Department of Artificial Intelligence and Data Science

TE-AI&DS- CYBER SECURITY

Unit-3

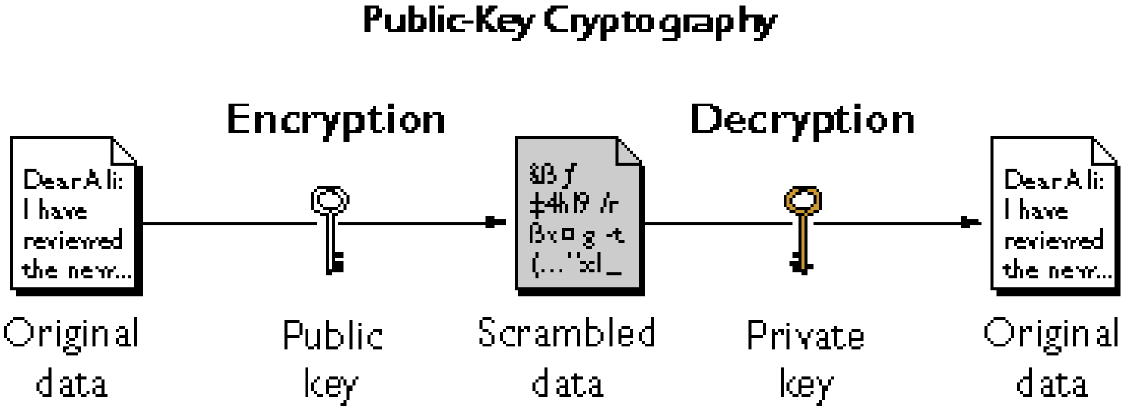
[NOV/DEC-2024]

Q.1)Explain Public Key Cryptography. [6]

[NOV/DEC-2024]

Ans:

Public key cryptography involves a pair of keys known as a public key and a private key (a *public key pair*), which are associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published and the corresponding private key is kept secret. Data that is encrypted with the public key can be decrypted only with the corresponding private key.



Q2) **Perform encryption and decryption using RSA algorithm for p=17, q=31, e=7 and M=2** **[6]**

[NOV/DEC-2024]

Ans: Given - P=17, q=31 and e=7

N = p*q =17*31=527

$\phi(n) = (p-1)(q-1)$
$=(17-1)(31-1) = 480$

$d = (1+k\phi(n))/e = (1+480k)/7$
$= -959/7=-1$ (for k= -2)

$d = -137(\text{mod } 480) = 343$

Encryption (C) = M^{e} (mod n) = 2 (mod 527) = 128

Decryption M = C^{d} (mod n)=128 ^343 (mod 527) =

2

Q3) **Explain the operations of Kerberos.** **[6]**

[NOV/DEC-2024]

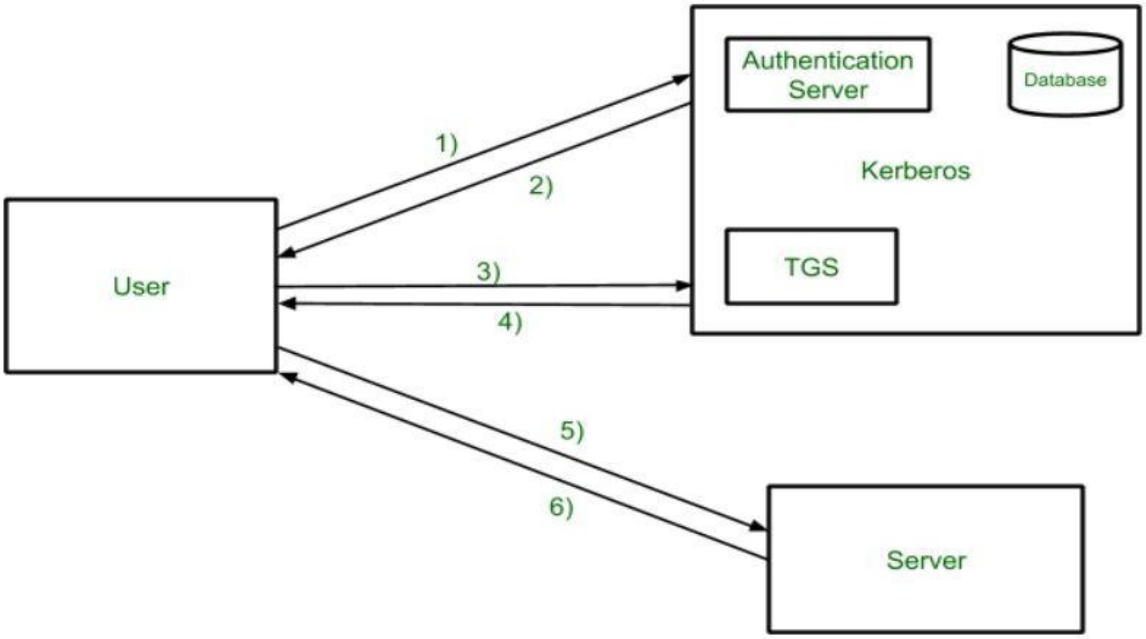
Ans :

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. The main components of Kerberos are:

Authentication Server (AS): The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

Database: The Authentication Server verifies the access rights of users in the database.

Ticket Granting Server (TGS): The Ticket Granting Server issues the ticket for the Server



- **Step-1:** User login and request services on the host. Thus user requests for ticket-granting service.

- **Step-2:** Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using the Password of the user.

- **Step-3:** The decryption of the message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user names and network addresses.

- **Step-4:** Ticket Granting Server decrypts the ticket sent by User and authenticator verifies the request then creates the ticket for requesting services from the Server.

- **Step-5:** The user sends the Ticket and Authenticator to the Server.

- **Step-6:** The server verifies the Ticket and authenticators then generate access to the service. After this User can access the services.

*Q4)*Explain operation of MD5 message digest algorithm [6]

[NOV/DEC-2024]

Ans :

- Digest Length=128 bit
- I/P Text=512 bit
- Sub Block size-32bit
- 512/32=16 total Sub blocks
- No. Of Rounds=4
- Iteration per round=16
- Chaining Variable = 4*32=128
- K[t] constant = Where t=0 to 63
- O/P-> four 32 bit blocks

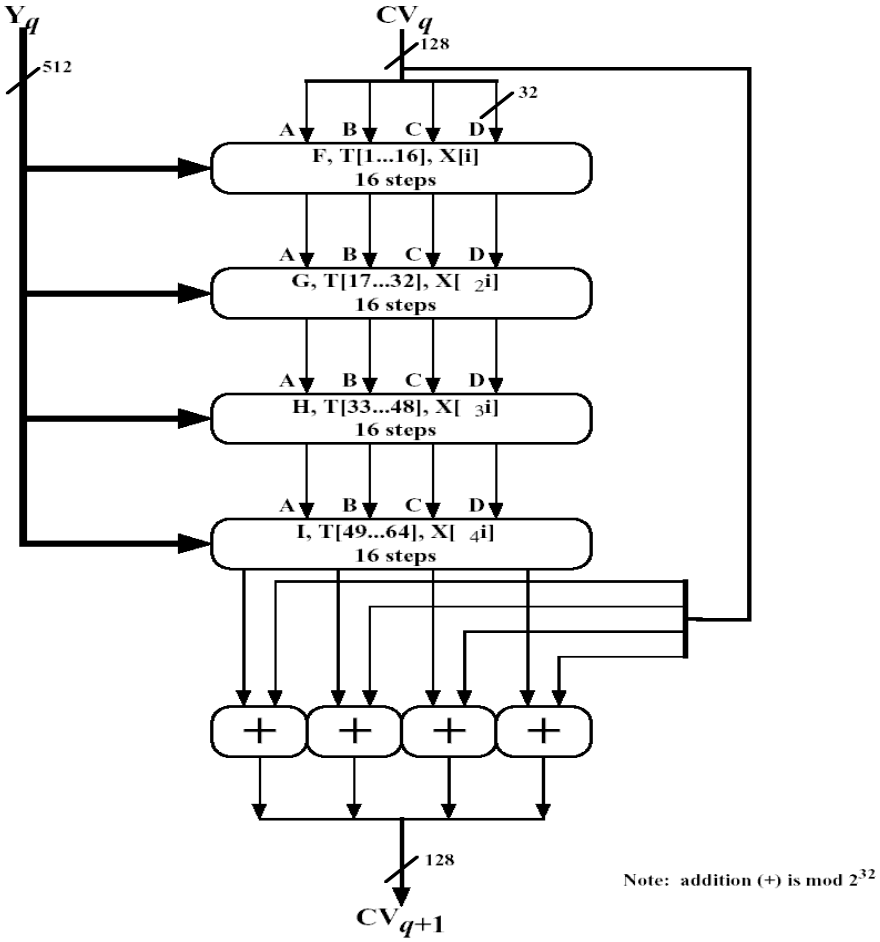


Figure 9.2 MD5 Processing of a Single 512-bit Block (MD5 Compression Function)

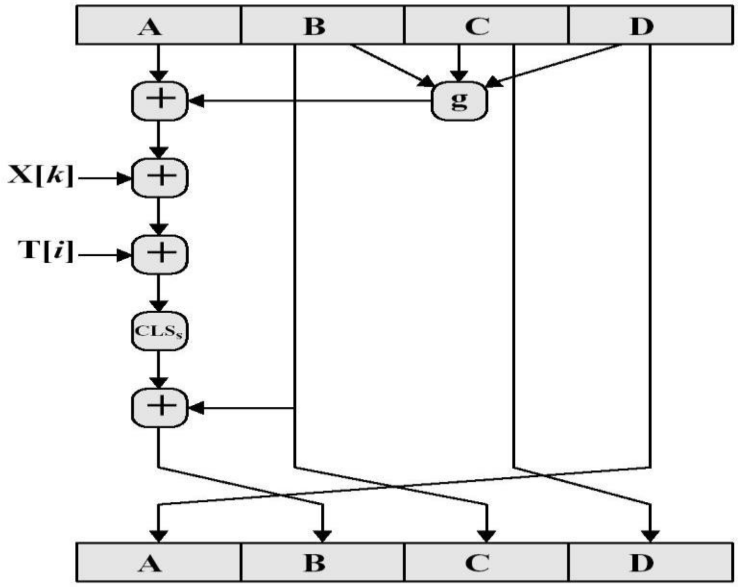


Figure 9.3 Elementary MD5 Operation (single step)

Q5) **User A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root α = 7.**

a. If user A has private key XA = 5, what is A's public key YA?
b. If user B has private key XB=12, what is B's public key YB?
c. What is the shared secret key? [6]

[NOV/DEC-2024]

Ans: a. A's public key YA

YA = α^XA mod q = (7)^5 mod 71

= 16807 mod 71 = 51

b. B's public key YB

YB = α^XB mod q = (7)^12 mod 71

= 13841287201 mod 71 = 4

c. Shared secret key

at user A K=(YB)^XA mod q

= (4)^5 mod 71 = 1024 mod 71

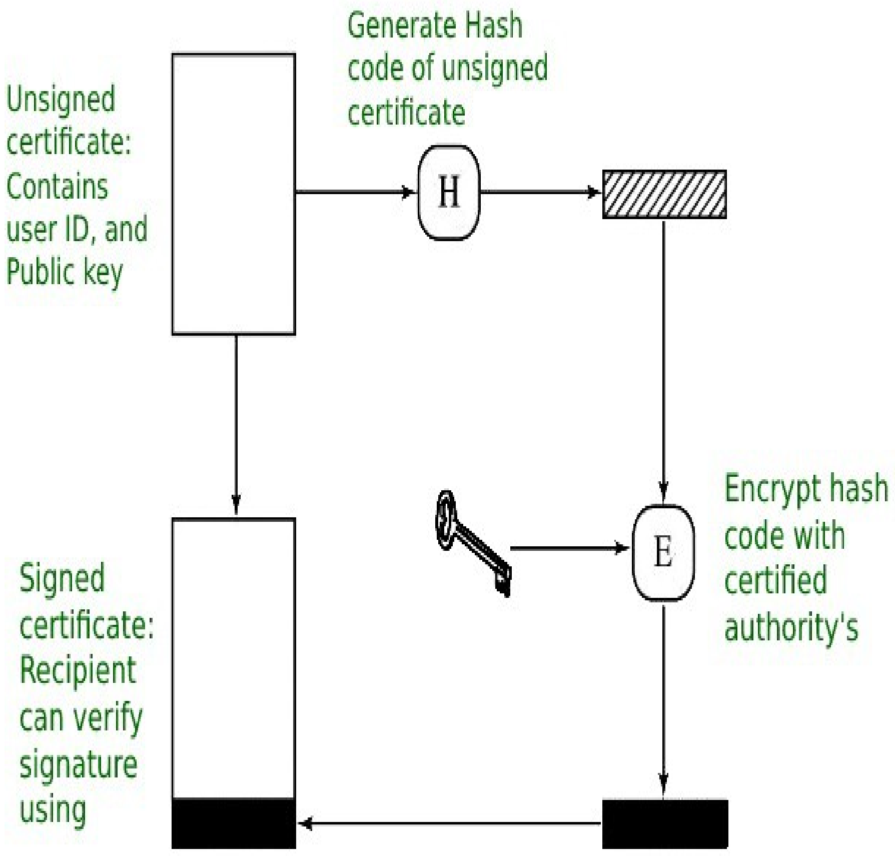
K = 30

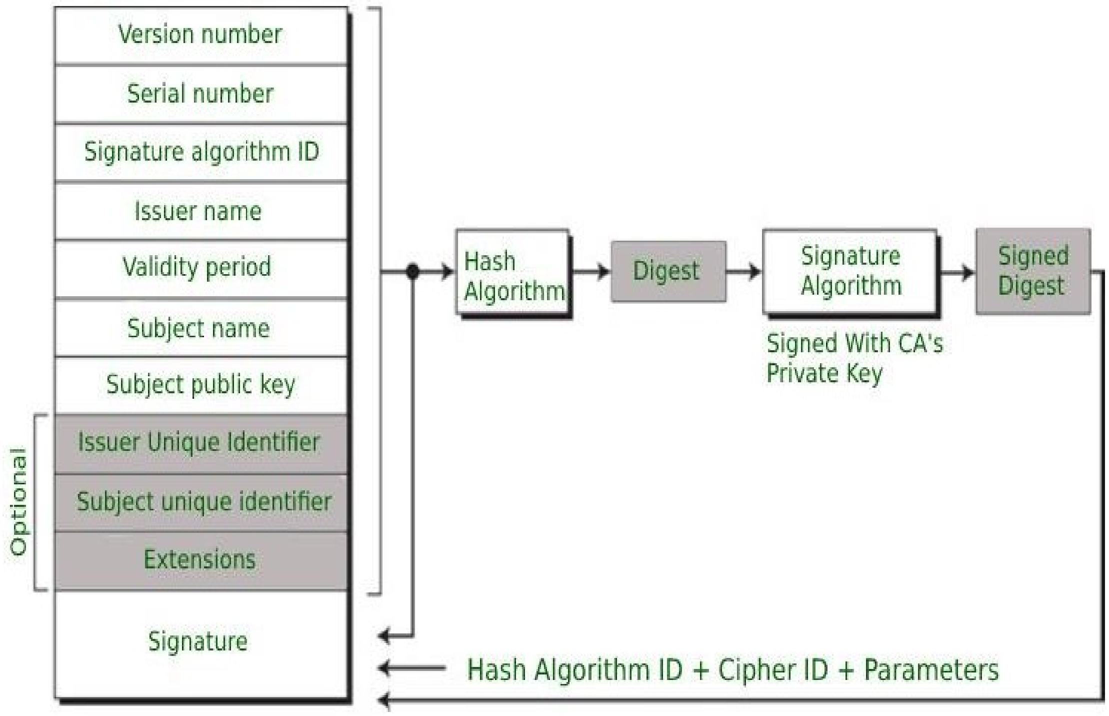
Q6) Explain X.509 Authentication Service [6]

[NOV/DEC-2024]

Ans : X.509 digital certificate is a certificate-based authentication security framework that can be used for providing secure transaction processing and private information. These are primarily used for handling the security and identity in computer networking and internet-based communications.

Working & Format of X.509 Authentication Service:


Generate Hash code of unsigned certificate
Unsigned certificate: Contains user ID, and Public key
H
E
Encrypt hash code with certified authority's
Signed certificate: Recipient can verify signature using


Version number
Serial number
Signature algorithm ID
Issuer name
Validity period
Subject name
Subject public key
Issuer Unique Identifier
Subject unique identifier
Extensions
Optional
Signature
Hash Algorithm
Digest
Signature Algorithm
Signed Digest
Signed With CA's Private Key
Hash Algorithm ID + Cipher ID + Parameters

Unit- 4

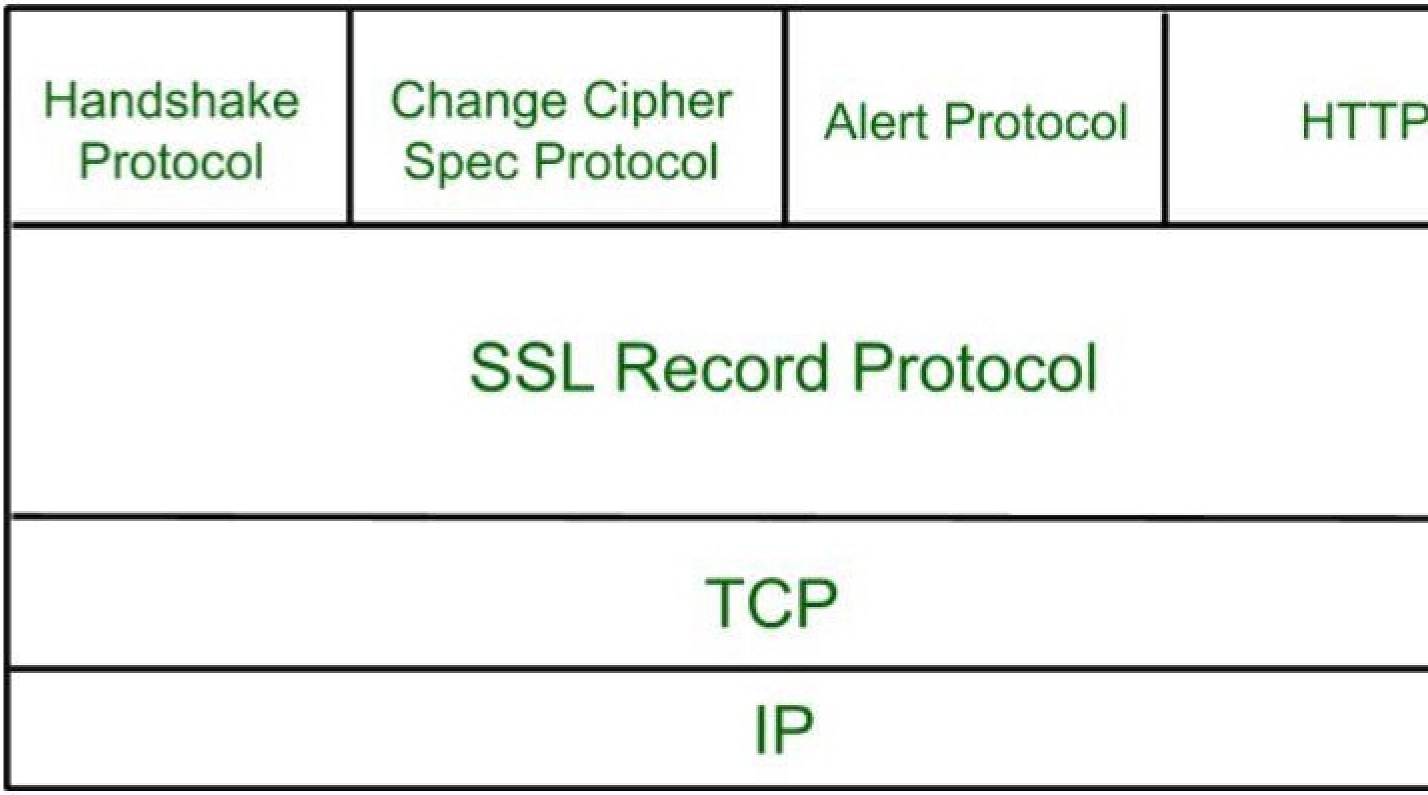
1) Explore Secure Socket Layer Handshake protocol in detail. **[6]**

Ans- **Secure Socket Layer (SSL)** provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL Protocol Stack:

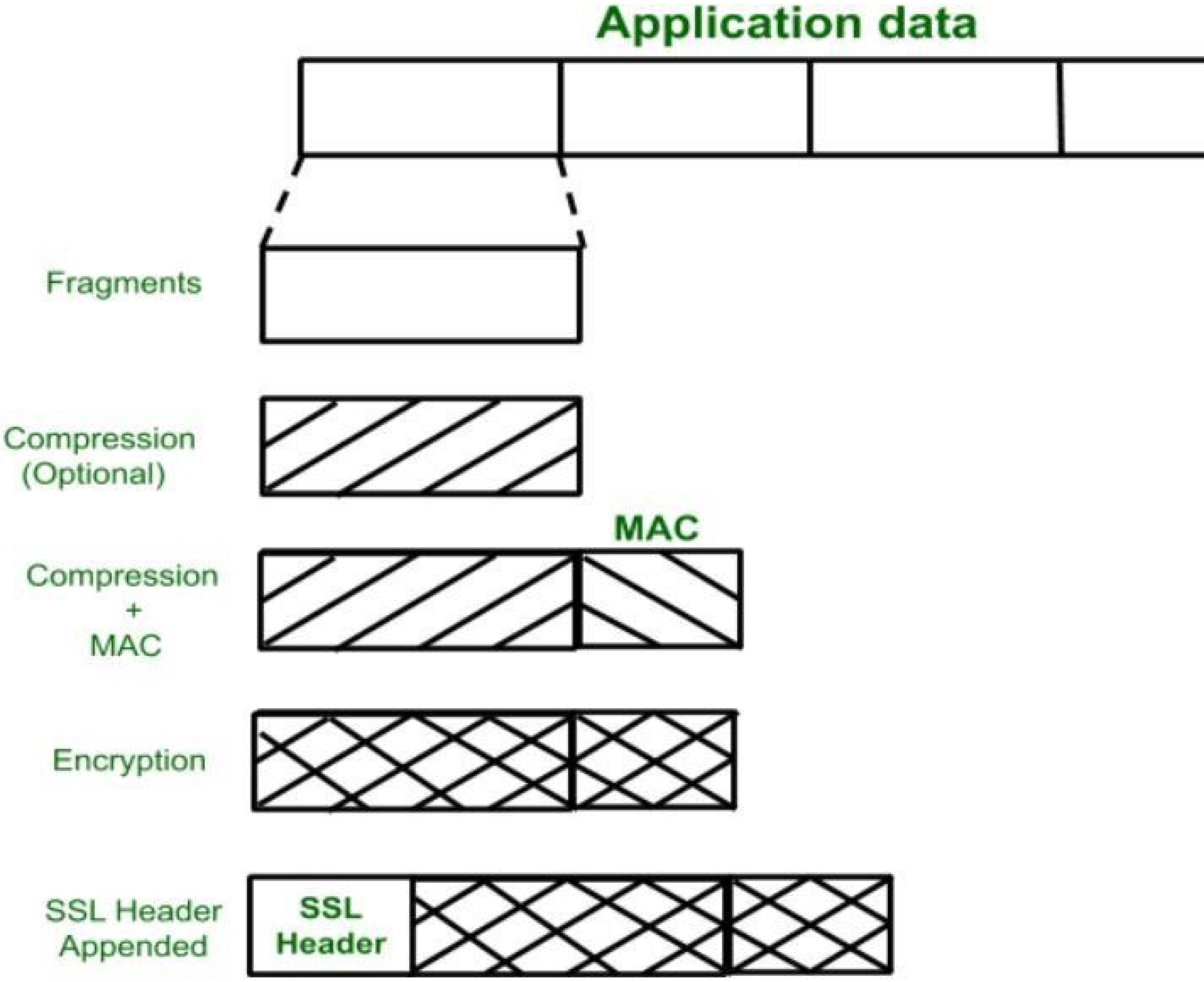


SSL Record Protocol:

SSL Record provides two services to SSL connection

- Confidentiality
- Message Integrity

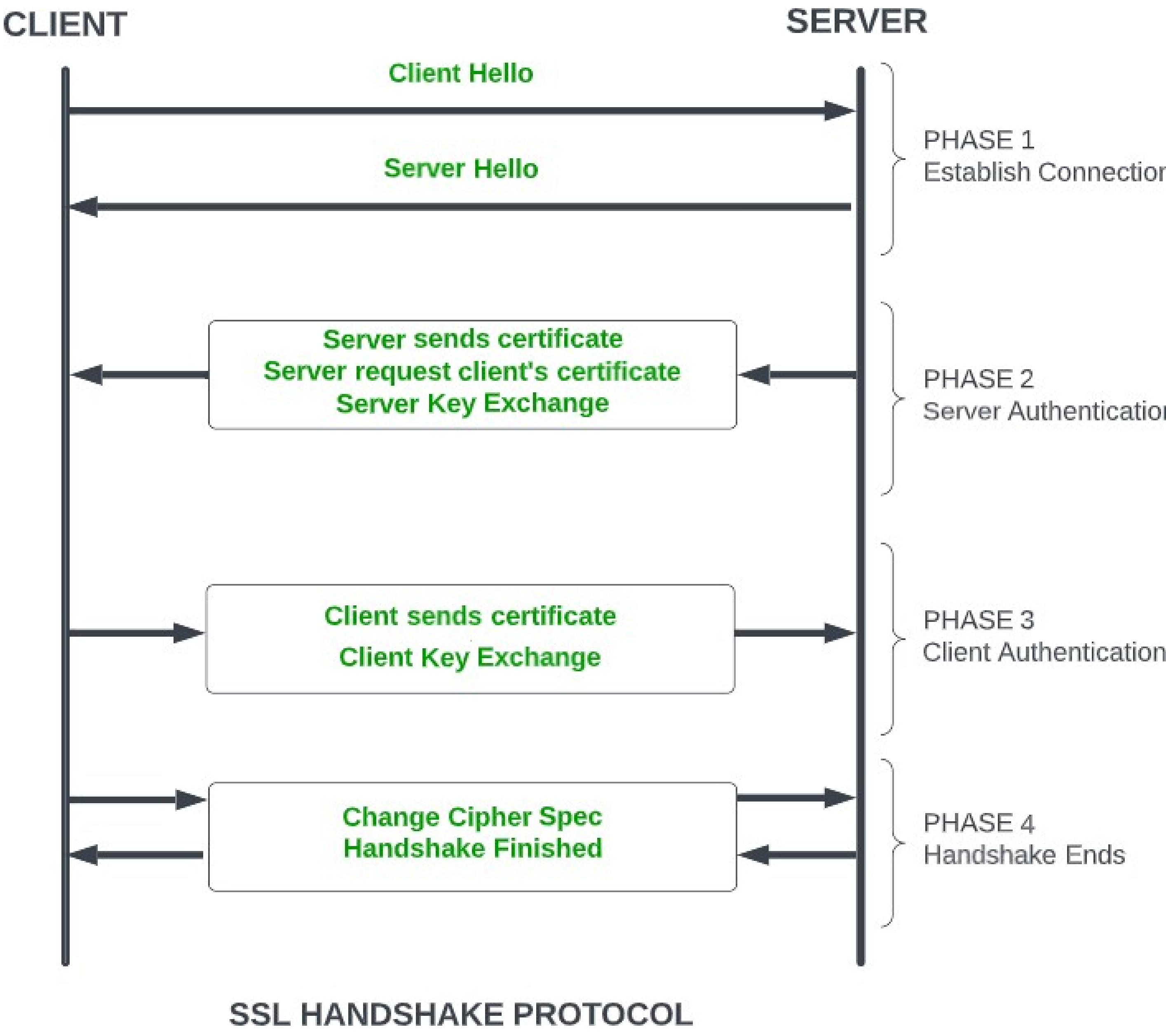
In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



Handshake Protocol:

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2:** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3:** In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- **Phase-4:** In Phase-4 Change-cipher suite occurs and after this the Handshake Protocol ends.



SSL Handshake Protocol Phases diagrammatic representation

2) What is VPN? Explain types of VPN. **[6]**

Ans- VPN stands for Virtual Private Network (VPN), that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection that is called VPN tunnel, and all Internet traffic and communication is passed through this secure tunnel. Virtual Private Network (VPN) is basically of 2 types:

1. Remote Access VPN

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both. An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.

2. Site to Site VPN

A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

- **Intranet based VPN:** When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
- **Extranet based VPN:** When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

3. Cloud VPN

A Cloud VPN is a virtual private network that allows users to securely connect to a cloud-based infrastructure or service. It uses the internet as the primary transport medium to connect the remote users to the cloud-based resources. Cloud VPNs are typically offered as a service by cloud providers such as Amazon Web Services (AWS) and Microsoft Azure. It uses the same encryption and security protocols as traditional VPNs, such as IPsec or SSL, to ensure that the data transmitted over the VPN is secure. Cloud VPNs are often used by organizations to securely connect their on-premises resources to cloud-based resources, such as cloud-based storage or software-as-a-service (SaaS) applications.

4. Mobile VPN

Mobile VPN is a virtual private network that allows mobile users to securely connect to a private network, typically through a cellular network. It creates a secure and encrypted connection between the mobile device and the VPN server, protecting the data transmitted over the connection. Mobile VPNs can be used to access corporate resources, such as email or internal websites, while the user is away from the office. They can also be used to securely access public Wi-Fi networks, protecting the user's personal information from being intercepted.

Mobile VPNs are available as standalone apps or can be integrated into mobile device management (MDM) solutions. These solutions are commonly used by organisations to secure their mobile workforce.

5. SSL VPN

SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses the SSL protocol to secure the connection between the user and the VPN server. It allows remote users to securely access a private network by establishing an encrypted tunnel between the user’s device and the VPN server. SSL VPNs are typically accessed through a web browser, rather than through a standalone client. This makes them easier to use and deploy, as they don’t require additional software to be installed on the user’s device. It can be used to access internal resources such as email, file servers, or databases. SSL VPNs are considered more secure than traditional IPsec VPNs because they use the same encryption protocols as HTTPS, the secure version of HTTP used for online transactions.

6. PPTP (Point-to-Point Tunneling Protocol) VPN

PPTP (Point-to-Point Tunneling Protocol) is a type of VPN that uses a simple and fast method for implementing VPNs. It creates a secure connection between two computers by encapsulating the data packets being sent between them. PPTP is relatively easy to set up and doesn’t require any additional software to be installed on the client’s device. It can be used to access internal resources such as email, file servers, or databases. PPTP is one of the oldest VPN protocols and is supported on a wide range of operating systems. However, it is considered less secure than other VPN protocols such as L2TP or OpenVPN, as it uses a weaker encryption algorithm and has been known to have security vulnerabilities.

7. L2TP (Layer 2 Tunneling Protocol) VPN

L2TP (Layer 2 Tunneling Protocol) is a type of VPN that creates a secure connection by encapsulating data packets being sent between two computers. L2TP is an extension of PPTP, it adds more security to the VPN connection by using a combination of PPTP and L2F (Layer 2 Forwarding Protocol) and it uses stronger encryption algorithm than PPTP. L2TP is relatively easy to set up and doesn’t require additional software to be installed on the client’s device. It can be used to access internal resources such as email, file servers, or databases. It is supported on a wide range of operating systems, but it is considered less secure than other VPN protocols such as OpenVPN, as it still has some vulnerabilities that can be exploited.

8. OpenVPN

OpenVPN is an open-source software application that uses SSL and is highly configurable and secure. It creates a secure and encrypted connection between two computers by encapsulating the data packets being sent between them. OpenVPN can be used to access internal resources such as email, file servers, or databases. It is supported on a wide range of operating systems and devices, and can be easily configured to work with various network configurations and security settings. It is considered one of the most secure VPN protocols as it uses the industry standard SSL/TLS encryption protocols and it offers advanced features such as two-factor authentication and kill switch.

3. Describe IPSec Protocol with its components and Security Services. **[6]**

IP Sec (Internet Protocol Security) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted, and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security

It has the following components:

1. Encapsulating Security Payload (ESP)
2. Authentication Header (AH)
3. Internet Key Exchange (IKE)

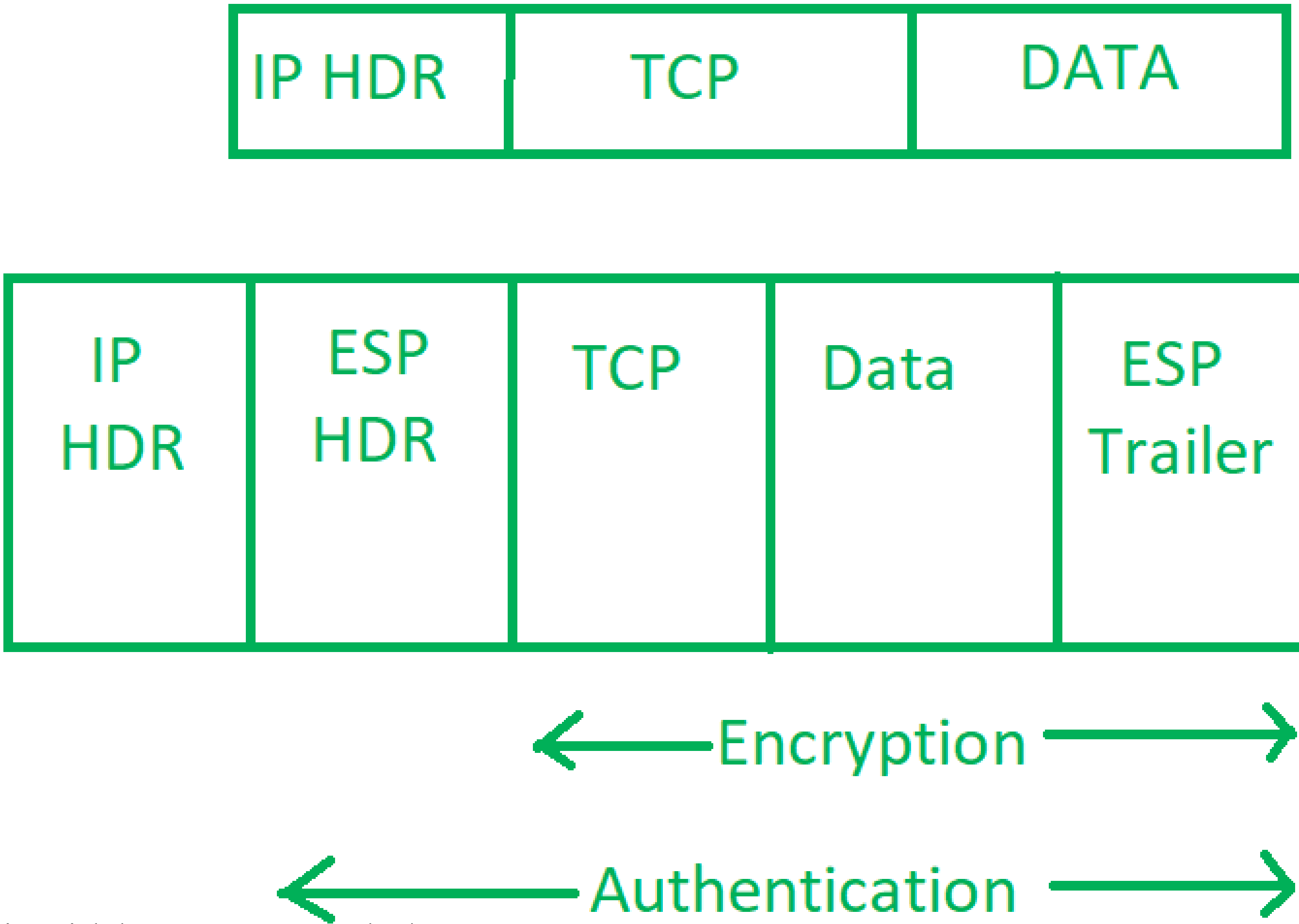
1. Encapsulating Security Payload (ESP): It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.

2. Authentication Header (AH): It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.

IP HDR	AH	TCP	DATA

IP Header

3. Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts are using IPsec. Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets that are not authorized are discarded and not given to the receiver.



4) Distinguish between PGP and S/MIME. **[6]**

Features	**PGP**	**S/MIME**
Full form	PGP is an abbreviation for Pretty Good Privacy.	S/MIME is an abbreviation for S Internet Mail Extension.
Effectively process	It is made to process emails in plain text.	It permits emails that also contain n
Cost	It is less costly than S/MIME.	It is more expensive than PGP.
Dependency	It relies on the user key exchange.	It relies on a hierarchically valid exchange.

Usage	It is useful for both personal and organizational purposes.	It is suitable for usage in the industr
Efficient	It is less efficient.	It is more efficient.
Convenient	It is less convenient.	It is more convenient because a securely transformed.
Public Keys	It has 4096 public keys.	It has only 1024 public keys.
Encryption	It is the standard for secure encryption.	It is a robust encryption sta limitations.
Digital Signature	It utilizes Diffie hellman's digital signature.	It utilizes Elgamal's digital signatur
VPN	It may be utilized in VPNs.	It is utilized with email services, no

5) Explain ISAKMP protocol of IPSec. **[6]**

Ans- Internet Security Association and Key Management Protocol (ISAKMP) is a framework for establishing security associations (SAs) and performing key exchange in a secure manner. SAS are agreements between two devices that define how they will communicate securely. Key exchange refers to the process of exchanging keys or other cryptographic material that is used to secure communication.

ISAKMP is a protocol that defines the structure and format of messages used to establish and maintain SAs. It does not specify the actual cryptographic algorithms or keys that are used. Instead, it provides a framework for negotiating these details and for establishing a secure channel between two devices.

ISAKMP is used in conjunction with other protocols, such as the Internet Key Exchange (IKE) protocol, which is used to negotiate and establish SAs. ISAKMP and IKE are commonly used to establish secure Virtual Private Network (VPN) connections, which allow devices to communicate securely over the internet.

ISAKMP is defined in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2408. It is an important component of many Internet security protocols and is widely used in enterprise networks and other environments where secure communication is important.

6) Identify Threats to web Security and figure out how any of two among listed are countered by particular feature of SSL. **[6]**
Ans-

a. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm..

b. Known Plaintext Dictionary Attack: Many messages will contain predictable plaintext, such as the HTTP GET command.

An attacker constructs a dictionary containing every possible encryption of the known-plaintext message.

When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary.

The ciphertext should match against an entry that was encrypted with the same secret key.

If there are several matches, each of these can be tried against the full ciphertext to determine the right one. This attack is especially effective against small key sizes (e.g., 40-bit keys)..

c. Replay Attack: Earlier SSL handshake messages are replayed..

d. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client..

e. Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped..

f. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data..

g. IP Hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts..

h. SYN Flooding:An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully.

The attacked TCP module typically leaves the "half-open connection" around for a few minutes.

Repeated SYN messages can clog the TCP module.

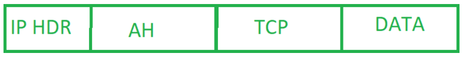
Web Security:

Web security means to protect the web pages and applications from cyber theft. The internet security threats are injection, authentication flaws, insecure direct object references, security misconfiguration, sensitive data exposure, a lack of function-level authorization, CSRF, insecure components, and unfiltered redirects.

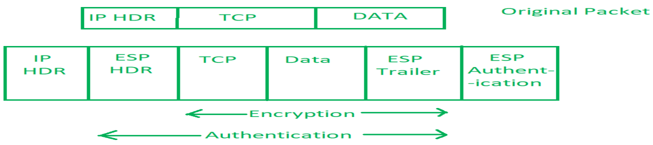
7) *Q3) a)* List and explain components of IPSec protocol [6]

Ans : Components of IP Security:

1. Encapsulating Security Payload (ESP): It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.
2. Authentication Header (AH): It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.

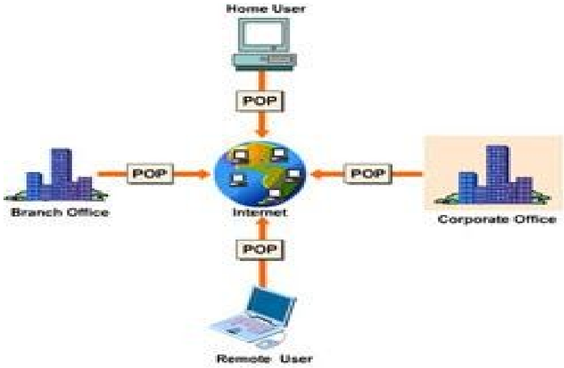


3.Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts are using IPsec.



***Q3) b)* What is VPN? Explain components of VPN. [6]**

Ans : A VPN is a private network that provides a low-cost and secure remote access communication framework. Organizations use it to provide controlled access to the corporate network. A VPN replaces physical dedicated leased line connections with secure virtual connections called tunnels set up over a public network. It provides the benefits of a traditional WAN at a lower cost.



Components of a VPN

- **VPN server**:
- **VPN client:**.
- **VPN connection**:
- **Tunnel:**
- **Tunneling protocols**:
- **Tunneled data**:
- **Shared or public network**:

***Q3) c)* Explain working of PGP in details. [6]**

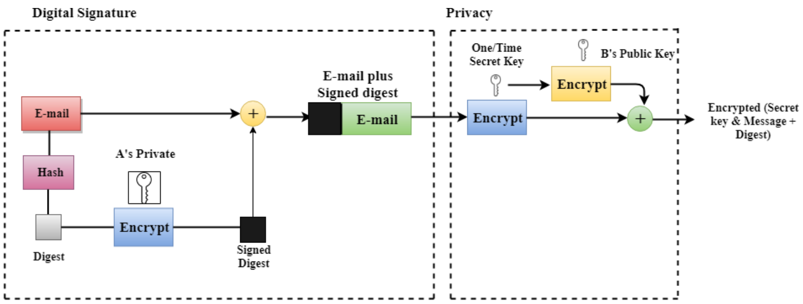
Ans : PGP stands for Pretty Good Privacy (PGP).

- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.

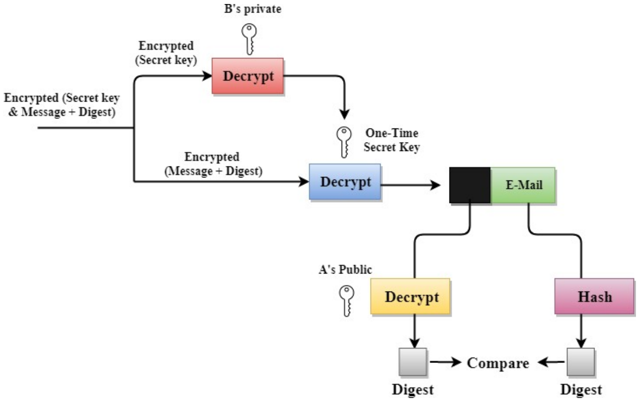
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

Following are the steps taken by PGP to create secure e-mail at the sender and receiver site:

PGP at the Sender site (A)



PGP at the Receiver site (B)

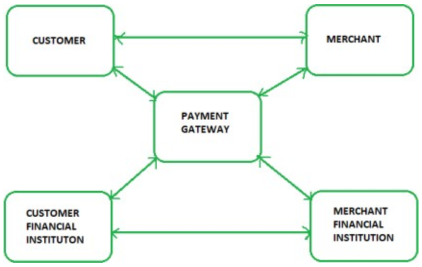


OR

_Q4) a)_ List and explain various participants involved in Secure Electronic Transaction (SET) [6]

Ans: SET is a system that ensures the security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied to those payments. It uses different encryption and hashing techniques to secure payments over the internet done through credit cards. The SET protocol was supported in development by major organizations like Visa, Mastercard, and Microsoft which provided its

Secure Transaction Technology (STT), and Netscape which provided the technology of Secure Socket Layer (SSL).



Participants in SET: In the general scenario of online transactions, SET includes similar participants:

1. **Cardholder –** customer
2. **Issuer –** customer financial institution
3. **Merchant**
4. **Acquirer –** Merchant financial
5. **Certificate authority –** Authority that follows certain standards and issues certificates to all other participants.

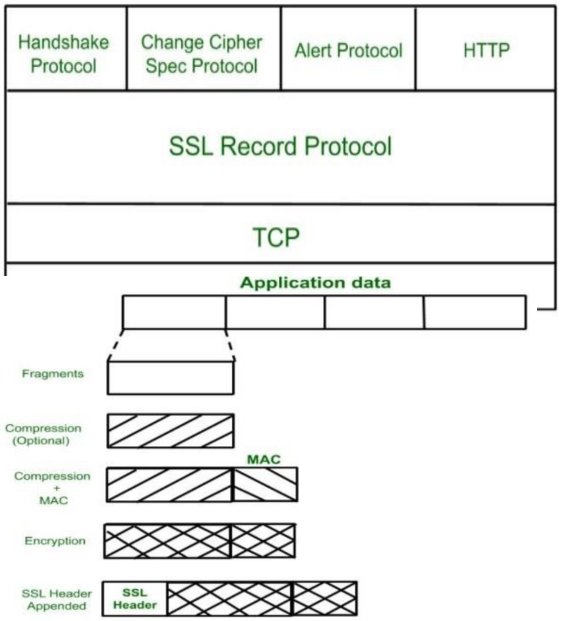
Q4) b) **Describe the SSL protocol in details.**
[6]

Ans : Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

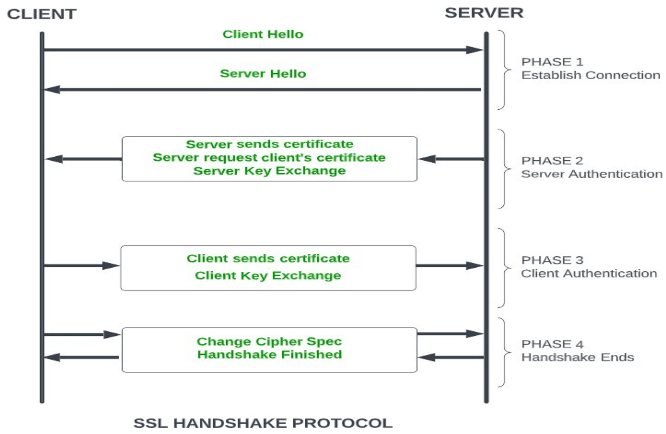
SSL Protocol Stack: **SSL Record Protocol:**



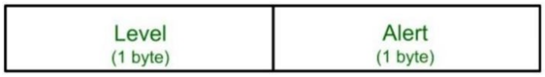
Change-cipher Protocol:

This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After the handshake protocol, the Pending state is converted into the current state. Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state tobe copied into the current state.

Handshake Protocol:



Alert Protocol: This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.



Level (1 byte)	Alert (1 byte)

***Q4) c)* What is S/MIME? What are the benefits of S/MIME? [6]**

Ans : S/MIME, or Secure Multipurpose Internet Mail Extension, is an email encryption and signing industry standard widely used by corporations to enhance email security. S/MIME is compatible with most enterprise email clients.In simple terms, S/MIME is an encryption protocol used to digitally sign and encrypt an email to ensure that the email is authenticated and its content is not altered.

Benefits of S/MIME:

- Email Encryption
- Data Confidentiality
- Digital Signature
- Signature Authentication
- Non-repudiation by the Sender
- Content Integrity of the Email