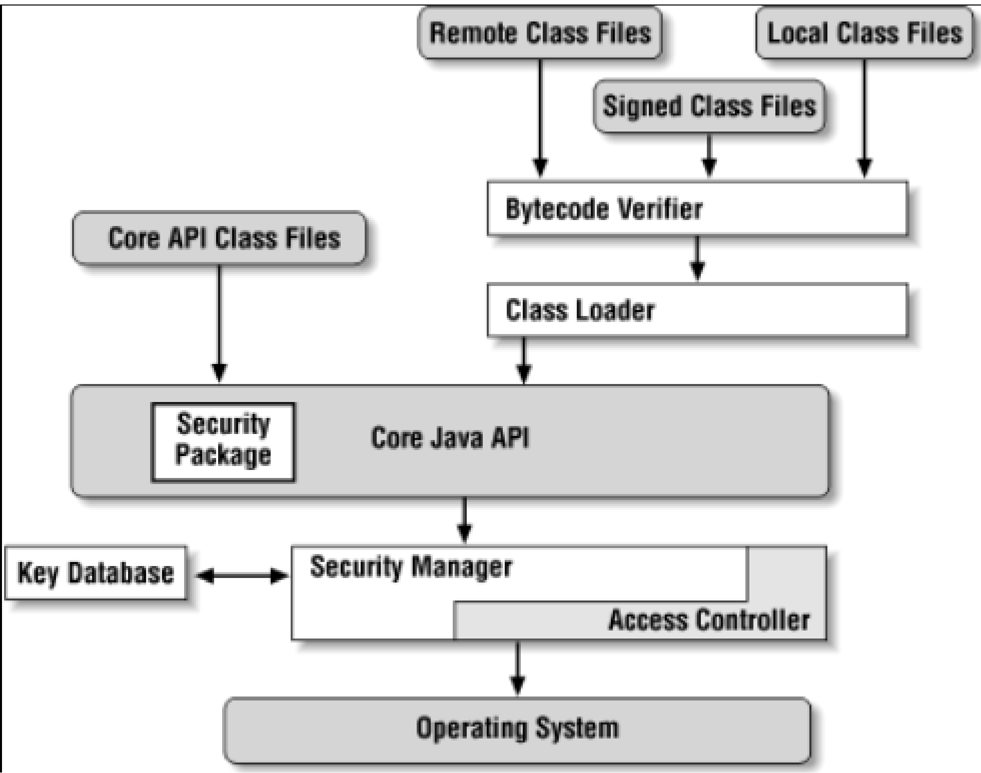
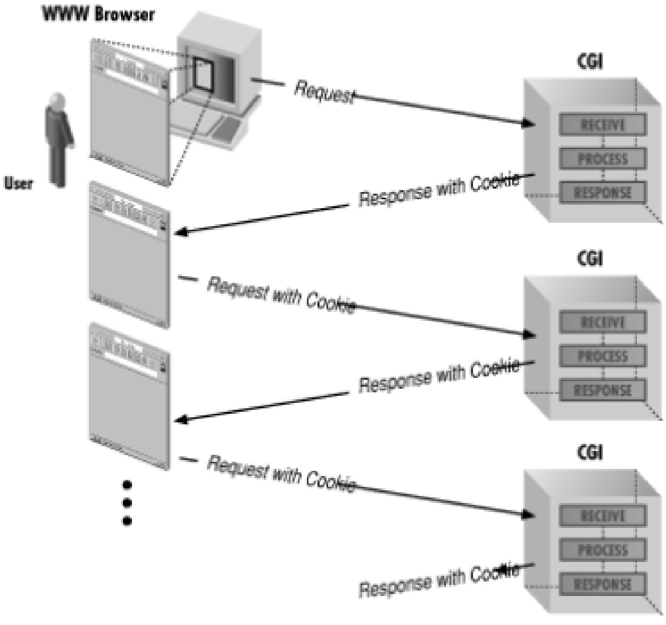
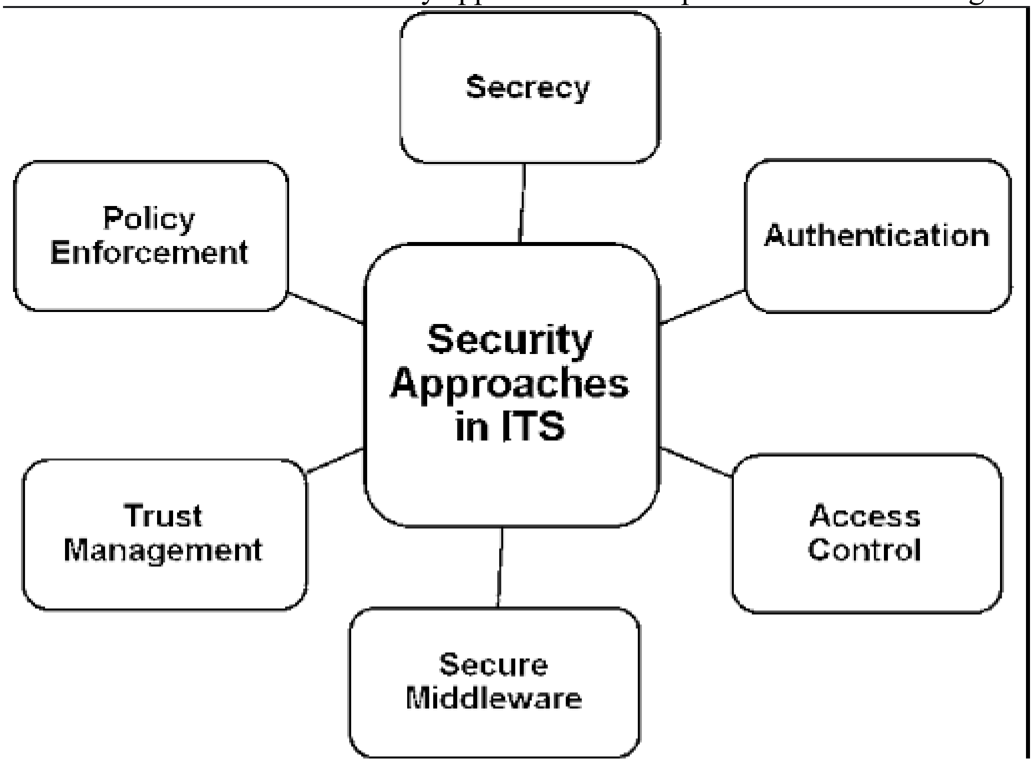
USN

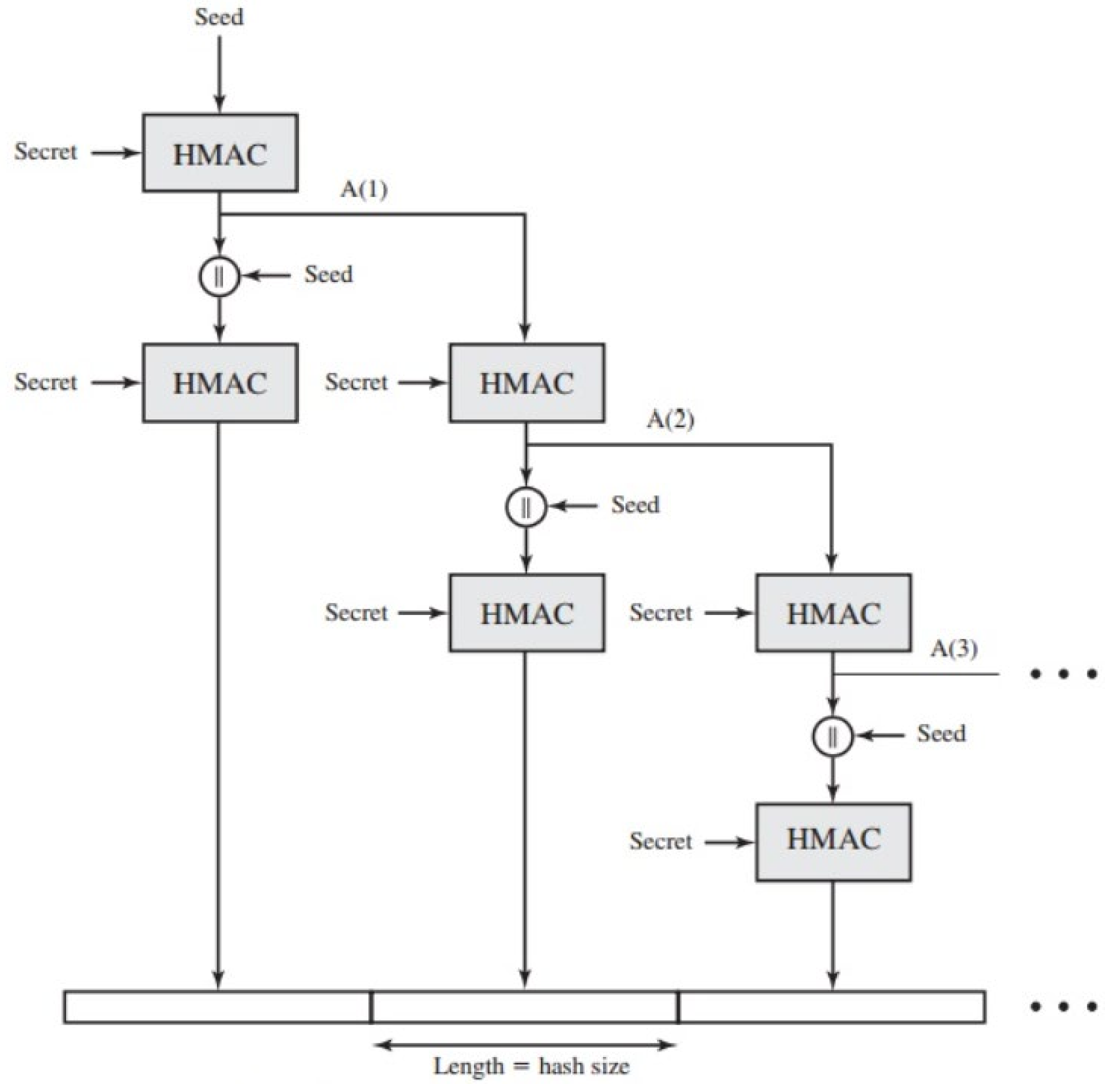
VTU QP Solution – Dec 2023-Jan 2024

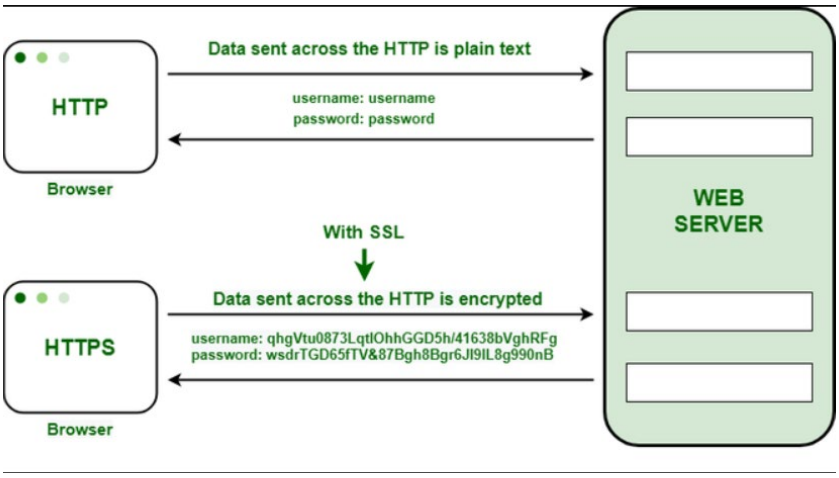
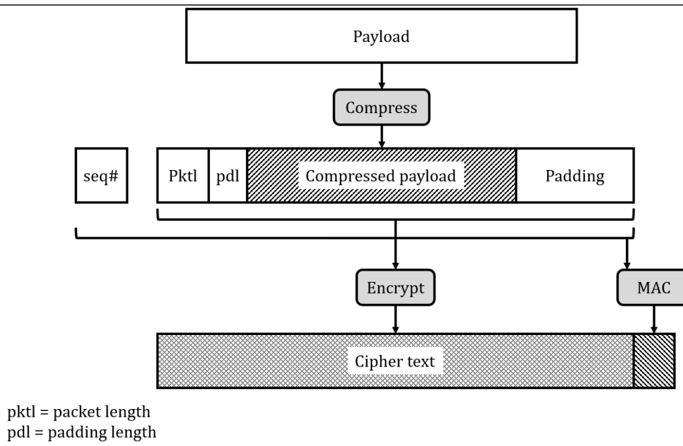
Sub:	Network Security	Sub Code:	**18EC821**	Branch:	ECE

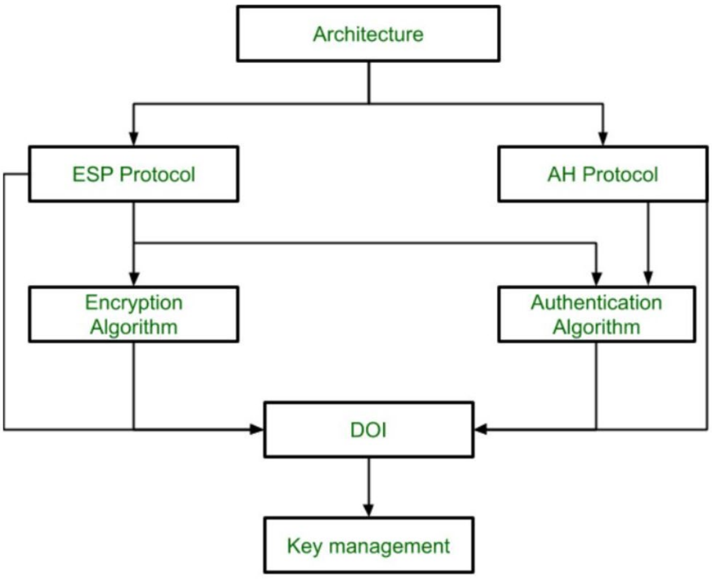
	Answer any FIVE FULL Questions	MARKS	CO	RBT
1a	Explain all the principles of security with suitable diagrams. Confidentiality: Ensures information is accessible only to authorized users. Encryption transforms data into an unreadable format, and access control restricts data access based on user roles. Integrity: Ensures data remains accurate and unaltered. Hashing creates a unique hash for data, detecting any changes, while checksums verify data integrity during transmission. Availability: Ensures systems and data are accessible to authorized users. Redundancy and failover systems maintain access even during failures. Authentication: Verifies user identities using passwords or multi-factor authentication (MFA). Authorization: Determines user permissions using access control lists (ACLs) or role-based access control (RBAC). Non-Repudiation: Ensures actions cannot be denied. Digital signatures and audit trails provide proof of actions.	10	CO2	L2
b	 Remote Class Files Local Class Files Signed Class Files Bytecode Verifier Core API Class Files Class Loader Security Package Core Java API Key Database Security Manager Access Controller Operating System The Java Sandbox is a security mechanism designed to provide a controlled environment for executing Java programs, particularly applets, to protect the host system from potentially malicious code. It enforces security restrictions and ensures that Java programs do not perform unauthorized operations.	10	CO2	L2
2a	Explain passive and active attacks with suitable diagrams. Passive Attacks:	07	Co2	L1

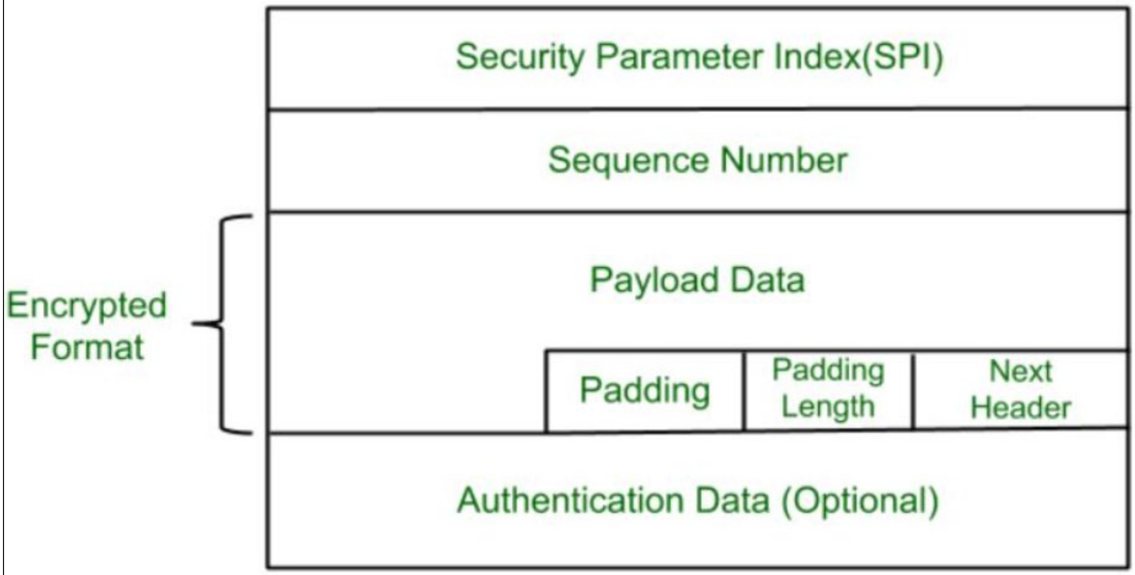
	Definition: Involve eavesdropping or monitoring data without altering or disrupting communication. Characteristics: The attacker intercepts data covertly without modifying it. Examples: Eavesdropping: Capturing sensitive data like passwords or personal information. Traffic Analysis: Analyzing communication patterns to infer sensitive details. Active Attacks: Definition: Involve altering or disrupting communication and data. Characteristics: The attacker modifies or interferes with data or communications. Examples: Man-in-the-Middle: Intercepting and altering messages between users. Denial of Service (DoS): Overloading a system to disrupt its availability.			
b	List out two types of specific attacks and explain in detail. 1. Man-in-the-Middle (MitM) Attack A Man-in-the-Middle attack occurs when an attacker intercepts and potentially alters communication between two parties without their knowledge. The attacker effectively sits between the sender and the receiver, allowing them to eavesdrop or manipulate the communication. 2. Denial of Service (DoS) Attack A Denial of Service attack aims to disrupt the availability of a service or network by overwhelming it with excessive requests or exploiting vulnerabilities to make it unavailable to legitimate users.	07	Co2	L1
c	What is cookie? Explain its creation and usage of cookies with relevant diagrams.  WWW Browser User Request CGI RECEIVE PROCESS RESPONSE Response with Cookie Request with Cookie 1. HTTPS (Hypertext Transfer Protocol Secure) Description: HTTPS encrypts data between the web browser and server using SSL/TLS protocols, ensuring confidentiality and integrity. 2. Web Application Firewalls (WAFs) Description: WAFs filter and monitor HTTP requests to protect web applications from common attacks like SQL injection and cross-site scripting (XSS). 3. Secure Sockets Layer (SSL) and Transport Layer Security (TLS)	06	Co2	L1

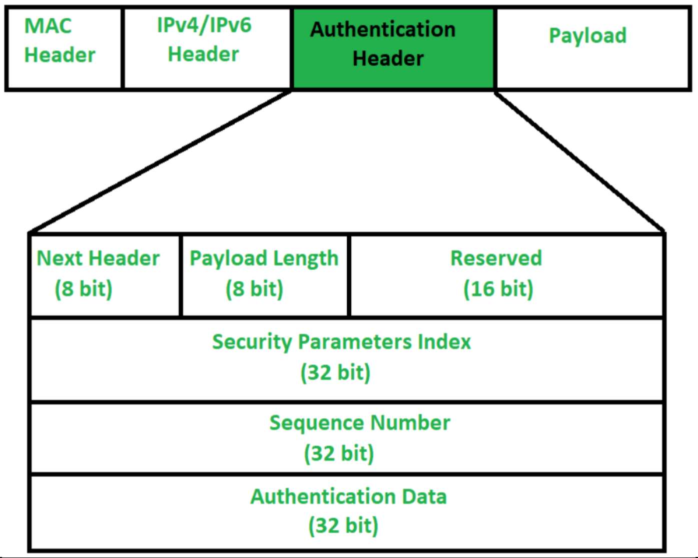
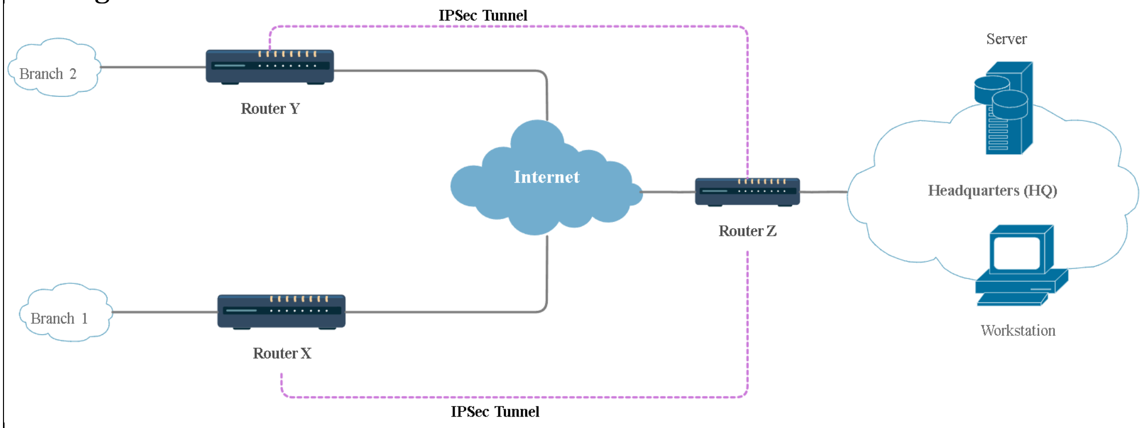
	Description: SSL/TLS protocols encrypt data transmitted over the internet, ensuring secure communication channels.			
3a	List the various web traffic security approaches and explain with relevant diagrams.  Security Approaches in ITS Secrecy Authentication Access Control Secure Middleware Trust Management Policy Enforcement SSL/TLS Encryption: Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), encrypt the data exchanged between the client and server, ensuring confidentiality and integrity. Web Application Firewalls (WAFs): WAFs filter and monitor HTTP traffic to protect web applications from threats like SQL injection and cross-site scripting (XSS). Content Security Policy (CSP): CSP helps prevent cross-site scripting attacks by specifying which dynamic resources are allowed to load. DDoS Protection: Distributed Denial of Service (DDoS) protection mitigates traffic floods aimed at overwhelming and disrupting services. Multi-Factor Authentication (MFA): MFA enhances security by requiring multiple forms of verification before granting access.	10	Co2	L2
b	With suitable diagrams, explain the working of handshake protocol action. The handshake protocol is a crucial part of establishing a secure connection between a client and server using SSL/TLS. Here’s how it works: Client Hello: The client sends a "Client Hello" message to the server, which includes supported SSL/TLS versions, cipher suites, and a random number. Server Hello: The server responds with a "Server Hello" message, including the chosen protocol version, cipher suite, and its own random number.	10	Co2	L2

	Server Certificate: The server sends its digital certificate to the client for authentication. Key Exchange: The server and client exchange key information needed to establish a shared secret. Finished Messages: Both parties send "Finished" messages to confirm that the handshake is complete and the secure connection is established.			
4a	What is transport layer security? Explain calculation of Message Authentication Code (MAC) and Generation of Pseudorandom function with suitable diagram.  Seed Secret HMAC A(1) Seed Secret HMAC Secret HMAC A(2) Seed Secret HMAC Secret HMAC A(3) Seed Secret HMAC Length = hash size Transport Layer Security (TLS) ensures secure communication over a network by encrypting data and providing authentication. Message Authentication Code (MAC) Calculation: Purpose: Verifies data integrity and authenticity. Process: A MAC is generated using a cryptographic hash function combined with a secret key. For a given message M, the MAC is computed as MAC = HMAC(key, M), where HMAC is a keyed hash function like SHA-256. Pseudorandom Function (PRF) Generation: Purpose: Generates secure random values for encryption and keys.	10	Co2	L1

	Process: A PRF takes a secret key and input data to produce a pseudorandom output. For TLS, a PRF combines a key with a message to produce a random-looking output used in key derivation.			
b	Explain the working of HTTPS with related connection initiation and connection closure.  Data sent across the HTTP is plain text username: username password: password HTTP Browser With SSL Data sent across the HTTP is encrypted username: qhgVtu0873LqtlOhhGGD5h/41638bVghRFg password: wsdrTGD65fTV&87Bgh8Bgr6JI9IL8g990nB HTTPS Browser WEB SERVER HTTPS (Hypertext Transfer Protocol Secure) ensures secure communication over the web using SSL/TLS encryption. Connection Initiation: Client Hello: The client initiates a connection by sending a "Client Hello" message to the server, specifying supported encryption algorithms and TLS versions. Server Hello: The server responds with a "Server Hello," selecting encryption parameters and providing its digital certificate for authentication. Key Exchange: The client and server exchange key information to establish a shared secret for encrypting data. Finished Messages: Both parties send "Finished" messages to confirm the successful establishment of a secure session. Connection Closure: Client/Server Closure: Either the client or server can initiate the closure by sending a "close_notify" alert. Session Termination: Both sides acknowledge the closure and terminate the secure session.	05	Co2	L1
c	 Payload Compress seq# Pktl pdl Compressed payload Padding Encrypt MAC Cipher text pktl = packet length pdl = padding length The SSH (Secure Shell) transport layer protocol ensures secure communication over a network by encrypting data and authenticating users.	05	Co2	L1

	Packet Header: Contains metadata, such as packet length and type. The header is crucial for identifying and managing the packet. Payload: The main part of the packet, which includes the encrypted data or command being sent. This part carries the actual information intended for transmission. Padding: Added to ensure the payload fits the encryption block size requirements. It helps in maintaining data integrity and security. MAC (Message Authentication Code): Ensures data integrity and authenticity by providing a checksum that verifies the packet has not been tampered with. Encrypted Data: The payload, padding, and MAC are encrypted using a symmetric encryption algorithm to protect the data during transmission.			
5a	Explain IP Security overview with suitable diagram and list its applications.  Architecture ESP Protocol AH Protocol Encryption Algorithm Authentication Algorithm DOI Key management IP Security (IPsec) is a suite of protocols designed to secure IP communications by authenticating and encrypting each IP packet in a data stream. Overview: IPsec Modes: Transport Mode: Encrypts only the payload of the IP packet, not the header. Used for end-to-end communication. Tunnel Mode: Encrypts the entire IP packet and adds a new header. Used for network-to-network or gateway-to-gateway communication. Components: Authentication Header (AH): Provides data integrity and authentication. Encapsulating Security Payload (ESP): Provides encryption, data integrity, and optional authentication. Applications: Virtual Private Networks (VPNs): Secures remote access to a network. Secure Site-to-Site Communication: Connects remote networks securely. Network Security: Protects data transmitted across insecure networks.	07	Co2	L1
b	Explain IPSec documents with suitable diagram and write a short note associations. IPsec Documents: Security Association (SA): Purpose: Defines the parameters for IPsec communication, including encryption and authentication methods.	08	Co2	L1

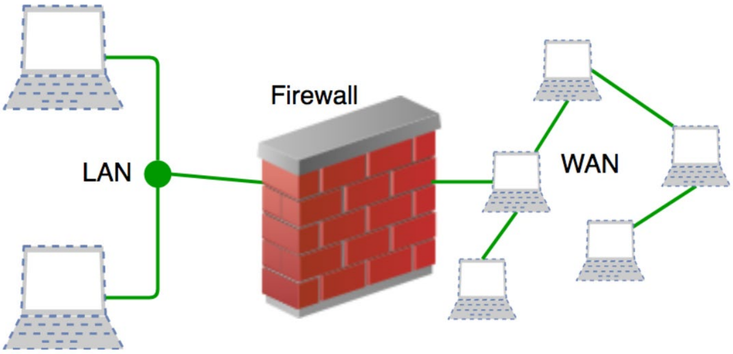
	Security Parameter Index (SPI): Purpose: A unique identifier used within the SA to distinguish between different SAs. IPsec Policies: Purpose: Specifies the rules for applying IPsec to network traffic, including which traffic to secure and the security mechanisms to use. Associations: IPsec uses Security Associations to establish secure communication channels. Policies define the application of IPsec, ensuring traffic is protected according to predefined rules. SPI helps in identifying and managing these associations during data transmission.  Security Parameter Index(SPI) Sequence Number Encrypted Format Payload Data Padding Padding Length Next Header Authentication Data (Optional)			
c	Explain how authentication header guards against the replay attack. The Authentication Header (AH) in IPsec is designed to provide data integrity, authentication, and protection against replay attacks. Replay Attack: Definition: An attacker captures and retransmits valid data packets to deceive the receiver, often to gain unauthorized access or disrupt services. AH Mechanism: Sequence Number: AH includes a sequence number field in its header. Each packet sent has a unique, incrementing sequence number. Receiver Check: Upon receiving a packet, the receiver checks the sequence number against a record of previously received numbers. Detection: If the sequence number is repeated or outside the expected range, the packet is identified as a replay and discarded. By using sequence numbers and maintaining a record of received packets, AH ensures that any attempt to replay captured packets is detected and prevented, thereby maintaining the integrity and security of the communication.	05	Co2	L1

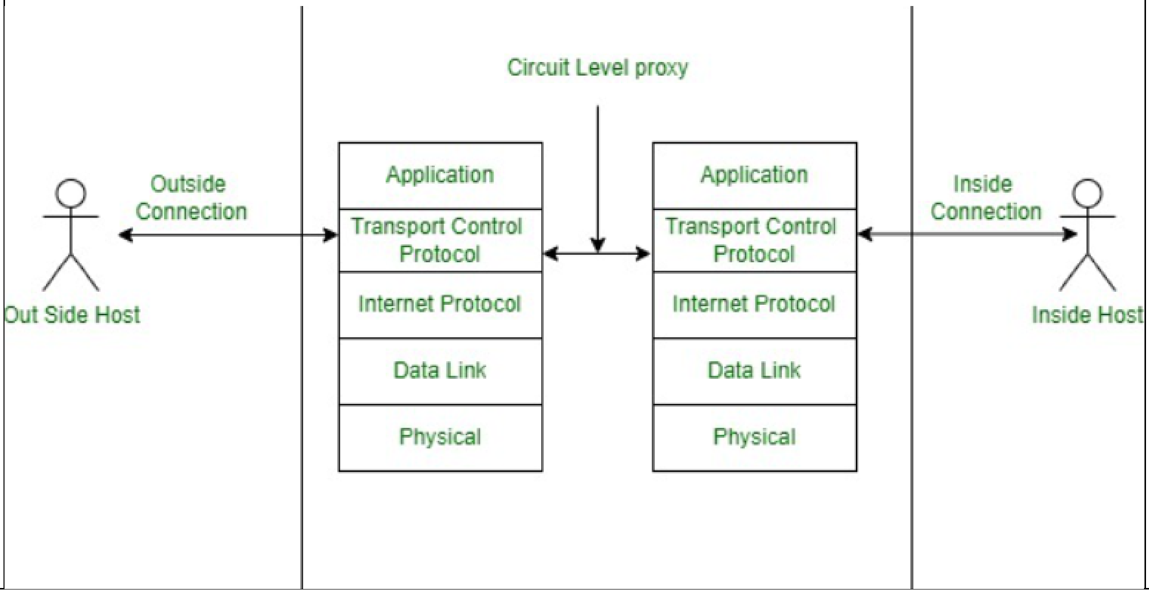
	 MAC Header IPv4/IPv6 Header Authentication Header Payload Next Header (8 bit) Payload Length (8 bit) Reserved (16 bit) Security Parameters Index (32 bit) Sequence Number (32 bit) Authentication Data (32 bit)			
6a	Explain the two ways in which IPSec authentication service can be used with related diagrams. IPsec's authentication service can be used in two primary ways: Transport Mode: Usage: Secures end-to-end communication between two hosts. Diagram: Functionality: Authenticates only the IP payload, not the entire IP packet, ensuring data integrity and authenticity while leaving the original IP header intact. Tunnel Mode: Usage: Secures communication between networks or gateways. Diagram: Functionality: Authenticates and encrypts the entire original IP packet, which is then encapsulated within a new IP packet, providing protection for both the payload and the original header.  IPSec Tunnel Branch 2 Router Y Server Internet Headquarters (HQ) Router Z Branch 1 Workstation Router X IPSec Tunnel	08	Co2	L1
b	Explain the various fields of ESP format with suitable diagrams. Encapsulating Security Payload (ESP) is a key protocol in IPsec that provides confidentiality, data integrity, and authentication. 1. Security Parameter Index (SPI): - Purpose: Identifies the security association (SA) that governs the packet. - Diagram: [SPI Field](https://example.com/esp_spi_diagram.png)	07	Co2	L1

	2. Sequence Number: - Purpose: A unique number to protect against replay attacks by ensuring each packet has a distinct sequence. - Diagram: [Sequence Number Field](https://example.com/esp_sequence_diagram.png) 3. Payload Data: - Purpose: Contains the encrypted data, which is the core of the packet. - Diagram: [Payload Data Field](https://example.com/esp_payload_diagram.png) 4. Padding: - Purpose: Ensures the payload aligns with the encryption algorithm's block size requirements. - Diagram: [Padding Field](https://example.com/esp_padding_diagram.png) 5. Pad Length: - Purpose: Indicates the size of the padding added. - Diagram: [Pad Length Field](https://example.com/esp_padlength_diagram.png) 6. Next Header: - Purpose: Specifies the type of data in the payload (e.g., TCP, UDP). - Diagram: [Next Header Field](https://example.com/esp_nextheader_diagram.png) 7. Authentication Data: - Purpose: Contains a Message Authentication Code (MAC) for data integrity and authentication. - Diagram: [Authentication Data Field](https://example.com/esp_authentication_diagram.png) These fields work together to provide robust security for IP packets, ensuring confidentiality, integrity, and authenticity during transmission.			
c	Explain the scope of ESP encryption and authentication in transport and tunnel mode with suitable frame format. Encapsulating Security Payload (ESP) in IPsec provides encryption and optional authentication, with its scope varying between Transport Mode and Tunnel Mode. - Transport Mode: ESP encrypts only the IP packet's payload, leaving the original IP header intact. This mode is typically used for end-to-end communication between two hosts. Authentication, if applied, covers the payload and ESP header, ensuring data integrity but does not protect the original IP header. - Tunnel Mode: ESP encrypts the entire original IP packet, including both the header and payload, and encapsulates it within a new IP header. This mode is commonly	05	Co1	L1

	used for communication between networks or gateways, such as in VPNs. Authentication in tunnel mode covers the entire encrypted packet, providing comprehensive protection by concealing the original IP header. Transport mode secures only the payload, while tunnel mode secures the entire IP packet, making it more suitable for secure network-to-network communication.			
7a	List and explain three classes of intruders. Explain various intrusion techniques. Three Classes of Intruders: 1. Masqueraders: Unauthorized users who infiltrate a system by pretending to be legitimate users, often through stolen credentials. 2. Misfeasors: Legitimate users who abuse their access privileges to perform unauthorized actions, such as accessing restricted data. 3. Clandestine Users: Intruders who gain supervisory control of a system to bypass security mechanisms, often leaving no trace of their activities. Intrusion Techniques: - Password Cracking: Using various methods to obtain or guess a user's password. - Phishing: Deceiving users into providing sensitive information. - Exploiting Vulnerabilities: Taking advantage of software flaws to gain unauthorized access.	10	Co2	L1
b	Define intrusion detection with suitable approaches. Explain statistical anomaly detection. Intrusion Detection is the process of monitoring network or system activities for malicious actions or policy violations. It helps identify potential security breaches in real-time. Approaches: 1. Signature-Based Detection: Identifies intrusions by comparing activities to a database of known attack patterns. 2. Anomaly-Based Detection: Detects deviations from normal behavior to identify potential threats. Statistical Anomaly Detection: This method establishes a baseline of normal activity using statistical models. Any significant deviation from this baseline is flagged as a potential intrusion. For example, unusually high network traffic from a single user might indicate an anomaly and trigger an alert.	10	Co2	L1
8a	a. i) Define virus. Explain its life phases. ii) Explain virus structure with suitable example. i) Virus Definition & Life Phases: A virus is a malicious software program designed to replicate itself and spread to other systems by infecting files or programs. Life Phases: 1. Dormant Phase: The virus is inactive and undetected. 2. Propagation Phase: The virus replicates and spreads. 3. Triggering Phase: The virus is activated by a specific event or condition. 4. Execution Phase: The virus performs its intended malicious activity. ii) Virus Structure: A virus typically consists of:	10	Co2	L2

	- Infection Mechanism: How it spreads (e.g., attaching to files). - Trigger: Condition for activation (e.g., specific date). - Payload: Malicious action (e.g., data corruption). Example: The ILOVEYOU virus spreads via email attachments, triggers when opened, and overwrites files.			
b	b. Write short notes on: (i) Digital immune system (ii) Antivirus approaches i) Digital Immune System: The Digital Immune System is a framework designed to automatically detect, analyze, and respond to malware threats. It involves coordinated efforts between user systems and centralized servers, where suspicious files are sent for analysis. If a virus is detected, a remedy is created and distributed to all affected systems, providing rapid and comprehensive protection. ii) Antivirus Approaches: Antivirus software employs various methods to combat malware: - Signature-Based Detection: Identifies known malware by matching code patterns. - Heuristic Analysis: Detects unknown threats by analyzing code behavior. - Behavioral Analysis: Monitors system behavior to identify suspicious activities. - Sandboxing: Isolates and executes suspicious files in a controlled environment to observe behavior.	10	Co2	L2
9a	List various types of firewalls. Explain the packet filtering router in detail. Types of Firewalls: 1. Packet Filtering Firewall: Filters traffic based on predefined rules at the network layer. 2. Stateful Inspection Firewall: Monitors the state of active connections and makes decisions based on the context of traffic. 3. Proxy Firewall: Intermediates requests between the user and the server, filtering content at the application layer. 4. Next-Generation Firewall (NGFW): Combines traditional firewall functions with additional features like intrusion prevention and deep packet inspection. Packet Filtering Router: A Packet Filtering Router examines each packet's header information (e.g., IP addresses, port numbers) and applies a set of rules to decide whether to allow or block the packet. It operates at the network layer, filtering incoming and outgoing traffic based on ACLs (Access Control Lists), ensuring only authorized traffic passes through.	10	Co2	L2
b	Explain various design goals of a fire wall. Also give details about the capabilities and limitations of firewall. Design Goals of a Firewall: 1. Traffic Control: Regulate incoming and outgoing network traffic based on security policies. 2. User Authentication: Ensure that only authorized users access network resources. 3. Data Protection: Prevent unauthorized access to sensitive data.	10	Co2	L2

	4. Logging and Monitoring: Track network activity for security audits and real-time threat detection. Capabilities: - Access Control: Filters traffic based on rules. - Network Segmentation: Isolates network segments for security. - Threat Detection: Identifies and blocks malicious traffic. Limitations: - Cannot Protect Against Insider Attacks: Firewalls focus on external threats. - Limited to Predefined Rules: Cannot stop new or sophisticated attacks. - Doesn't Protect Beyond the Perimeter: Can't secure data once it leaves the network.			
10a	Define firewall configuration. Explain in detail the various configurations with suitable diagrams.  Firewall Configuration involves setting up rules and parameters to control network traffic and enforce security policies. Configurations: 1. Packet Filtering: - Diagram: [Packet Filtering](https://example.com/packet_filtering_diagram.png) - Explanation: Rules based on IP addresses, ports, and protocols to allow or block packets. 2. Stateful Inspection: - Diagram: [Stateful Inspection](https://example.com/stateful_inspection_diagram.png) - Explanation: Tracks active connections and filters packets based on connection state. 3. Proxy Firewall: - Diagram: [Proxy Firewall](https://example.com/proxy_firewall_diagram.png) - Explanation: Acts as an intermediary, filtering requests and responses at the application layer. 4. Next-Generation Firewall (NGFW): - Diagram: [NGFW](https://example.com/ngfw_diagram.png) - Explanation: Combines traditional firewall functions with advanced features like intrusion prevention and deep packet inspection.	10	Co2	L2

b	Explain in detail the circuit level gateway with suitable diagrams. A Circuit-Level Gateway operates at the transport layer (Layer 4) and manages network connections between clients and servers. It establishes and maintains connections based on security policies without inspecting the packet content. Working: 1. Connection Request: Client requests access through the gateway. 2. Validation: Gateway checks if the request meets security rules. 3. Circuit Creation: Gateway sets up a connection, allowing data transfer. 4. Data Transfer: Forwards packets between client and server. 5. Termination: Closes the connection when done. Advantages: Efficient and simple, with low overhead. Limitations: Limited security, as it doesn't inspect packet content.  Circuit Level proxy Outside Connection Out Side Host Application Transport Control Protocol Internet Protocol Data Link Physical Application Transport Control Protocol Internet Protocol Data Link Physical Inside Connection Inside Host	10	Co2	L2