Seat No :

Total No. of Questions: 08] **[Total No. of Pages: 02**

T.E. (AI&DS)
CYBER SECURITY
(2019 Pattern) (Semester - II) (317530)

Time: 2½ Hours] ***[Max. Marks: 70***

Instructions to the candidates:

1) ***Answer Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q.6, Q.7 or Q.8***
2) ***Neat diagrams must be drawn whenever necessary.***
3) ***Draw neat figures wherever necessary.***
4) ***Figures to the right side indicate full marks.***
5) ***Use of calculator is allowed.***
6) ***Assume suitable data if necessary.***

Q1) a) Explain Public Key Cryptography. **[6]**

b) Perform encryption and decryption using RSA algorithm for p=17, q=11, e=7 and M=2 **[6]**

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

OR

Q2) a) Explain operation of MD5 message digest algorithm. **[6]**

b) 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 $X_A = 5$, what is A's public key Y_A?
b. If user B has private key X_B=12, what is B's public key Y_B?
c. What is the shared secret key? **[6]**

c) Explain X.509 Authentication Service. **[6]**

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

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

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

OR

Q4) a) List and explain various participants involved in Secure Electronic Transaction (SET) **[6]**

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

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

P.T.O.

Q5) a) Explain the architecture of firewall. **[6]**

b) What is trusted system? Explain in brief. **[6]**

c) Difference between IDS and IPS **[5]**

OR

Q6) a) List and explain types of Intrusion Detection System. **[6]**

b) What is access control security service? **[6]**

c) Describe operation of packet filtering firewall. **[5]**

Q7) a) What is Cyber Staking **[6]**

b) Write short note on Mobile Hacking **[6]**

c) Explain Indian IT Act **[5]**

OR

Q8) a) Explain PII impact level with examples. **[6]**

b) Write short note on Cybercrime. **[6]**

c) Write Advantages of cyber law. **[5]**

▽▽▽▽

TE-AI&DS- CYBER SECURITY

Unit-4

[NOV/DEC-2024]

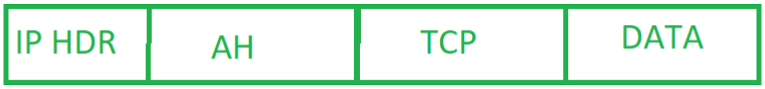
Q.1) List and explain components of IPSec protocol **[6]**

[NOV/DEC-2024]

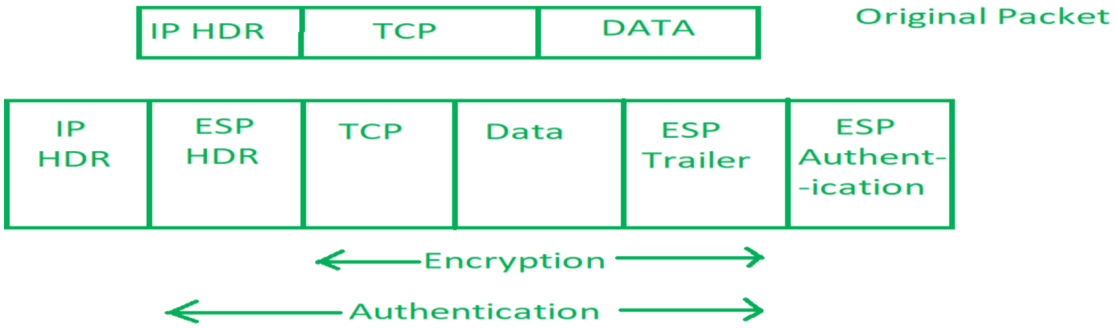
Ans : Components of IP Security:

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.



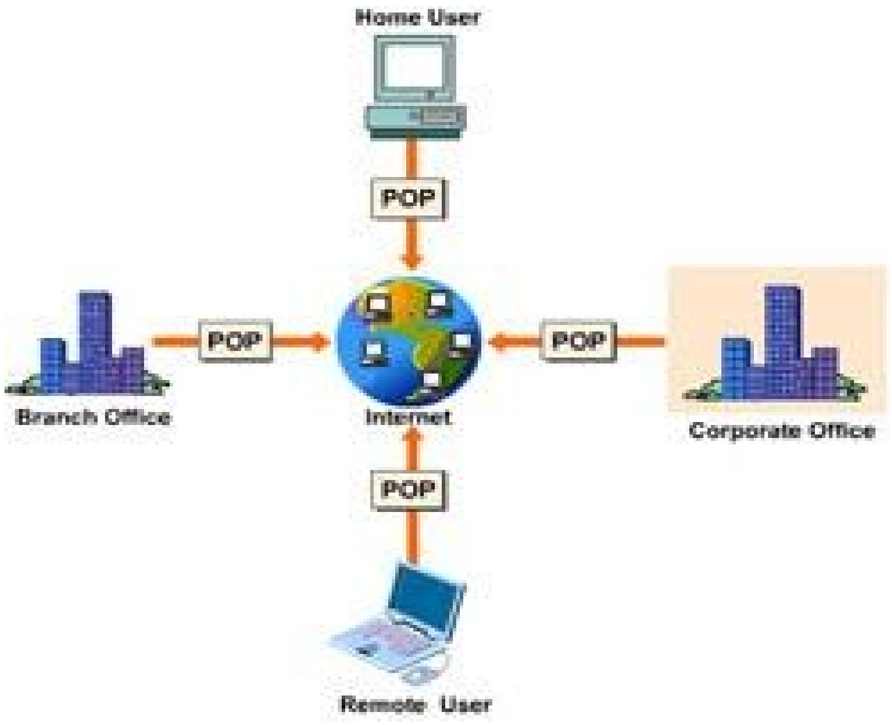
3.Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. 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.



***Q2)* What is VPN? Explain components of VPN.** **[6]**

[NOV/DEC-2024]

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

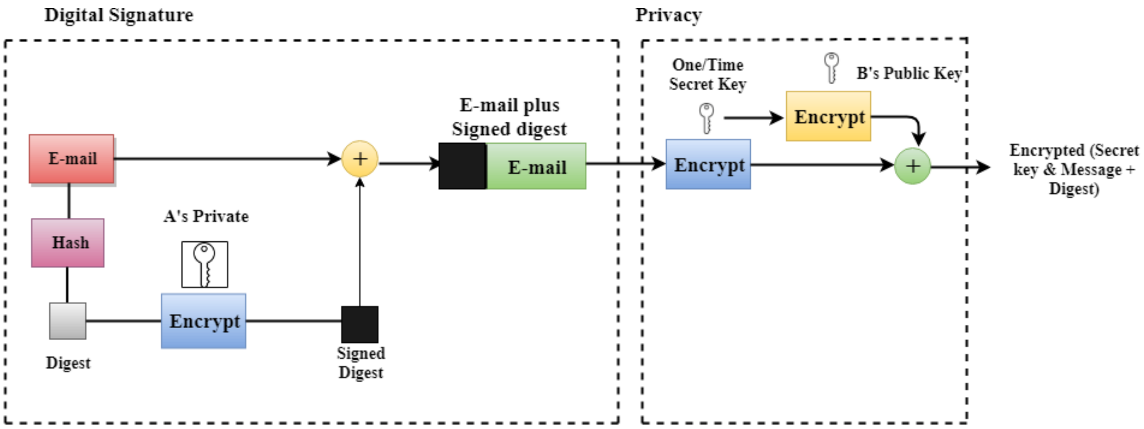
[NOV/DEC-2024]

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

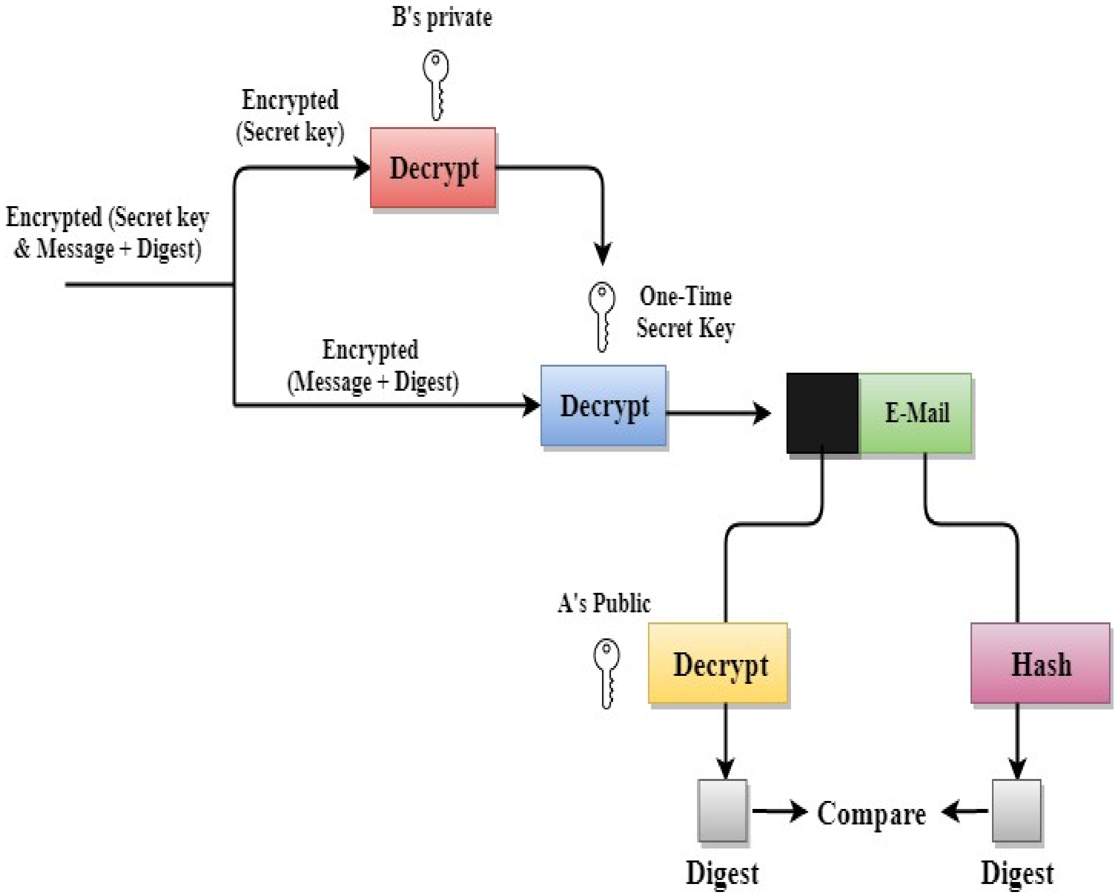
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It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

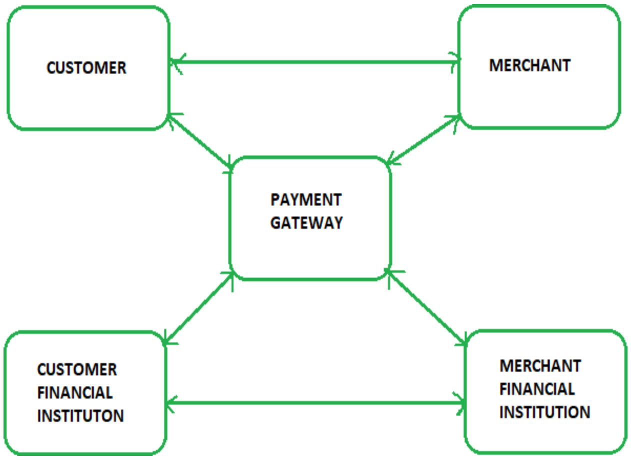


***Q4)* List and explain various participants involved in Secure Electronic Transaction (SET) [6]**

[NOV/DEC-2024]

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.

***Q5)* Describe the SSL protocol in details.** **[6] [NOV/DEC-2024]**

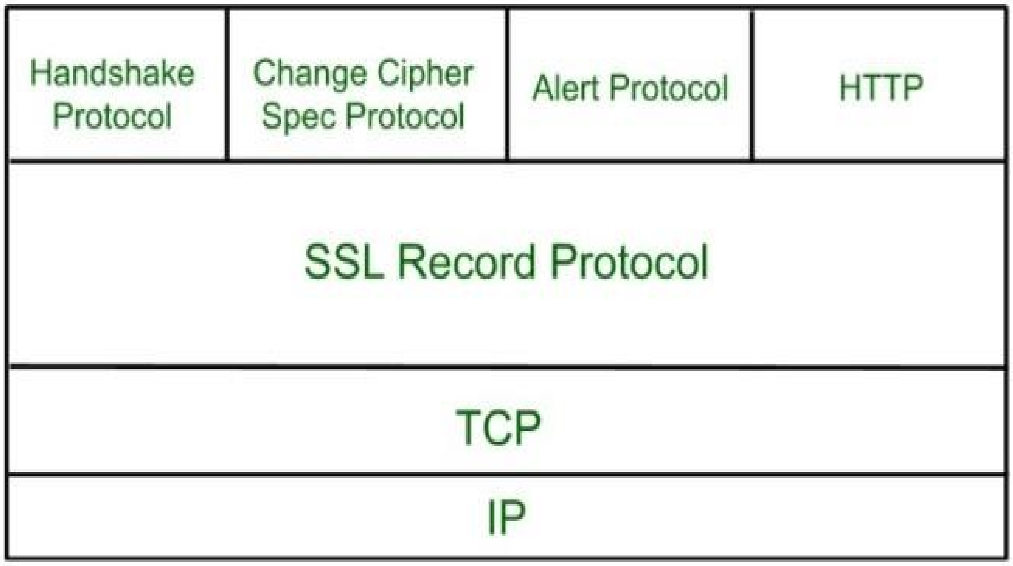
Ans :

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.

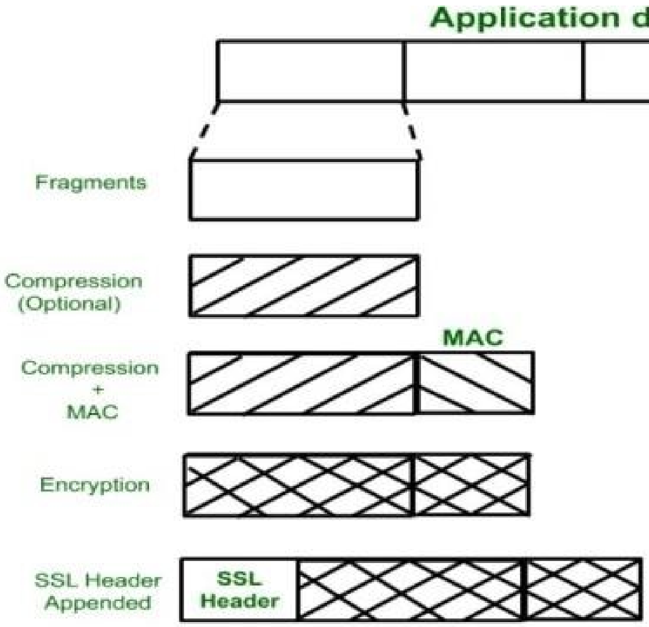
Secure Socket Layer Protocols:

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

SSL Protocol Stack:



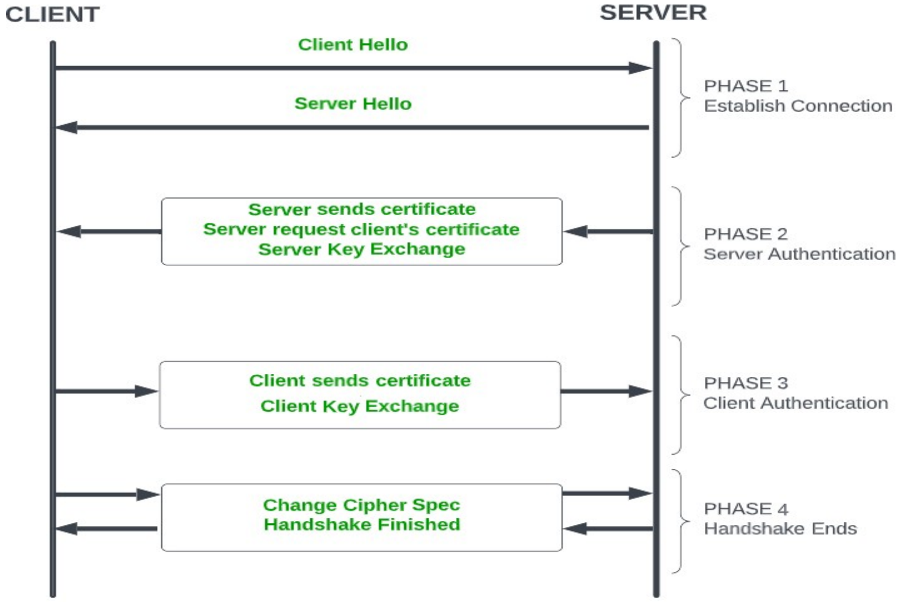
SSL Record Protocol:



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:



SSL 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)

***Q6)*What is S/MIME? What are the benefits of S/MIME? [6]**

[NOV/DEC-2024]

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

Shree Ramchandra Education Society's

SHREE RAMCHANDRA COLLEGE OF ENGINEERING

Lonikand, Pune – 412216

Department of Artificial Intelligence and Data Science

TE-AI&DS- CYBER SECURITY

Unit-4

[NOV/DEC-2024]

Q.1) List and explain components of IPSec protocol **[6]**

[NOV/DEC-2024]

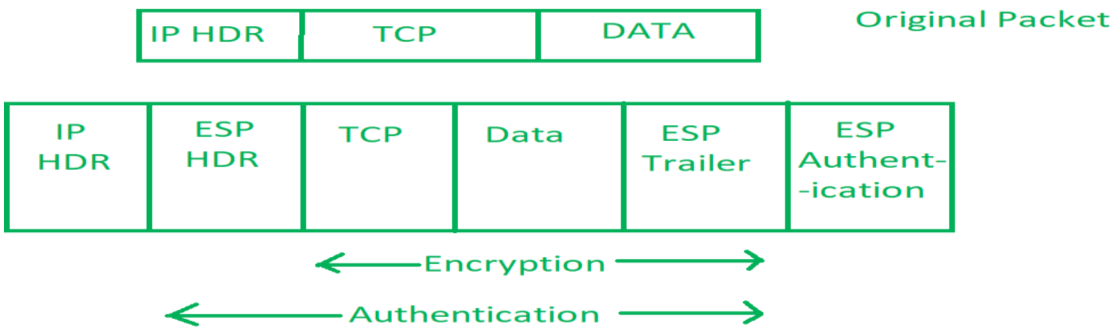
Ans : Components of IP Security:

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.

IP HDR	AH	TCP	DATA

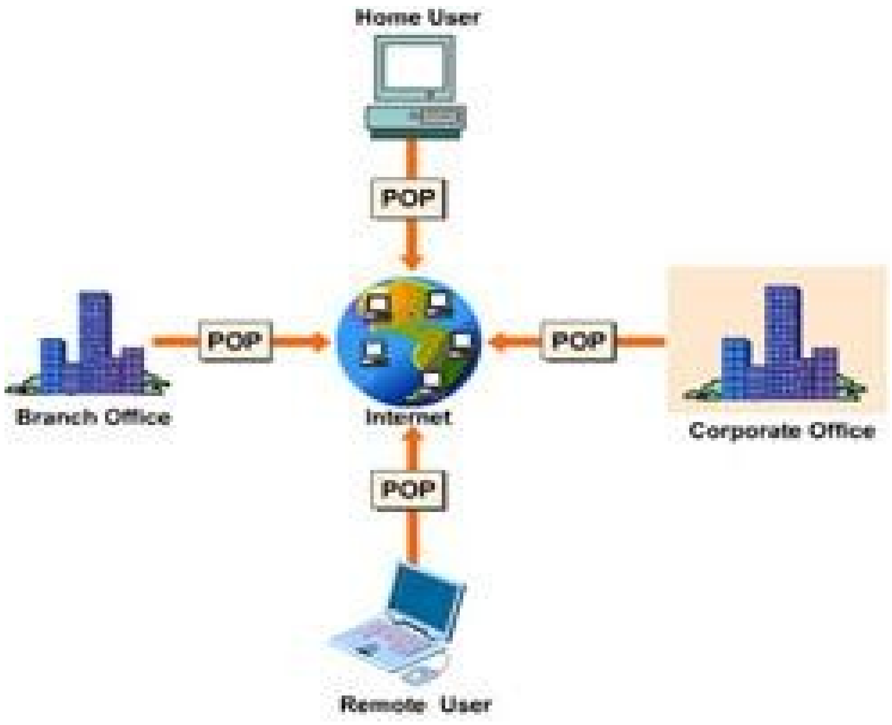
3.Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. 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.



***Q2)* What is VPN? Explain components of VPN.** **[6]**

[NOV/DEC-2024]

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

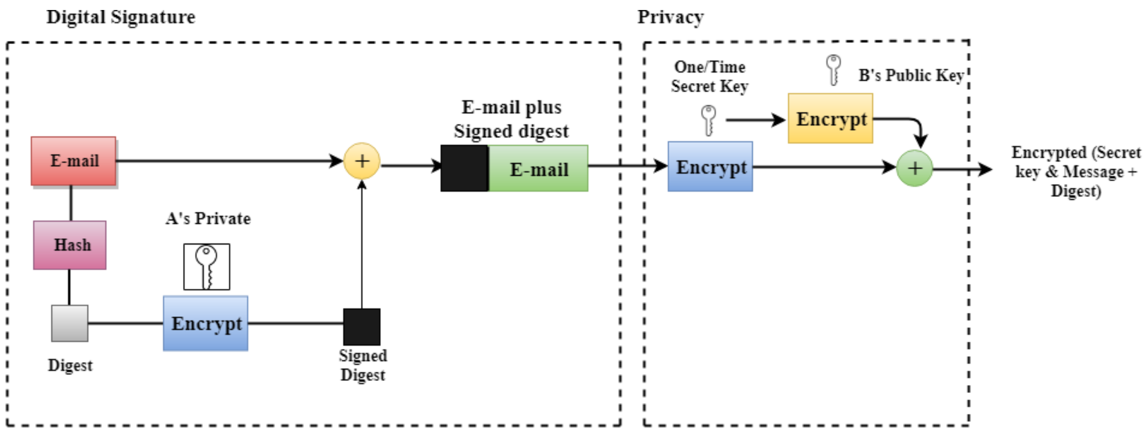
[NOV/DEC-2024]

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

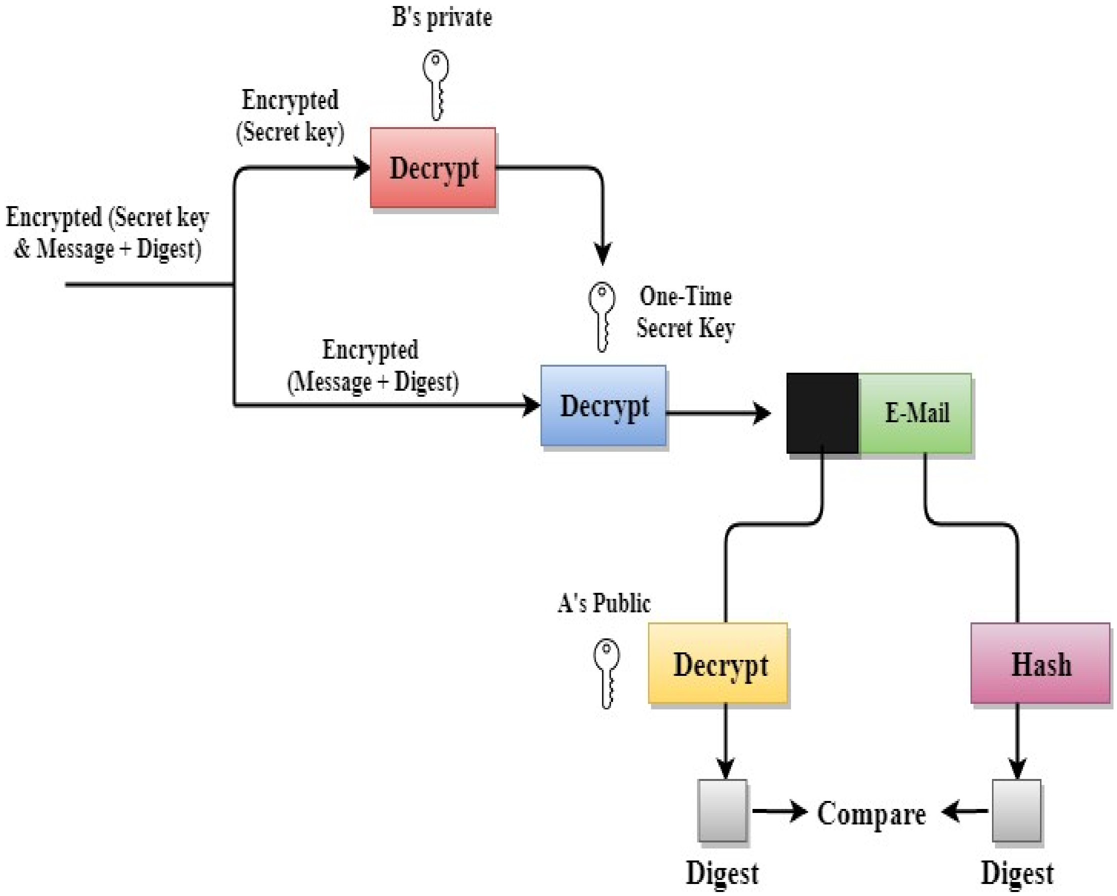
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It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

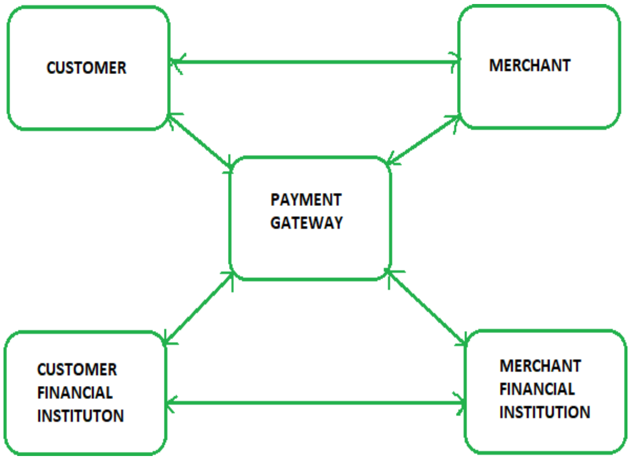


***Q4)* List and explain various participants involved in Secure Electronic Transaction (SET) [6]**

[NOV/DEC-2024]

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.

***Q5)* Describe the SSL protocol in details. [6] [NOV/DEC-2024]**

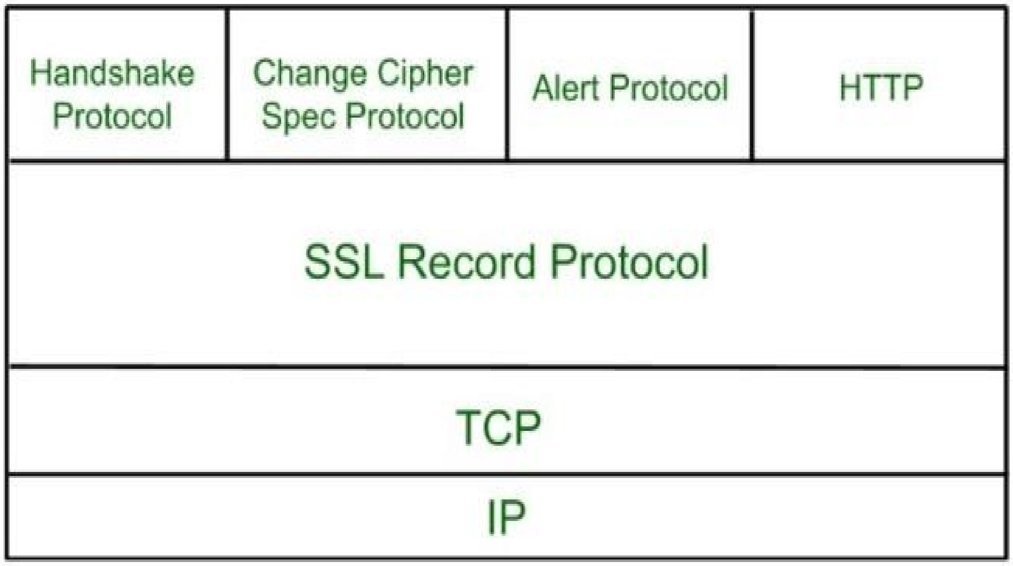
Ans :

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.

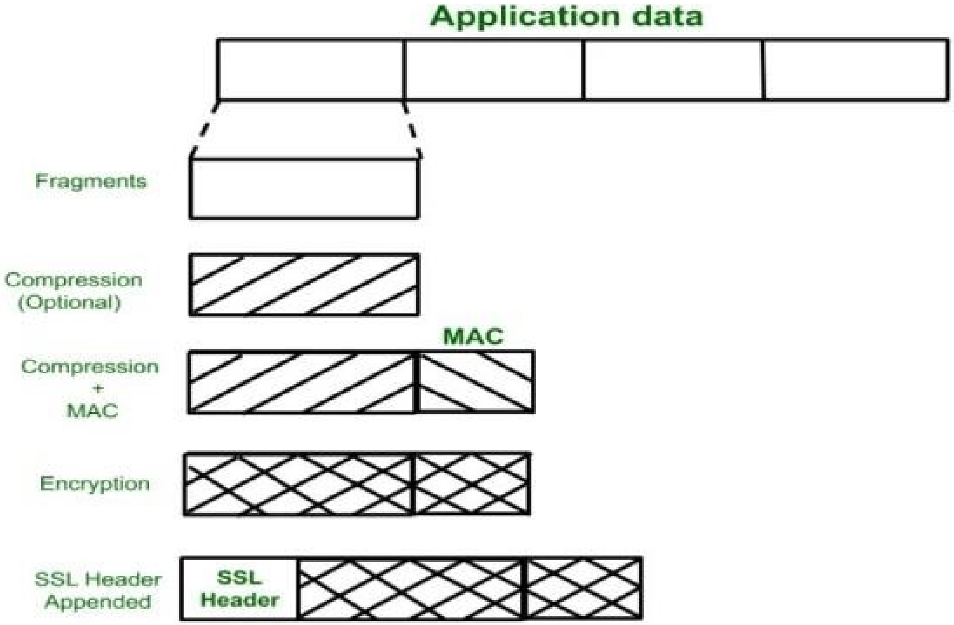
Secure Socket Layer Protocols:

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

SSL Protocol Stack:



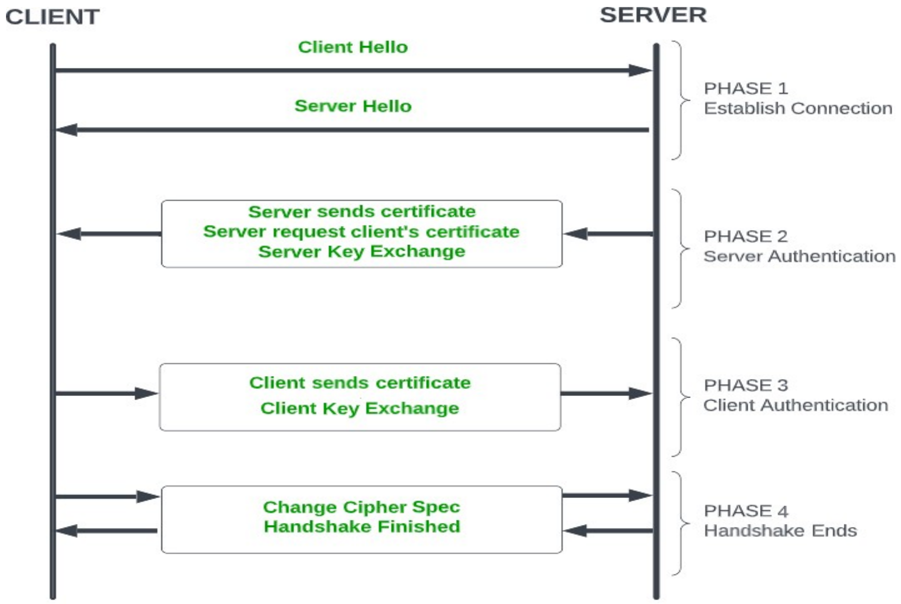
SSL Record Protocol:



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:



SSL 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)

Q6)**What is S/MIME? What are the benefits of S/MIME?** **[6]**

[NOV/DEC-2024]

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