Name : Binod Kumar
Roll no. : 23203006
Class : M.Tech CSE
Semester : 2nd
Subject : Cyber Forensics
Assignment : 02

Q1. Analyze how is the security Association used in the following parameters:

a) security policy Database
b) security Association Database
c) Transport mode SA
d) Tunnel Mode SA

Ans:

a) security policy Database (SPD):

- Security policy is one of the important aspect of IPsec, which defines the types security applied to the packet when it is to be sent or when it has arrived. Before using security association database, a host must determine the predefined policy for the packet.
- Security policy Database is a database which store the security policy. Each host that is using the IPsec needs to keep a security policy database. Again there is a need of an inbound SPD and an outbound SPD.
- Each entry in the SPD can be accessed using a six tuple index.

Index	Policy
<SA, DA, Name, P, SPort, DPort>	
<SA, DA, Name, P, SPort, DPort>	
<SA, DA, Name, P, SPort, DPort>	
<SA, DA, Name, P, SPort, DPort>	

- SA: Source Address
- DA: Destination address
- SPort: Source Port
- DPort: Destination Port
- P: Protocol

b) Security Association Database (SAD):

- The security Association database is the heart of the security mechanism. It stores the actual security Associations. Each SA contain a set of security parameters for a specific secure communication channel between two devices.
- The database can be thought as a two dimensional table with each row defining a single SA.
- Normally, there are two SADs. one inbound and one outbound.

<SPI, DA, P>						
<SPI, DA, P>						
<SPI, DA, P>						
<SPI, DA, P>						

Security Association Database

Legend:

- SPI : Security Parameter Index
- DA : Destination address
- P : Protocol
- SN : Sequence numbers
- LT : Lifetime

Now,

⇒ SPI is 32-bit number that defines the SA at the destination.

⇒ Destination Address is the 2nd index which is the destination address of the host.

⇒ Protocol such as AH and ESP.

c) Transport mode SA

- A transport mode SA is used to secure the data portion (payload) of a packet.
- It operates at layer four of the OSI model.

How it uses SA

i) The transport mode SA defines the cryptographic algorithms and keys used to encrypt/decrypt the data payload packets.

ii) only the payload is secured, leaving the header information such as source/Dest IP, Port etc unencrypted.

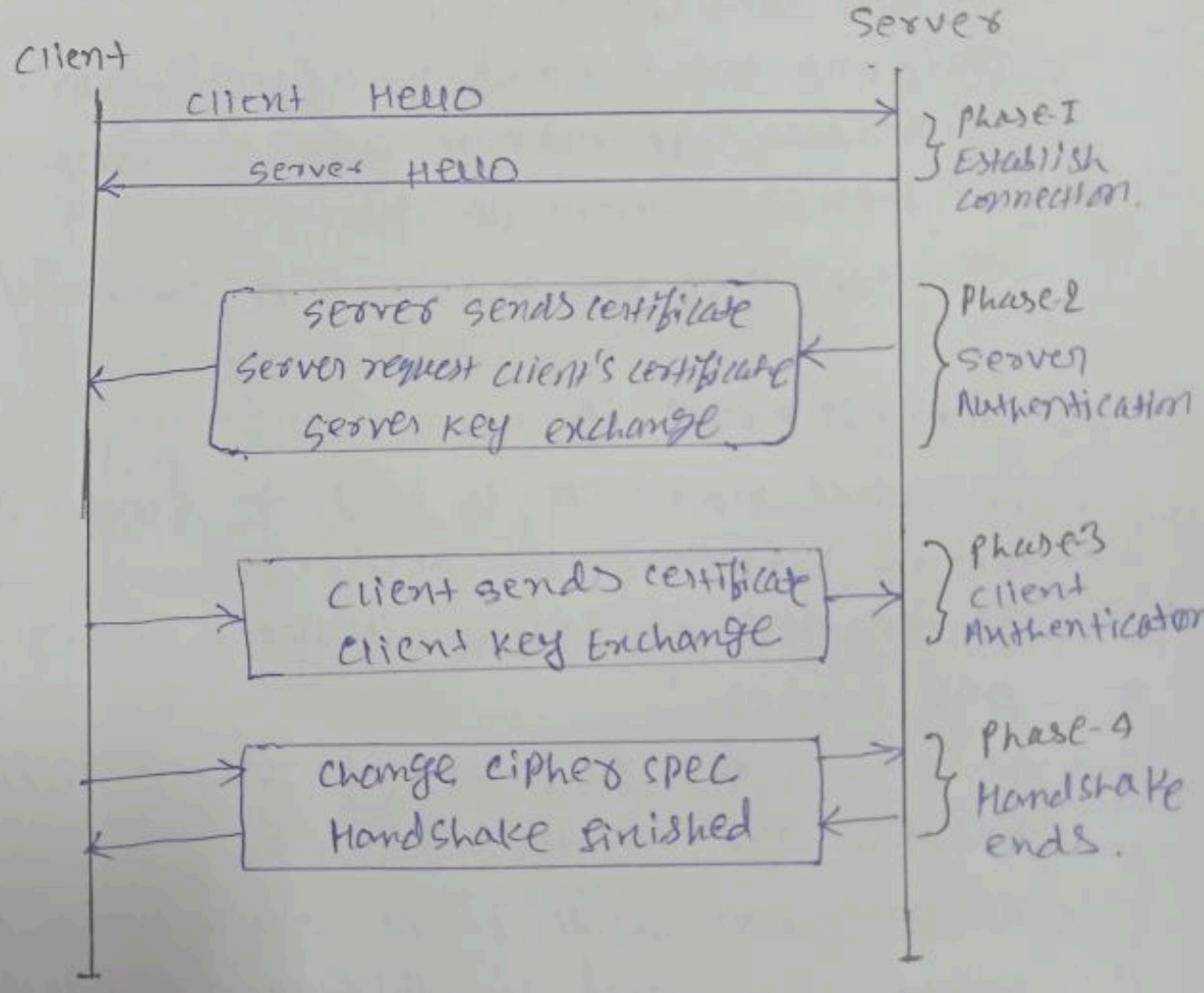
iii) Typically for end-to-end communication.

d) Tunnel mode SA.

- The Tunnel mode SA is used to create a secure tunnel between two devices.
- It operates at layer 3 (Network layer) of the OSI model.
- It secures the IP packet as whole including header.
- Actually puts an IP packet within another outer one.
- Packet is delivered according to the outer IP header
- Typically for router-to-router, or firewall-to-firewall communication.

8.25 Explain in detail about SSL Handshaking protocol between a server and client connection with an appropriate diagram.

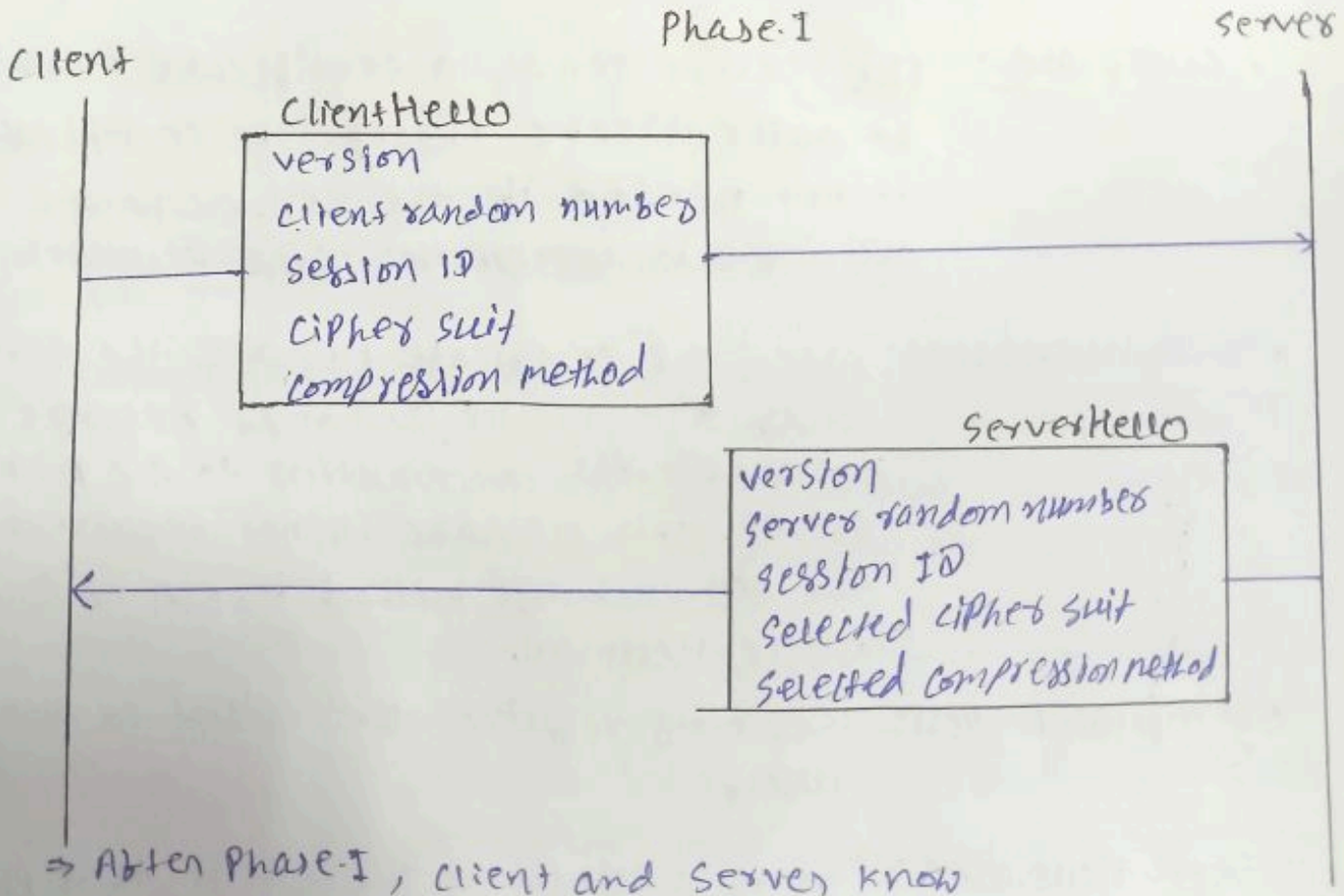
Ans:
- Handshake protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other.
- Handshake protocol uses four phases to complete its cycle.



SSL Handshake Protocol.

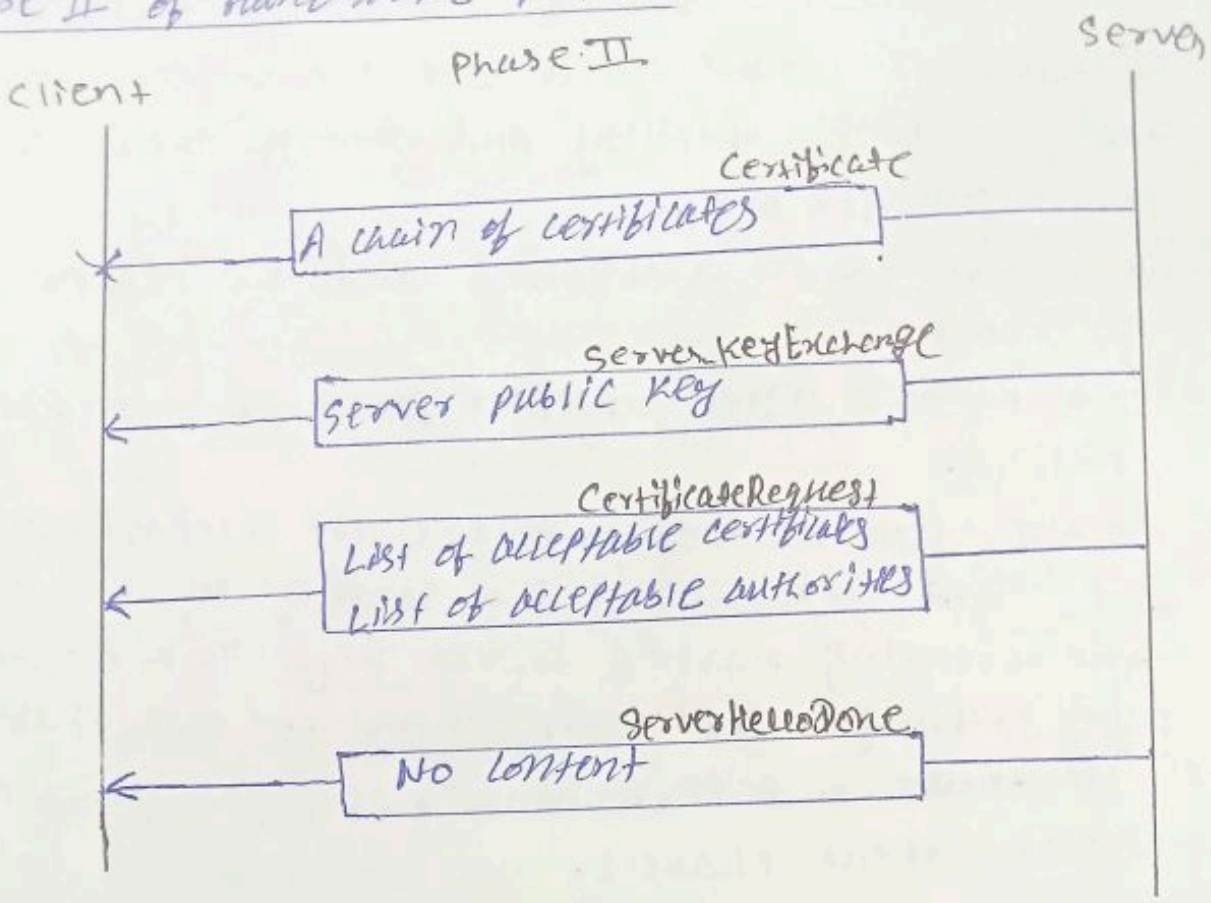
Phase-I : Establishing security capability/connection

- In this phase, the client and the server announce their security capability and choose those that are convenient for both.
- a session ID is established and the cipher suit is chosen.
- The parties agree upon a particular compression method.
- Finally, two random numbers are selected, one by the client and one by the server, to be used for creating master secret key. Two messages are exchanged between them in this phase.
- ClientHello and ServerHello messages gives additional details about phase-1.



⇒ After Phase-I, client and server know
i) version of SSL
ii) Algorithm for key exchange. Authentication & encryption.
iii) compression method
iv) Two random nos for key generation

Phase II of Handshake Protocol



- **Certificate**: The server sends a certificate message to authenticate itself. The certificate is not needed if the key-exchange algorithm is anonymous Diffie-Hellman.
- **ServerKeyExchange**: After the certificate message, the server sends a serverkeyexchange message that includes its contribution to the pre-master secret. This message is not required if the key-exchange method is RSA or fixed Diffie-Hellman.
- **CertificateRequest**: The may require the clients to authenticate itself.

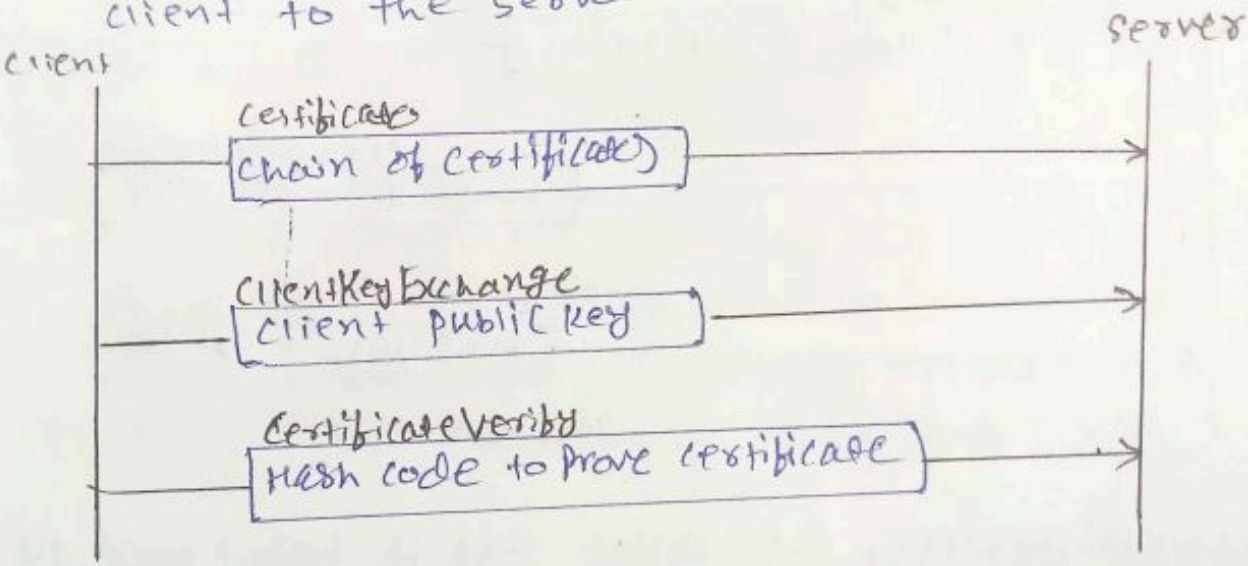
ServerHelloDone: It is a signal to the client that Phase-II is over and that client needs to start phase III.

⇒ After Phase II,

- The server is authenticated to the client.
- The client knows the public key of the server if required.

Phase III : client key Exchange and Authentication

- It is designed to authenticate the client.
- UP to three messages can be sent from the client to the server.



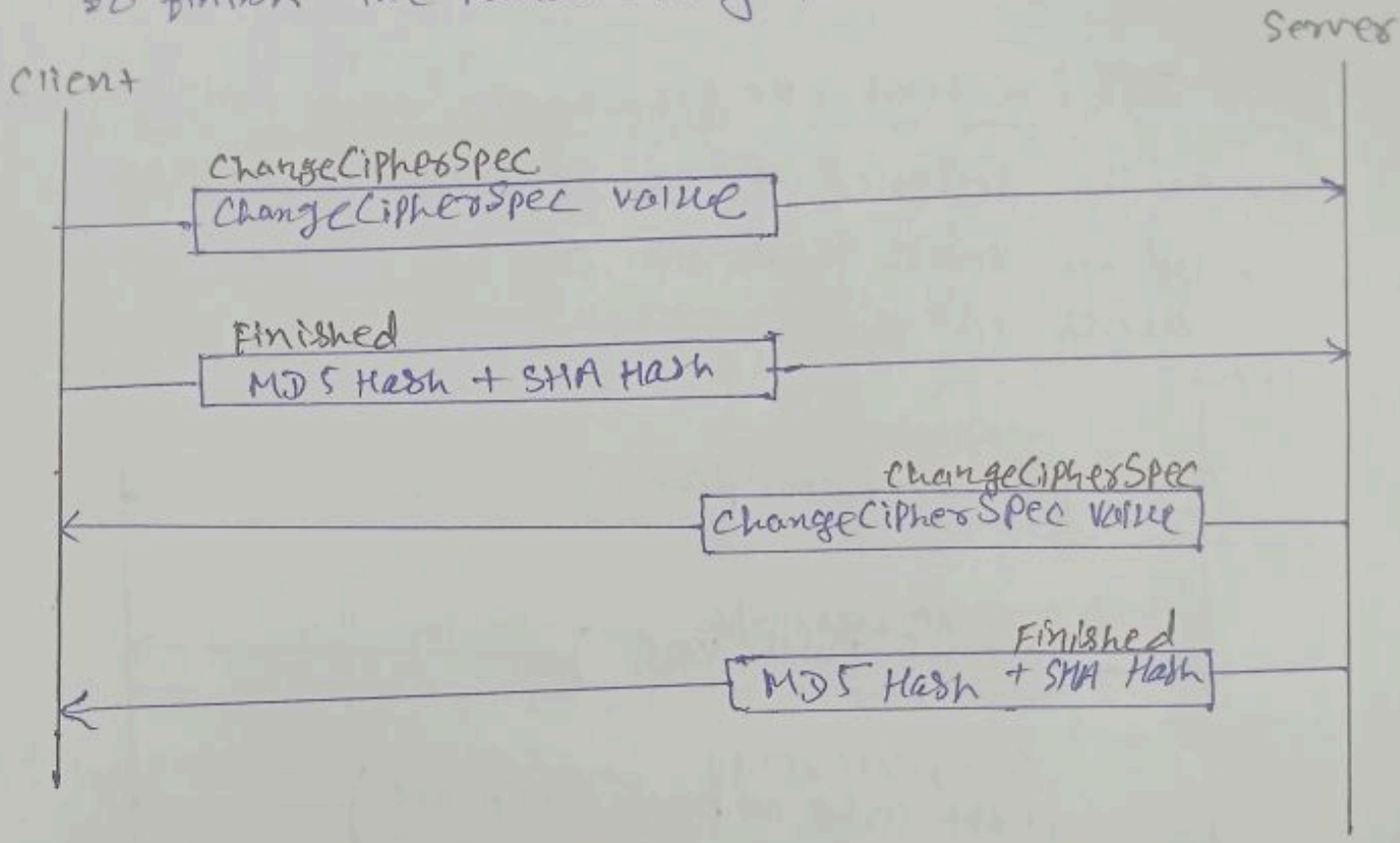
- certificate : To verify itself to the server.
- ClientKeyExchange: After sending the certificate message, the client sends a ClientKeyExchange message, which includes its contribution to the pre-master secret.
- CertificateVerify: If the client has sent a certificate declaring that its own the public key in the certificate, it needs to prove that it knows the corresponding private key.

⇒ After phase III:

- The client is authenticated by the server
- Both client and server know the pre master secret

Phase IV: Finalizing and Finishing

In this phase, the client and server send messages to change ciphers specification and to finish the handshaking protocol.



- ChangeCipherSpec: It shows that it has moved all of the cipher suit set and the parameters from the pending state to the active state.
- Finished: which announces the end of the handshaking protocol.

Q.3) Explain S/MIME and the general syntax it uses to support different content types?

Ans: S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for securing email communication. It leverages existing MIME technology to add encryption and digital signatures to email messages.

S/MIME utilizes public-key cryptography to achieve two main functionalities:

i) Digital signature:

This allows the senders to sign the email message with their private key. The recipient can then verify the signature using the sender's public key, ensuring the message originated from the claimed senders and hasn't been tampered with in transit.

ii) Encryption:

S/MIME allows encryption of the email content using the recipient's public key. only the recipient with the corresponding private key can decrypt the message, ensuring confidentiality.

- All of new content types include the parameter "application/PKCS7-mime" in which "PKCS" defined public key cryptography specification.

There are following content type.

1) signed-data content type:

- This type provides only integrity of data.
- It contains any type and zero or more signature values
- The encoded result is an object called signedData.

The following are the steps in the process of signed-Data content type

i) for each signer, a message digest is created from the content using the specific hash algorithm chosen by that signer.

ii) Each message digest is signed with the private key of the signer.

iii) The content, signature values, certificates and algorithms are then collected to create the signedData object.

2.) Enveloped-Data content type:

- This type is used to provide privacy for the message.
- It contains any type and zero or more encrypted keys and certificates.
- The encoded result is an object called envelopedData.

Process

i) A pseudorandom session key is created for the symmetric key algorithms to be used.

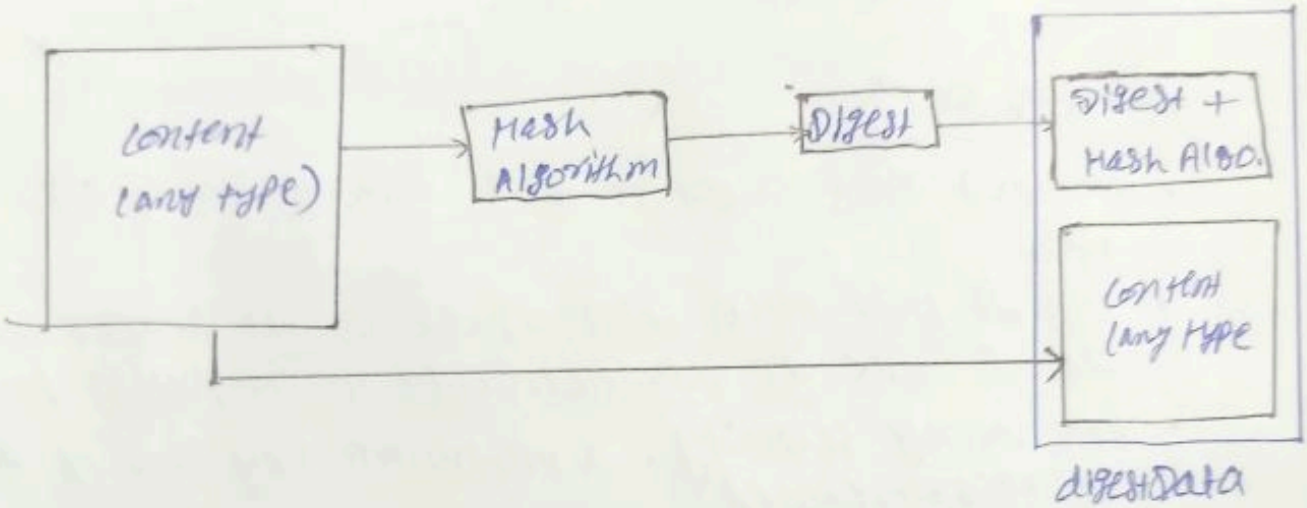
ii) for each recipient, a copy of the session key is encrypted with the public key of each recipient.

iii) The content is encrypted using the defined algorithm and created session key.

iv) The encrypted contents, encrypted session keys, algorithm used and certificates are encoded using Radix-64.

3. Digested-Data content type:

- This type is used to provide integrity for the message.
- The result is normally used as the content for the enveloped-data content type.
- The encoded result is an object called digestedData.



4. Authenticated-Data content type:

This type is used to provide authentication of data. The object is called authenticatedData.

Process

i) Using a pseudorandom generator, a MAC key is generated for each recipients.

ii) The MAC key is encrypted with the public key of the recipient.

iii) A MAC is created for the content

iv) The content, MAC, algorithms and other information are collected together to form the authenticatedData object.

Q.4] What is PGP? What key size is allowed in PGP? How does PGP provides encryption and authentication

Ans:
- PGP, which stands for pretty good privacy. It is a software that allows you to encrypt and decrypt digital messages and files.
- PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

PGP key sizes

- Allowed key sizes in PGP range from 512 to 4096 bits.
- 512 bit was once common, it is no longer considered secure due to advancements in computing power.
- For strong security, a minimum key size of 2048 bits is recommended.

Encryption and Authentication

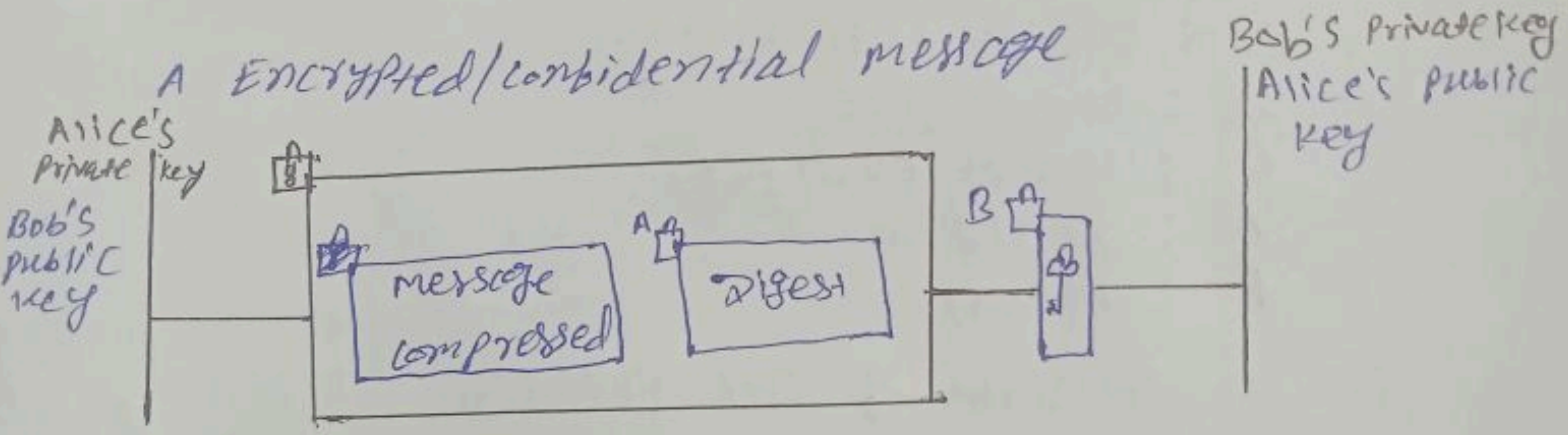
PGP uses a combination of techniques to provide both encryption and authentication.

- Public-key encryption:

  PGP uses a public-key encryption system like RSA. This means you have two keys: a public key and a private key. You share your public key with anyone you want to send encrypted messages to. They can use your public key to encrypt messages that only you, with your private key can decrypt.

· Symmetric Key Encryption:

For faster encryption/decryption of large amounts of data, PGP creates a temporary symmetric key. This symmetric key is then encrypted with the recipient's public key. Only the recipient can decrypt the symmetric key using their private key. The actual message is then encrypted with the decrypted symmetric key.



- A : Digitally signed with Alice's private key
- B : Encrypted with Bob's public key
- : Encrypted with shared session key.

For authentication

Alice creates a digest of the message and signs it with her private key. When Bob receives the message, he verifies the message by using Alice's public key.

Q.5) Draw the OSCAR framework for network forensics methodology and explain the steps involved.

Ans: This methodology consists of five phases or stages that are followed in sequence while managing the life-cycle of the network forensic investigation.

- The methodology is usually referred as the OSCAR methodology.

O : Obtain Information
S : Strategize
C : collect evidence
A : Analyze
R : Report.

So, it consists of five phases.

Phase I : Obtain Information

Obtain the information whether you are law enforcement, internal security staff or a forensic consultant, you will always need to do two things at the begining of an investigation.

i) obtain information about the incident itself
ii) obtain information about the environment.

i) Incident

- Description of what happened
- Date, time and method of incident
- Person involved
- Systems and data involved
- Actions taken since discovery
- Summary of internal discussions
- Incident manager and process
- Legal issues
- Goals

ii) The Environment

The information you gather about the environment will depend on your level of familiarity with it.

Usually you will want to know the following things about the environment.

- Business model
- Legal issues
- Network topology
- Available sources of network evidence
- communication systems.
- The process and procedures for incident response.
- Budget, time & equipment.

Phase-II Strategize:

An investigator should have a strategy for dealing with an incident.

Here are some tips for developing an investigative strategy.

- Understand the goals and time frame for the investigation.
- Identify likely sources of evidence.
- For each source of evidence, estimate the value and cost of obtaining it.
- Prioritize your evidence acquisition.
- Plan the evidence acquisition and analysis processes.

Phase-III Collect evidence

There are three components you must address every time you acquire evidence.

i) Document
ii) Capture
iii) Store/Transport

Document:

All evidence should be carefully documented in logs that record all the steps perform during the evidence collection process.

Capture:

Capturing the evidence itself. This may involve capturing packets and writing them to hard derive copying logs to hard derive or CD.

Store/Transport

Ensure that the evidence is stored securely and maintain the chain of custody. Keep an accurate, signed, verifiable log of the persons who have accessed or possessed the evidence. Since the admissibility of evidence is dependent upon its relevance and reliability, investigators should carefully track the source, method of acquisition and chain of custody.

Phase IV Analyze

During the analysis step, multiples concepts are applied such as

- Correlation: how to correlate data collected from different source and of different type.
- Corroboration: In some cases, the collection of data from multiple sources of network and system log may produce false positives. As a result, evidence should be corroborated across multiple sources to enhance trust levels.
- Interpretation: Investigators may have their own hypothesis that need to be proved before presentation to a court.

Phase-V: Report

It is very important for an investigator to be able to amalgamate all results and steps into a professional and convicing report.

The produced report must be:

- clear and meaningfull for non-technical people such as legal stakeholders, Human resources personnel.
- defendable and accurate.

Q.6> A company named 'Alpha' has noticed many suspicious entries and IP address while observing the log records. Further, some clients have reported that they have been receiving a message prompt, redirecting them to a payment gateway that does not look genuine. You are now the forensic investigator. Explain:

a> How will you ascertain if malware activity has been taken place or malware is present in the systems?

Ans: If malware is present in the systems, I would conduct the following steps.

i> Collect Logs and Artifacts

Gather log records from various sources such as firewalls, intrusion detection systems, antivirus logs and network traffic captures.

ii> Perform malware analysis:

Use antivirus and anti-malware tools to scan the systems for known malware signatures. Also conduct static and dynamic analysis of suspicious files to identify any IOCs, such as file hashes, file name, registry entries.

iii) Check system integrity
iv) verify the integrity of system files and configurations by comparing them against known good copies or system baselines.

b) How will you disinfect malware-affected machines?

Ans: To disinfect malware-affected machines, I would follow these steps.

i) Isolate infected systems.
Immediately disconnect the infected systems from the network to prevent further spread of malware.

ii) Run full system scans using reputable antiviruses and anti-malware software to detect or remove the malware from the infected systems.

iii) Manually remove any identified malicious files,

iv) Apply security patches and updates to the operating system and software to address any vulnerabilities exploited by the malware.

c) How will you ensure that the malware activity has not been spread to all other systems in the network?

Ans: To ensure that malware activity has not spread to all other systems in the network, I would take the following measures.

i) Implement network segmentation to isolate infected systems from the rest of the network
ii) Continuously monitor network traffic for signs of malware.
iii) Deploy endpoint protection solution such as firewalls, IDS and IPS (intrusion prevention systems).
iv) Educate employees.

d) Perform forensic investigation and trace the causes for the incidents.

Ans:

Here are steps for forensic investigation and cause tracing.

1. Log analysis

- Collect and analyze relevant logs from network devices, firewalls, and compromised systems.
- Look for timestamps, source and destination and any indicators of how the malware may have entered the network.

2. Network traffic capture:

Capture and analyze network traffic to identify communication patterns and identify the command-and-control servers the malware might be communicating with.

3. Memory forensics:

Acquire and analyze memory dumps from compromised machines to identify active malware processes.

4. Timeline Development:

Based on the collected evidence, create a timeline of events to understands the sequence of the attack.

5. Identify Root cause:

Analyze the findings to determine how the attackers gained access to the network. This might involve vulnerabilities in software, weak passwords or successful phishing attacks.