmail attempts, or harmful messages.
4. **Impersonation:**
   - Fake accounts made in your name to damage reputation or harass others.
5. **Digital Tracking:**
   - Suspicious apps, tracking links, or malware on your device.

Q8(b) Types of Cyber Crimes [4 Marks]

Cyber crimes are **criminal activities carried out using computers or the internet**.

Common Types:

1. **Hacking:**
    - Unauthorized access to computer systems or networks.
2. **Phishing:**
    - Fake emails or websites tricking users to reveal sensitive information.
3. **Identity Theft:**
    - Stealing someone’s personal information (like Aadhar number, credit card) for fraud.
4. **Cyber Bullying:**
    - Harassing or threatening someone through online platforms.
5. **Online Fraud and Scams:**
    - Financial frauds like lottery scams, fake shopping websites, etc.
6. **Cyber Terrorism:**
    - Attacks on critical systems (power grid, transport) to spread terror.
7. **Child Pornography and Exploitation:**
    - Creating or sharing illegal content involving minors.

Let me know if you want these notes in a summarized, printable format or in PDF!