JUNE-2023 [END SEM] [6003] - 543 | Solved Paper

Course 2019

Time : $2\frac{1}{2}$ 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 wherever 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.*

Q.1 a) *Describe the Deffie-Hellman key exchange in detail.*
(Refer Q.17 of Chapter - 3) **[6]**

b) *Identify and explain the authentication methods.*
(Refer Q.21 of Chapter - 3) **[6]**

c) *Distinguish between Kerberos and X.509 authentication service.* **[5]**

Ans. :

Protocol	X.509	Kerberos 5
Channel	Many to one	One to one
Encryption	Asymmetric	Symmetric
Algorithm	RSA	DES
RFC	5280	4120
Generate	Certificate	Ticket
Storing	Public key	Private key
Use of public key cryptography	Yes	No
Pros	Authenticity, integrity and non-repudiation	Single-sign on, non-transmission of passwords, strong authentication
Technical deficiencies	Compromise of private keys	Double encryption, session keys, password attacks
Trusted third party	CA	KDC

OR

Q.2 a) *What is digital signature standard ? Explain the DSS approach.* **(Refer Q.33 of Chapter - 3)** [6]

b) *Explain the RSA algorithm in detail with the help of diagram.* **(Refer Q.6 of Chapter - 3)** [6]

c) *Explain message digest algorithm in detail.* **(Refer Q.24 and Q.25 of Chapter - 3)** [5]

Q.3 a) *Explore secure socket layer handshake protocol in detail.* **(Refer Q.17 of Chapter - 4)** [6]

b) *What is VPN ? Explain types of VPN.* **(Refer Q.12 of Chapter - 4)** [6]

c) *Describe IPSec protocol with its components and security services.* **(Refer Q.4 of Chapter - 4)** [6]

OR

Q.4 a) *Distinguish between PGP and S / MIME.* **(Refer Q.27 of Chapter - 4)** [6]

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

Ans. : • Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.

- ISAKMP defines procedures and packet formats to establish, negotiate, modify and delete security associations.
- ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.
- ISAKMP by itself does not dictate a specific key exchange algorithm; rather, ISAKMP consists of a set of message types that enable the use of a variety of key exchange algorithms.
- ISAKMP provides a "cookie" or an Anti-Clogging Token (ACT) to make it easier to handle denial of service and prevents connection hijacking by linking the authentication, key exchange and security association exchanges.

• Fig. 1 shows ISAKMP header format.

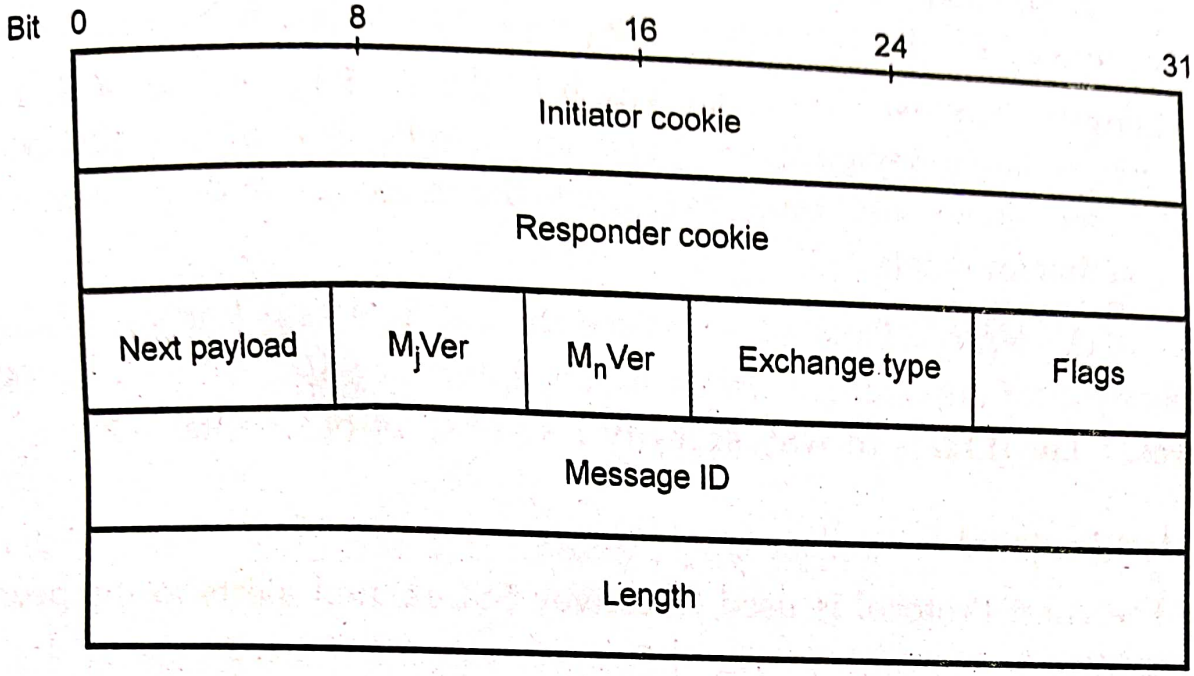


Fig. 1 ISAKMP header format

- **Initiator cookie (8 bytes) :** The cookie of the entity that initiated SA establishment, SA notification or SA deletion.
- **Responder cookie (8 bytes) :** The cookie of the entity that is responding to an SA establishment request, SA notification or SA deletion.
- **Next payload (8 bits) :** Indicates the type of the first payload in the message.
- **Mj version (4 bits) :** The major version of the ISAKMP protocol in use.
- **Mn version (4 bits) :** The minor version of the ISAKMP protocol in use.
- **Exchange type (8 bits) :** Indicates the type of exchange being used. This dictates the message and payload orderings in the ISAKMP exchanges.
- **Flags (8 bits) :** Indicates the options that are set for the ISAKMP exchange.

- **Message ID (4 bytes) :** A unique value used to identify the protocol state during phase 2 negotiations. It is randomly generated by the initiator of the phase 2 negotiation.
- **Length (4 bytes) :** The total length of the ISAKMP header and the encapsulated payloads in bytes. The length field of the ISAKMP header shows the total length of the message and the header together in octets.

c) *Identify threats to web security and figure out how any of two among listed are countered by particular feature of SSL.* [6]

Ans. : For threats to web security : Refer Q.14 of Chapter - 4.

Alert Protocol :

- The Alert Protocol is used to convey SSL-related alerts to the peer entity.
- Alert messages are encrypted and compressed, as specified by the current connection state.
- Alert messages with a level of fatal, result in the immediate termination of the connection.
- In this case, other connections corresponding to the session may continue, however the session identifier must be cancel, preventing the failed session from being used to establish new connections.
- Each message in this protocol consists of two bytes. The first byte takes the value warning (1) or fatal (2) to convey the severity of the message.
- If the level is fatal, SSL immediately terminates the connection. Other connections on the same session may continue, but no new connections on this session may be established. The second byte contains a code that indicates the specific alert.

Q.5 a) *Differentiate packet filtering router and stateful inspection firewall.* [6]

Ans. : Packet filtering router controls data flow to and from a network. Controlling and monitoring network data to assure its validity and compliance is a key role of packet filtering firewalls.

- It examines Access Control Lists (ACLs) to separate packets based on upper-layer protocol ID, source and destination port numbers, source and destination IP addresses and packet transmission route.
- Packet-filtering firewalls are very fast because there is not much logic going behind the decisions they make. They do not do any internal inspection of the traffic.
- Stateful packet inspection firewalls is generally referred to as stateful firewalls and its function on the same general principle as packet filtering firewalls, but they are able to keep track of the traffic at a granular level.
- While a packet filtering firewall only examines an individual packet out of context, a stateful firewall is able to watch the traffic over a given connection, generally defined by the source and destination IP addresses, the ports being used and the already existing network traffic.
- Stateful packet inspection is a technology used by stateful firewalls to determine which packets to allow through the firewall. It works by examining the contents of a data packet and then comparing them against data pertaining to packets that have previously passed through the firewall.
- Stateful packet filtering keeps track of all connections on the network, making sure they are all legitimate. Network-based static packet filtering also examines network connections, but only as they come in, focusing on the data in the packets' headers. This data provides less information to the firewall, limiting it to where it came from and where it is going.
- Also refer Q.4 of Chapter - 5.

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

(Refer Q.6 of Chapter - 5)

c) *List limitations of firewall.* **[5]**

Ans. :

- A firewall cannot prevent individual users with modems from dialing into or out of the network, by passing the firewall altogether.

- Employee misconduct or carelessness cannot be controlled by firewalls.
- Policies involving the use and misuse of passwords and user accounts must be strictly enforced. These are management issues that should be raised during the planning of any security policy but that cannot be solved with firewalls alone.

OR

Q.6 a) *Illustrate screened subnet firewall architecture.*
(Refer Q.5 of Chapter - 5) [6]

b) *List and explain types of Intrusion Detection System (IDS).*
(Refer Q.13 of Chapter - 5) [6]

c) *Identify and explore any two-password management practice.*
(Refer Q.7 of Chapter - 5) [5]

Q.7 a) *Identify and explore the different types of cyber stalker attacks.*
(Refer Q.2 and Q.3 of Chapter - 6) [6]

b) *Illustrate life cycle of cyber forensics ?*
(Refer Q.12 of Chapter - 6) [6]

c) *List VoIP hacking types and explore any 3 ? What are the counter measures for it.* [6]

Ans. : Various categories of remote hacking include :

1. Dial-up hacking
2. PBX (Private Branch Exchange) hacking
3. Voice mail hacking
4. VPN hacking
5. VoIP attacks

1. Dial-up hacking

- Dial-up hacking is possible by both ways analog dial-up hacking and wardialing. This can be done by phone number footprinting, social engineering and corporate websites.

2. PBX hacking

- A PBX connects the internal telephones of a company and saves money on intra-company calls.

- PBX vendor usually tells their customers that they need dial-in access for external support. But it is done often insecurly, leaving a modem always on and connected to PBX. It should be turned off except when needed.

3. Voice-mail hacking

- Voice mail is often important confidential and poorly secured.
- Executives often neglect to pick an unique code for voice mail.
- People often use simple geometrical patterns on the keypads.

4. VPN hacking

- VPN has replaced dial-up as the remote access mechanism.
- VPN connects two computers using tunneling.

OR

Q.8 a) *Who are cyber criminals ? What are types of cyber crimes.* **(Refer Q.5 of Chapter - 6)** **[6]**

b) *What is botnet ? How to protect from botnet ?* **(Refer Q.6 of Chapter - 6)** **[6]**

c) *Explain the terms : i) Virus ii) Phishing iii) Spoofing iv) Phone phishing v) Internet pharming vi) Cyber forensic.* **[6]**

Ans. :

i) **Virus :** A virus is a block of code that inserts copies of itself into other programs. A virus generally carries a payload, which may have nuisance value or serious consequences. To avoid early detection, viruses may delay the performance of functions other than replication. Virus is one type of system threats. A virus is any unauthorized program that is designed to gain access to a computer system. Viruses need other programs to spread. Due to its spreading nature, a virus can cause severe damage to a system.

ii) **Phishing :** Phishing is a type of cyber security attack during which malicious actors send messages pretending to be a trusted person or entity. Phishing messages manipulate a user, causing them to perform actions like installing a malicious file, clicking a malicious link or divulging sensitive information such as access credentials.

iii) **Spoofing :** Spoofing is a type of cyber criminal activity where someone or something forges the sender's information and pretends to be a legitimate source, business, colleague or other trusted contact for the purpose of gaining access to personal information, acquiring money, spreading malware or stealing data.

iv) **Phone phishing :** Phone phishing is a type of phishing attack that uses mobile devices, such as smartphones and tablets, to deliver malicious content. Historically, phishing attacks have been conducted through email messages and web pages. Mobile phishing strategies employ deceitful techniques to trick users on mobile devices into divulging sensitive information. The most common methods include : URL padding, Tiny URLs and screen overlays.

v) **Internet pharming :** Pharming is a type of cyber attack involving the redirection of web traffic from a legitimate site to a fake site for the purpose of stealing usernames, passwords, financial data and other personal information.

vi) **Cyber forensic :** Cyber forensics is the science of collecting, inspecting, interpreting, reporting and presenting computer-related electronic evidence. Evidence can be found on the hard drive or in deleted files. It is the process of examining, acquiring and analyzing data from a system or device so that it can be transcribed into physical documentation and presented in court.

END...

Unit III

3 Public Key and Management

3.1 : Public Key Cryptography

Q.1 What are the essential ingredients of a symmetric cipher ?

Ans. : A public key encryption scheme has six ingredients. Fig. Q.1.1 shows public key cryptography. (See Fig. Q.1.1 on next page)

1. **Plaintext :** It is input to algorithm and in a readable message or data.
2. **Encryption algorithm :** It performs various transformations on the plaintext.
3. **Public and private keys :** One key is used for encryption and other is used for decryption.
4. **Ciphertext :** This is the scrambled message produced as output. It depends on the plaintext and the key.
5. **Decryption algorithm :** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

- The essential steps are the following :

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register. This is the public key. The companion key is kept private.
3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4. Alice decrypts the message using her private key.

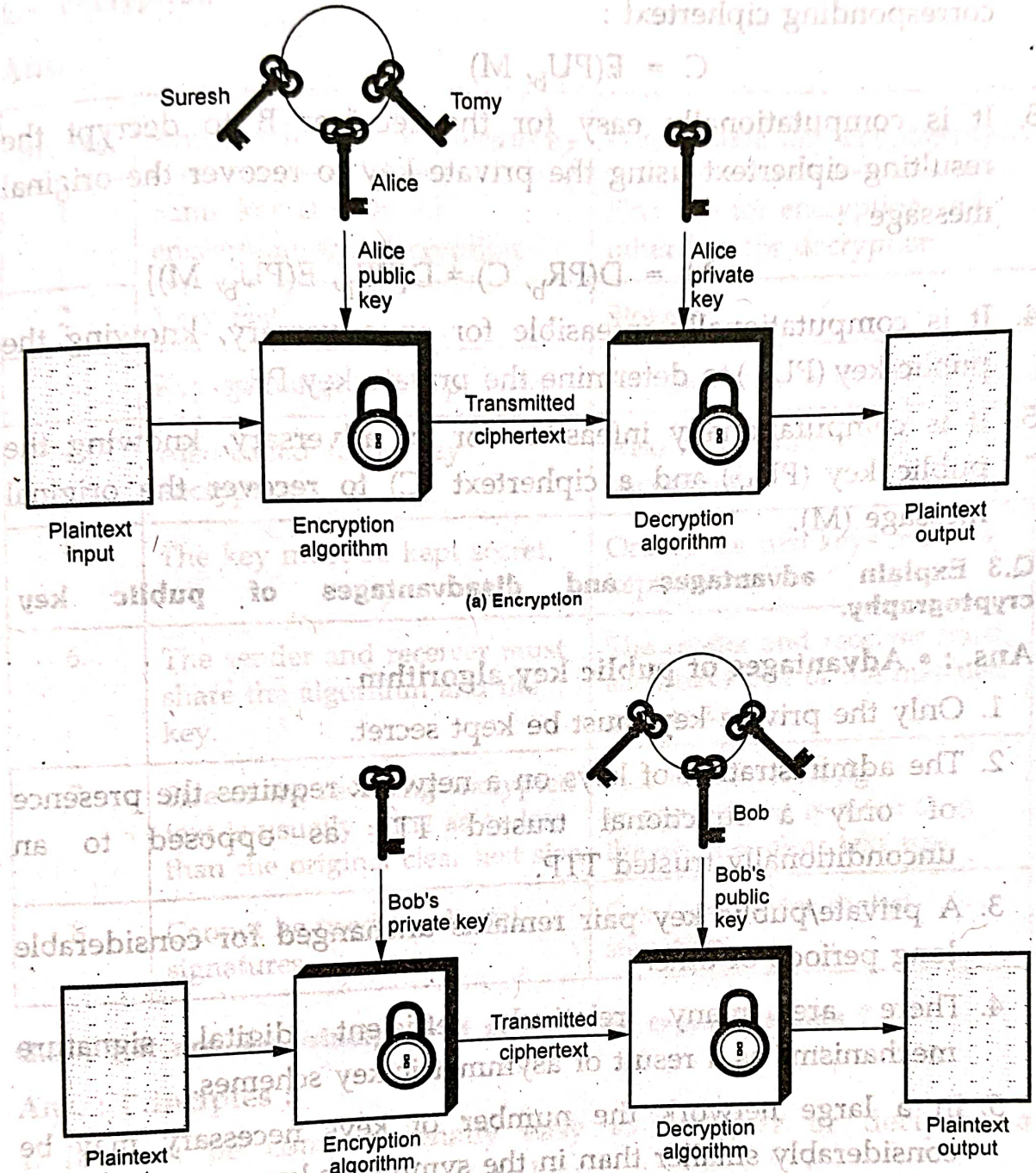


Fig. Q.1.1 Public key cryptography

Q.2 Explain requirement of public key cryptography.

Ans. : Requirements for public key cryptography

1. It is computationally easy for a party B to generate a pair.

2. It is computationally easy for a sender A, to generate the corresponding ciphertext :

$$C = E(PU_b, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message :

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

4. It is computationally infeasible for an adversary, knowing the public key (PU_b) to determine the private key PR_b.
5. It is computationally infeasible for an adversary, knowing the public key (PU_b) and a ciphertext (C) to recover the original message (M).

Q.3 Explain advantages and disadvantages of public key cryptography.

Ans. : • Advantages of public key algorithm

1. Only the private key must be kept secret.
2. The administration of keys on a network requires the presence of only a functional trusted TTP as opposed to an unconditionally trusted TTP.
3. A private/public key pair remains unchanged for considerable long periods of time.
4. There are many relatively efficient digital signature mechanisms as a result of asymmetric-key schemes.
5. In a large network the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

• Disadvantages of public key algorithm

1. Slower throughput rates than the best known symmetric-key schemes.
2. Large key size.
3. No asymmetric-key scheme has been proven to be secure.
4. Lack of extensive history.

Q.4 Compare between symmetric key encryption and asymmetric key encryption.

Ans. :

Sr. No.	Symmetric key cryptography	Asymmetric key cryptography
1.	Same key is used for encryption and decryption.	One key for encryption and other key for decryption.
2.	Very fast	Slower
3.	Key exchange is big problem.	Key exchange is not a problem.
4.	Also called **secret key** encryption.	Also called **public key** encryption.
5.	The key must be kept secret.	One of the two keys must be kept secret.
6.	The sender and receiver must share the algorithm and the key.	The sender and receiver must each have one of the matched pair of keys.
7.	Size of the resulting encrypted text is usually same as or less than the original clear text size.	Size of the resulting encrypted text is more than the original clear text size.
8.	Cannot be used for digital signatures.	Can be used for digital signature.

Q.5 What are the principles of public key cryptosystems ?

Ans. : Principles :

1. It must be computationally easy to encipher or decipher a message given the appropriate key.
2. It must be computationally infeasible to derive the private key from the public key.
3. It must be computationally infeasible to determine the private key from a chosen plaintext attack.

3.2 : RSA Algorithm

Q.6 Explain the operation of RSA public key encryption algorithm.

OR What is public key cryptography ? Explain RSA algorithm used for public key cryptography.

Ans. : • Public key cryptography means one key is used for encryption and other key for decryption. The public key is accessed to all participants and private key is generated locally by each participant.

RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and n – 1 for some n. RSA algorithm is public key encryption type algorithm. In this algorithm, one user uses a public key and other user uses a secret (private key) key. In the RSA algorithm each station independently and randomly chooses two large primes p and q number and multiplies them to produce $n = p \times q$ which is the modulus used in the arithmetic calculations of the algorithm.

Key generation :

1) Pick two large prime numbers p and q, $p \neq q$;
2) Calculate $n = p \times q$;
3) Calculate $\phi(n) = (p - 1)(q - 1)$;
4) Pick e, so that gcd $(e, \phi(n)) = 1$, $1 < e < \phi(n)$;
5) Calculate d, so that $d \cdot e \bmod \phi(n) = 1$, i.e. d is the multiplicative inverse of e in mod $\phi(n)$;
6) Get public key as $K_U = \{e, n\}$;
7) Get private key as $K_R = \{d, n\}$.

Encryption : For plaintext block $P < n$, its ciphertext $C = P^e \bmod n$.

Decryption : For ciphertext block C, its plaintext is $P = C^d \bmod n$.

The modulus n must be selected in such a manner that the following is guaranteed :

$$(M^e)^d) \equiv M^{ed} \equiv M \pmod n$$

We want this guarantee because $C = M^e \bmod m$ is the encrypted form of the message integer M and decryption is carried out by $C^d \bmod n$.

We also need to ensure that n is not factorizable by one of the modern integer factorization algorithms.

- As we have seen from the RSA design, RSA algorithm uses modular exponentiation operation. For $n = p \cdot q$, e which is relatively prime to $\phi(n)$ has exponential inverse in mod n.
- Its exponential inverse d can be calculated as the multiplicative inverse of e in mod $\phi(n)$. The reason is illustrated as follows : Based on Euler's theorem, for y which satisfies $y \bmod \phi(n) = 1$, the following equation holds :
  $x^y \bmod n = x \bmod n$
  AS $d \cdot e \bmod \phi(n) = 1$, we have that $p^{ed} \equiv P \bmod n$. So the correctness of RSA cryptosystem is shown as follows :

Encyption : $C = P^e \bmod n$;

Decryption : $P = C^d \bmod n = (P^e)^d \bmod n = P^{ed} \bmod n = P \bmod n = P$.

Q.7 For the given parameters 'P' = 3 and 'Q' = 19 find the value of 'e' and 'd' using RSA algorithm and encrypt message 'M' = 6.

Ans. : $P = 3 \qquad Q = 19$

$N = PQ$

$= 3 \times 19$

$N = 57$

Calculate $\phi(n) = (P - 1)(Q - 1)$

$= (3 - 1)(19 - 1)$

$= 36$

Public key 'e' is calculated by using Euclid algorithm. Using 36, GCD is calculated and 5 and 7 gives GCD = 1

So you can select e = 5 or 7. Here we selected e = 7

So public key (7, 57)

Private key generation (d) :

Determine d such that $ed = 1 \bmod \phi(n)$

$$7d = 1 \pmod{36}$$

$$7 \times 31 = 1 \pmod{36}$$

So d = 31

Encryption of message :

Ciphertext (C) $= M^e \bmod n$

$= 6^7 \bmod 57$

$C = 9$

Q.8 Explain RSA algorithm with suitable example.

Ans. : Refer Q.6 and Q.7.

Q.9 Use RSA algorithm to encrypt the plaintext " 3 " use following parameters p = 11, q = 3, e = 13.

Ans. : p = 11, q = 3, e = 13

Plaintext = 3

$$N = p \times q = 11 \times 3 = 33$$

$$\phi(n) = (p-1)(q-1) = (11-1)(3-1) = 20$$

Given $e = 13;$

Determine d such that

$$ed = 1 \bmod \phi(n)$$

$$13\,d = 1 \bmod 20$$

$$13 \times 17 = 1 \bmod 20$$

$$221 = 1 \bmod 20$$

So $d = 17$

Ciphertext $(C) = M^e \bmod (n)$

$C = 3^{13} \bmod 33 \quad C = 27$

Q.10 Perform encryption and decryption using RSA algorithm. p = 7, q = 11, e = 17 and M = 8.

Ans. : RSA algorithm :

$$N = p \times q = 7 \times 11$$
$$= 77$$

$$\text{Calculate } \phi(n) = (p - 1)(q - 1) = (7 - 1)(11 - 1)$$
$$= 6 \times 10$$
$$= 60$$

So, $e = 17$

Determine d such that

$$ed = 1 \bmod \phi(n)$$
$$17d = 1 \bmod 60$$

According to GCD :

$$60 = 17 * 3 + 9$$
$$17 = 9 * 1 + 8$$
$$9 = 8 * 1 + 1$$
$$8 = 1 * 8 + 0$$

Therefore, we have :

$$1 = 9 - 8$$
$$= 9 - (17 - 9)$$
$$= 9 - (17 - (60 - 17 * 3))$$
$$= 60 - 17 * 3 - (17 - 60 + 17 * 3)$$
$$= 60 - 17 * 3 + 60 - 17 * 4$$
$$= 60 * 2 - 17 * 7$$

Hence, we get,

$$d = e^{-1} \bmod f(n)$$
$$= e^{-1} \bmod 60$$
$$= -7 \bmod 60$$
$$= (53 - 60) \bmod 60$$

$= 53$

So, the public key is {17, 77} and the private key is {53, 77}

Encryption :

$$\text{Ciphertext (C)} = M^e \bmod N$$
$$= (8)^{17} \bmod 77$$
$$C = 57$$

Q.11 In a public key cryptosystem using RSA, given N = 187 and the encryption key (E) as 17, find out the corresponding private key (D).

Ans. :

$$N = 187$$
$$N = p \times q = 17 \times 11$$
$$N = 187$$

So

$$p = 17, \quad q = 11$$
$$\phi(n) = (p - 1) \times (q - 1)$$
$$= (17 - 1) \times (11 - 1) = 160$$
$$ED = 1 \bmod \phi(n)$$
$$17\ d = 1 \bmod 160$$
$$d = 113$$

Q.12 Let the given data be - Prime numbers p = 11, q = 19 and the plain text to be sent is 4. Assume public key e as 23. Using RSA algorithm determine the cipher text for the given plain text. Also perform the reverse process of finding the plain text. Also perform the reverse process of finding the plain text from the cipher text.

Ans. : Given $p = 11$, $q = 19$, plain text $(m) = 40$,

Public key $e = 23$

$$n = p \times q = 11 \times 19 = 209$$
$$\phi(n) = (p - 1) \times (q - 1)$$
$$= (11 - 1) \times (19 - 1) = 180$$

Encryption :

$$C = M^e \pmod n$$
$$= (40)^{23} \bmod 180$$
$$C = 160$$

Q.13 Given two prime numbers P = 17 and Q = 29 find out N, E and D in an RSA encryption process.

Ans. : Given data : P = 17, Q = 27

$$N = P \times Q = 17 \times 27$$
$$N = 459$$
$$\phi(N) = (P - 1) \times (Q - 1) = (17 - 1) \times (27 - 1)$$
$$\phi(N) = 416$$

- The number e is allowed to be any number, which has no factors in common with this new number 416
- We can break 416 into a bunch of prime numbers multiplied together : $416 = 2 \times 2 \times 2 \times 2 \times 2 \times 13$
- So there are lots of possibilities. Let's suppose chooses e = 5.

$$e \times d = 1 \bmod (\phi(N))$$
$$5 \times d = 1 \bmod (416)$$
$$d = 83$$

3.3 : Key Distribution

Q.14 What are the methods used in key distribution in public key cryptography ?

OR Explain various public key distribution approaches.

OR What are different approaches of public key distribution ? Explain any one.

Ans. : Different methods have been proposed for the distribution of public keys. These are,

1. Public announcement
2. Publicly available directory
3. Public key authority
4. Public key certificates.

- **Public announcement :** In public key algorithm, any participant can send his or her public key to any other participant or broadcast the key to the community at large.
- Because of the growing popularity of PGP, which makes use of RSA, many PGP users have adopted the practice of appending their public key to messages that they send to public forums, such as USENET new groups and Internet mailing lists.
- **Public available directory :** Greater degree of security can be achieved by maintaining a publicly available dynamic directory of public keys. Maintenance and distribution of the public directory would have to be the responsibility of some trusted entity or organization.
- **Public key authority :** User uses third party for key distribution.
- **Public key certificates :** Certificates can be used by participants to exchange keys without contacting a public key authority. Certificate consists of a public key plus an identifier of the key owner, with the whole block signed by a trusted third party.
- The third party is a certificate authority, such as government agency or a financial institution, that is trusted by the user community.
- A user can present his or her public key to the authority in a secure manner, and obtain a certificate. The user can then publish the certificate.

Q.15 What is PKI ? List benefits and limitation of PKI.

Ans. : • Public Key Infrastructure (PKI) is a well-known technology that can be used to establish identities, encrypt information and digitally sign documents.

- PKI identifies and manages relationships of parties in an electronic exchange, serving a wide array of security needs including access control, confidentiality, integrity, authentication and non-repudiation.

- PKI also uses unique Digital Certificates (DC) to secure eCommerce, email, data exchange and Virtual Private Networks (VPN) and intranets and is also used to verify the identity and privileges of each user.
- The Certificate Authority (CA) provides a full life-cycle management of public keys and certificates, including issuance, authentication, storage, retrieval, backup, recovery, updating and revocation to the PKI.
- All users of PKI must have a registered identity, which is stored in a digital certificate issued by a CA.
- Remote users and sites using public private keys and public key certificates can authenticate each other with a high degree of confidence.
- Authentication is dependent on three conditions :
  1. It must be established that each party have a private key that has not been stolen or copied from the owner.
  2. The certificate must be issued to the owner in accord with the stated policy of the certificate issuer.
  3. The policies of the certificate issuer must be satisfactory to the parties so as to verify identity.

Benefits of PKI

1. **Confidential communication** : Only intended recipients can read files.
2. **Data integrity** : Guarantees files are unaltered during transmission.
3. **Authentication** : Ensures that parties involved are who they claim to be.
4. **Non-repudiation** : Prevents individuals from denying.

Limitation of PKI

The problems encountered deploying a PKI can be categorized as follows :

1. Public key infrastructure is new
2. Lack of standards
3. Shortage of trained personnel
4. Public key infrastructure is mostly about policies.

Q.16 What is key distribution ? Explain in detail.

Ans. : • For symmetric encryption to work, the two parties to an exchange must share the same key, and that key must be protected from access by others. **Key distribution** refers to the means of delivering a key to two parties who wish to exchange data, without allowing others to see the key.

- For two parties A and B, key distribution can be achieved in a number of ways, as follows.
  1. User A can select a key and physically deliver it to user B.
  2. A third party can select the key and physically deliver it to user A and user B.
  3. If user A and user B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
  4. If user A and user B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to user A and user B.
- For manual delivery of key, **options 1 and 2** are used. These options are suitable for **link encryption.**
- Option 3 is suitable for link encryption or end-to-end encryption.
- For end-to-end encryption, some variation on option 4 has been widely adopted.

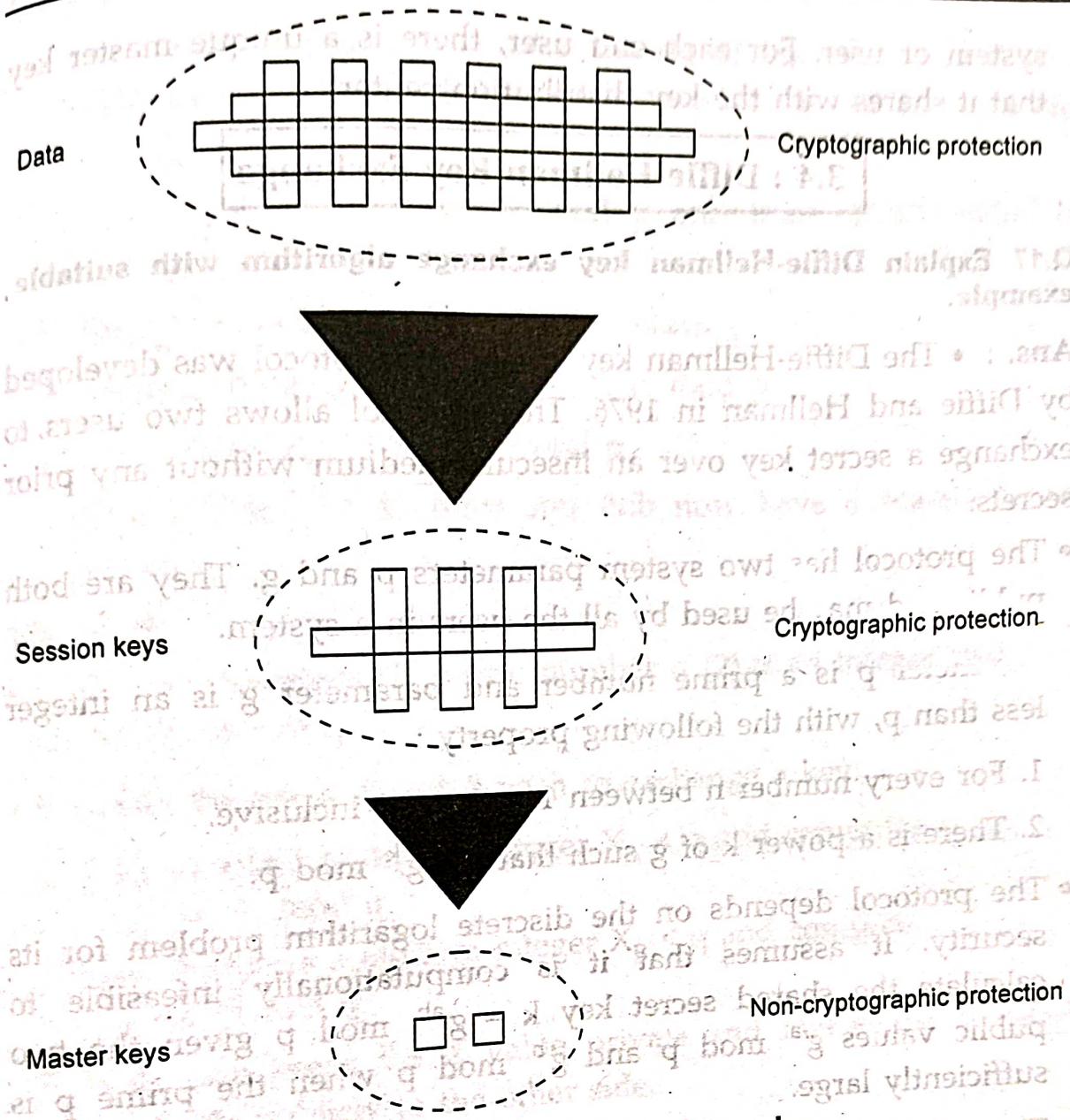


Fig. Q.16.1 Use of a key hierarchy

- The use of a key distribution center is based on the use of a hierarchy of keys. Minimum two levels of keys are used. Fig. Q.16.1 shows the use of a key hierarchy.
- Communication between end systems is encrypted using a temporary key, often referred to as a **session key**. The **session key** is used for the duration of a logical connection, such as a frame relay connection, or transport connection and then discarded.
- Session keys are transmitted in encrypted form, using a **master key** that is shared by the key distribution center and an end

system or user. For each end user, there is a unique master key that it shares with the key distribution center.

3.4 : Diffie-Hellman Key Exchange

Q.17 Explain Diffie-Hellman key exchange algorithm with suitable example.

Ans. : • The Diffie-Hellman key agreement protocol was developed by Diffie and Hellman in 1976. This protocol allows two users to exchange a secret key over an insecure medium without any prior secrets.

- The protocol has two system parameters p and g. They are both public and may be used by all the users in a system.

  Parameter p is a prime number and parameter g is an integer less than p, with the following property :

  1. For every number n between 1 and p – 1 inclusive.
  2. There is a power k of g such that $n = g^k \bmod p$.

- The protocol depends on the discrete logarithm problem for its security. It assumes that it is computationally infeasible to calculate the shared secret key $k = g^{ab} \bmod p$ given the two public values $g^a \bmod p$ and $g^b \bmod p$ when the prime p is sufficiently large.

- The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack. This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants. Possible solutions include the use of digital signatures and other protocol variants.

- Suppose Alice and Bob want to agree on a shared secret key using the Diffie-Hellman key agreement protocol. They proceed as follows :

  1. First, Alice generates a random private value a and Bob generates a random private value b.

2. Both a and b are drawn from the set of integers. They derive their public values using parameters p and g and their private values.
3. Alice's public value is $g^a \bmod p$ and Bob's public value is $g^b \bmod p$.
4. They then exchange their public values.
5. Finally, Alice computes $g^{ab} = (g^b)^a \bmod p$.
6. Bob computes $g^{ba} = (g^a)^b \bmod p$.
7. Since $g^{ab} = g^{ba} = k$, Alice and Bob now have a shared secret key k.

Algorithm :

- Select two numbers (1) prime number q (2) α an integer that primitive root of q.
- Suppose the users A and B wish to exchange a key.

1. User A select a random integer $X_A < q$ and computes $Y_A = \alpha^{X_A} \bmod q$.
2. User B selects a random integer $X_B < q$ and compute $Y_B = \alpha^{X_B} \bmod q$.
3. Both side keeps the X value private and makes the Y value available publicly to the other side.
4. User A computes the key as $K = (Y_B)^{X_B} \bmod q$.
5. User B computes the key as $K = (Y_A)^{X_B} \bmod q$.

- Both side gets same results :

$$\begin{aligned} K &= (Y_B)^{X_A} \bmod q \\ &= (\alpha^{X_B} \bmod q)^{X_A} \bmod q \\ &= (\alpha^{X_B})^{X_A} \bmod q \\ &= \alpha^{X_B X_A} \bmod q \\ &= (\alpha^{X_A} \bmod q)^{X_B} \bmod q \\ &= (Y_A)^{X_B} \bmod q \end{aligned}$$

Example

- Key exchange is based on the use of the prime number and a primitive root of prime number.
- Prime number $q = 353$

  Primitive root $\alpha = 3$
- A and B select secret keys.

  $X_A = 97$ $X_B = 233$
- Calculates the public keys

A computes $Y_A = \alpha^{X_A} \bmod q$

$= (3)^{97} \bmod 353$

$= (1.9080 \times 10^{97}) \bmod 353 = 40$

B computes $Y_B = \alpha^{X_B} \bmod q$

$= (3)^{233} \bmod 353$

$= (1.4765 \times 10^{111}) \bmod 353 = 248$

- After they exchange public keys, each can compute the common *secret key.*

A computes $K = (Y_B)^{X_A} \bmod q = (248)^{97} \bmod 353$

$= (1.8273 \times 10^{232}) \bmod 353 = 160$

B computes $K = (Y_A)^{X_B} \bmod q = (40)^{233} \bmod 353$

$= (1.9053 \times 10^{373}) \bmod 353 = 160$

Q.18 Consider a Diffie-Hellman scheme with a common prime $q = 11$ and a primitive root $\alpha = 2$.
i) If user A has the public key $Y_A = 9$; what is A's private key X_A ?
ii) If user A has a public key $Y_A = 3$; what is the shared secret key X_A ?

Ans. : i) $q = 11$, $\alpha = 2$, $Y_A = 9$, $X_A = ?$

$2 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$

$2^6 \bmod 11 = 9$

$2^7 \bmod 11 = 7$

$2^8 \bmod 11 = 3$

Since $2^e \bmod 11$ for $0 < i < 11$ contains all numbers from 1 to 11 – 1, the size of this set is equal to $\phi(q)$, the order of q.

From the above values $2^6 \bmod 11 = 9$ therefore $X_A = 6$

ii) From the above values

$$\alpha^{X_A} \bmod 11 = Y_A$$

$$2^{X_A} \bmod 11 = 3$$

$$2^{X_8} \bmod 11 = 3$$

$\therefore$ $X_A = 8$

3.5 : Elliptic Curve

Q.19 What are elliptic curve cryptosystems ? Explain with example.

Ans. : • An elliptic curve is a set of points on the coordinate plane satisfying an equation of the form $y^2 + axy + by = x^3 + cx^2 + dx + e$. In order to use elliptic curves for say, Difie-Hellman, there needs to be some mathematical operation on two points in the set that will always produce a point also in the set.

- ECC can be done with at least two types of arithmetic, each of which gives different definitions of multiplication. The two types of arithmetic are,
  1. Zp arithmetic
  2. GF (2^n) arithmetic, which can be done with shifts and $\oplus$ s.
- To form a cryptographic system using elliptic curves, we need to find a hard problem corresponding to factoring the product of two primes or taking the discrete logarithm.

- Consider the equation Q = KP where Q, P ∈ $E_P(a, b)$ and K < P. It is relatively easy to calculate Q given K and P, but it is relatively hard to determine K given Q and P. This is called the **discrete logarithm problem for elliptic curves.**

Q.20 Consider the group $E_{23}(9, 17)$. This is the group defined by the equation $y^2 \bmod 23 = (x^3 + 9x + 17) \bmod 23$. What is the discrete logarithm K of Q = (4, 5) to the base P = (16, 5) ?

Ans. : The brute-force method is to compute multiples of P until Q is found.

Thus,

P = (16, 5)

2P = (20, 20)

3P = (14, 14)

4P = (19, 20)

5P = (13, 10)

6P = (7, 3)

7P = (8, 7)

8P = (12, 17)

9P = (4, 5)

Because 9P = (4, 5) = Q, the discrete logarithm Q = (4, 5) to the base P = (16, 5) is K = 9.

3.6 : Authentication Methods

Q.21 What is authentication ? Explain various methods for authentication.

Ans. : • Authentication techniques are used to verify identity. The authentication of authorized users prevents unauthorized users from gaining access to corporate information systems.

- Authentication method is of validating the identity of user, service or application. The use of authentication mechanisms can

also prevent authorized users from accessing information that they are not authorized to view.

- Various methods for authentication are as follows :

1. One way authentication :

- It involves single transfer of information from one user to other. Client authenticates itself to the server. The server may or may not be authenticated to the client. This is referred to as one way authentication.
- Password is a front line protection against the unauthorized access to the system. Passwords authenticate the identifier (ID) and provide security to the system. Therefore almost all systems are password protected.
- Encrypted passwords : Instead of storing the names and passwords in plain text form, they are encrypted and stored in cipher text form in the table.
- One time passwords : Set of paired passwords solve the problem of password sniffing. When a session begins, the system randomly selects and presents one part of a password pair; user must supply the other part

2. Certificate based authentication :

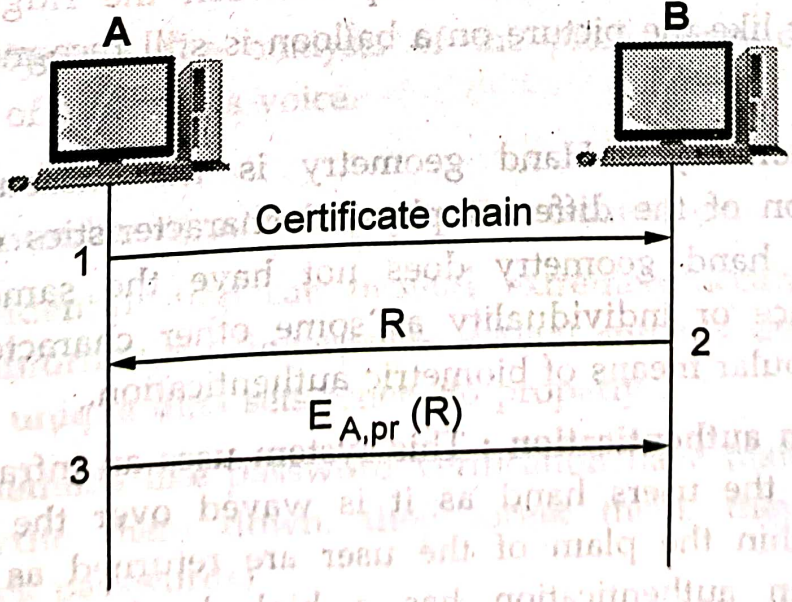


Fig. Q.21.1 Certificate based authentication

- Client have a public key certificate. Fig. Q.21.1 shows the certificate based authentication.
- A sends his certificate in message 1.
- B performs certain checks which includes principal name, validity period, certificate authority etc.
- B then sends his challenge i.e a nonce R.
- A responds by encrypting the challenge with his private key.
- When B receives $E_{A,pr}(R)$, he decrypts it with A's public key and compares it with the nonce he transmitted in message 2.
- It they match, he concludes that A has used the private key corresponding to the public key in his certificate.

Q.22 Explain biometric authentication.

Ans. : Biometric identification systems can be grouped based on the main physical characteristic that lends itself to biometric identification.

- **Fingerprint identification :** Fingerprint ridges are formed in the womb; you have fingerprints by the fourth month of fetal development. Once formed, fingerprint ridges are like a picture on the surface of a balloon. As the person ages, the fingers do get larger. However, the relationship between the ridges stays the same, just like the picture on a balloon is still recognizable as the balloon is inflated.
- **Hand geometry :** Hand geometry is the measurement and comparison of the different physical characteristics of the hand. Although hand geometry does not have the same degree of permanence or individuality as some other characteristics, it is still a popular means of biometric authentication.
- **Palm vein authentication :** This system uses an infrared beam to penetrate the users hand as it is waved over the system; the veins within the plam of the user are returned as black lines. Palm vein authentication has a high level of authentication

accuracy due to the complexity of vein patterns of the palm. Because the palm vein patterns are internal to the body, this would be a difficult system to counterfeit. Also, the system is contactless and therefore hygienic for use in public areas.

- **Retina scan :** A retina scan provides an analysis of the capillary blood vessels located in the back of the eye; the pattern remains the same throughout life. A scan uses a low intensity light to take an image of the pattern formed by the blood vessels. Retina scans were first suggested in the 1930's.
- **Iris scan :** An iris scan provides an analysis of the rings, furrows and freckles in the colored ring that surrounds the pupil of the eye. More than 200 points are used for comparison.
- **Face recognition :** Facial characteristics are depends on the size and shape of facial characteristics, and their relationship to each other. Although this method is the one that human beings have always used with each other, it is not easy to automate it. Typically, this method uses relative distances between common landmarks on the face to generate a unique "faceprint".
- **Signature :** Although the way you sign your name does change over time, and can be consciously changed to some extent, it provides a basic means of identification.
- **Voice analysis :** The analysis of the pitch, tone, cadence and frequency of a person's voice.

Advantages

There are a number of advantages to this technology,

- Biometric identification can provide extremely accurate, secured access to information; fingerprints, retinal and iris scan produce absolutely unique data sets when do properly.
- Current methods like password verification have many problems (people write them down, they forget them, they make up easy-to-hack passwords).

- Automated biometric identification can be done very rapidly and uniformly, with a minimum of training.
- Your identity can be verified without resort to documents that may be stolen, lost or altered.

Q.23 Write short note on extensible authentication protocol.

Ans. : • Extensible Authentication Protocol is a universal authentication framework frequently used in wireless networks and Point-to-Point connections.

- The Extensible Authentication Protocol is a protocol commonly used in 802.1x to authenticate users.
- WPA and WPA2 standard has officially adopted five EAP types as its official authentication mechanisms.
- EAP is a way for a supplicant to authenticate, usually against a back-end RADIUS server. EAP comes from the dial access world and PPP.
- EAP sits inside PPP's authentication protocol. It provides a generalized framework for all sorts of authentication methods.
- EAP is supposed **to head off** proprietary authentication systems and let everything from **passwords to challenge-response tokens** and **PKI certificates** work smoothly.
- With a **standardized EAP,** interoperability and compatibility across authentication methods becomes simpler.
- Only the client and the authentication server have to be coordinated.
- By supporting **EAP authentication,** a RAS server **(in wireless this is the AP) gets out of** the business of actively participating in the authentication dialog.
- EAP supports multiple authentication methods, such as token card, Kerberos, one-time password, certificate, public key authentication, and smart card.

3.7 : Message Digest

Q.24 Explain operation of MD5 message digest algorithm.

Ans. : • Suppose if we have b-bit message as input, and that we wish to find its message digest. Here b is an arbitrary non-negative integer; b may be zero, it need not be a multiple of eight, and it may be arbitrarily large. The bits of the message written down as follows :

m_0 m_1 ... m_{b-1}

• The following five steps are performed to compute the message digest of the message.

Step 1 : Append Padding Bits

• The message is "padded" so that its length is congruent to 448, modulo 512. Padding is always performed, even if the length of the message is already congruent to 448, modulo 512.

• Padding is performed as follows : A single "1" bit is appended to the message and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448, modulo 512. In all, at least one bit and at most 512 bits are appended.

Step 2 : Append Length

• A 64-bit representation of b is appended to the result of the previous step. In the unlikely event that b is greater than 2^{64} and then only the low-order 64 bits of b are used.

• At this point the resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. Equivalently, this message has a length that is an exact multiple of 16 (32-bit) words.

• Let M[0 ... N-1] denote the words of the resulting message, where N is a multiple of 16.

Step 3 : Initialize MD Buffer

- A four-word buffer (A, B, C and D) is used to compute the message digest. Here each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal :

  Word A : 01 23 45 67

  Word B : 89 ab cd ef

  Word C : fe dc ba 98

  Word D : 76 54 32 10

Step 4 : Process Message in 16-Word Blocks

- We first define four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word.

  F(X,Y,Z) = XY v not(X) Z

  G(X,Y,Z) = XZ v Y not(Z)

  H(X,Y,Z) = X xor Y xor Z

  I(X,Y,Z) = Y xor (X v not(Z))

- In each bit position F acts as a conditional: if X then Y else Z. The function F could have been defined using + instead of v since XY and not(X)Z will never have 1's in the same bit position.
- It is interesting to note that if the bits of X, Y, and Z are independent and unbiased, the each bit of F(X, Y, Z) will be independent and unbiased.
- The functions G, H and I are similar to the function F, in that they act in "bitwise parallel" to produce their output from the bits of X, Y, and Z, in such a manner that if the corresponding bits of X, Y, and Z are independent and unbiased, then each bit of G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) will be independent and unbiased.
- This step uses a 64-element table T[1 ... 64] constructed from the sine function. Let T[i] denote the i-th element of the table, which

is equal to the integer part of 4294967296 times abs(sin(i)), where i is in radians.

Step 5 : Output

- The message digest produced as output is A, B, C, and D. That is, we begin with the low-order byte of A, and end with the high-order byte of D.

Q.25 What is message digest ? Compare MD5 with SHA-1.

Ans. : Message digest : • A message-digest algorithm is also called **a hash function** or a cryptographic hash function.

- It accepts a message as input and generates a fixed-length output, which is generally less than the length of the input message. The output is called a **hash value**, a fingerprint or a message digest.
- Message Digest 5 (MD5) processes the input text in 512-bit blocks. These blocks are further divided into 16 32-bit sub blocks.
- MD5 is a 128-bit hash.
- The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem such as RSA.

Sr. No.	MD5	SHA
1.	MD length is 128-bits	Length is 160-bits
2.	Speed is faster than SHA	Slower than MD5
3.	Number of iteration is 64	Number of iteration is 80
4.	Buffer space is 128-bits	Buffer space is 160-bits
5.	MD5 is vulnerable to cryptanalytic attacks	SHA-1 appears not to be vulnerable to cryptanalytic attack
6.	MD5 uses a little endian scheme	SHA-1 uses a big endian scheme

7.	Simple to implement and do not need any large programs or complex table	Simple to implement and do not need any large programs or complex table.
8.	No limit on maximum message size.	Maximum message size is $2^{64} - 1$ bits.

Q.26 Explain in details the need and implementation of one way hash function (MD5).

Ans. : MD5 is used in many situations where a potentially long message needs to be processed and/or compared quickly. The most common application is the creation and verification of digital signatures.

Also Refer Q.24 Chapter - 3.

3.8 : Kerberos

Q.27 Explain the operation of Kerberos.

OR What is Kerberos ? Explain its operation.

Ans. : • Kerberos is an authentication protocol. Kerberos allows centralized authentication schemes among the users and sever.

• Kerberos does not employ public - key encryption but uses symmetric encryption.

Simple Authentication Dialogue

• For a secure transaction, server should confirm the client and its request. In unprotected network it creates burden on server, therefore an Authentication Server (AS) is used. The Authentication Server (AS) maintains password of all users in centralized database. Also the authentication server shares a unique secret key with each server.

• Let,

Client is represented as C

Authentication server is represented as AS

Server is represented as V

Identifier of user on C is represented as ID_C

Identifier of V is represented as ID_V

Passward of user on C is P_C

Network address of C is represented as AD_C

Secret encryption key shared by AS and V is K_V

Then consider a hypothetical dialogue.

	Sender and receiver		Contents of message
1.	$C \rightarrow AS$	:	$ID_C \| P_C \| ID_V$
2.	$AS \rightarrow C$	:	Ticket
3.	$C \rightarrow V$	:	$ID_C \|$ Ticket
4.	Ticket	=	$E [K_V , (ID_C \| AD_C \| ID_V)]$

Explanation

1. **Client Clogs on to workstation requesting to access to server V :** The workstation requests user's passward and sends message to AS including user ID + server ID + user passward. The AS checks this message with database and verifies it.
2. **AS issues ticket :** On verifying the tests. AS issues ticket containing user ID + server ID + network address.
3. **Client C applies server V :** With this ticket, client C asks server V for access. Server V decrypts the ticket and verify the aunthenticity of data then grants the requested service. In above hypothetical dialogue, symbol || represents concatenation.

Secure Authentication Dialogue

- Kerberos version 4 protocol ensures secure authentication dialogue involving three sessions.

i] Authentication Service - Exchange to obtain ticket-granting ticket.

ii] Ticket-granting Service - Exchange to obtain service granting ticket.

iii] Client/server authentication - Exchange to obtain service.

- Each of the above session has two steps, as shown in table below

Session	Step	Sender-Receiver
[i]	1. 2.	C → AS AS → C
[ii]	3. 4.	C → TGS (Ticket-granting server) TGS → C
[iii]	5.	C → V V → C

- Fig. Q.27.1 shows how the steps are executed in Kerberos version 4.

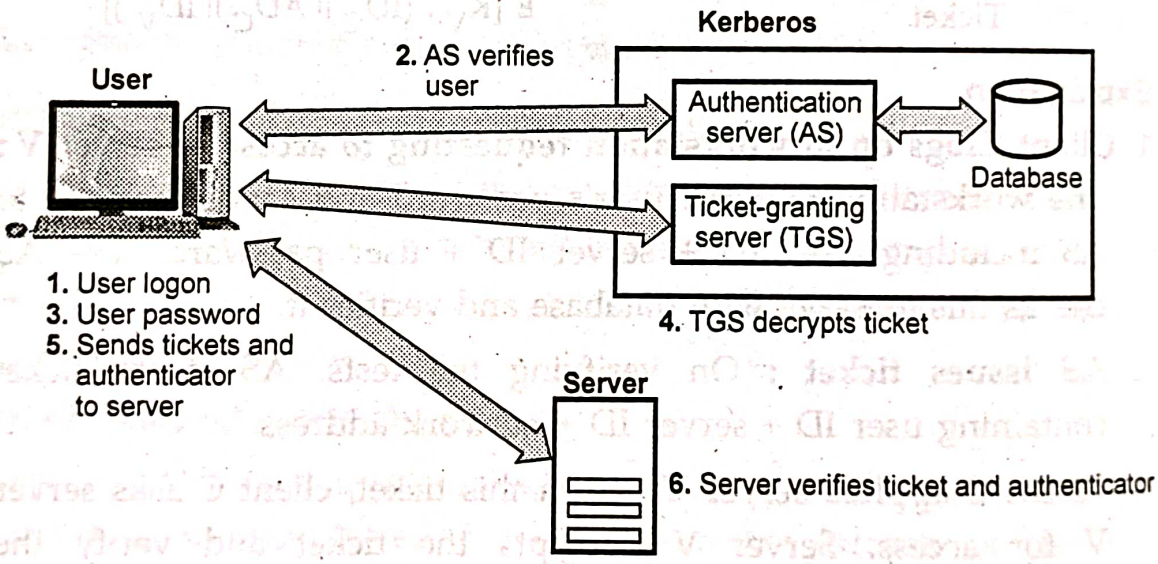


Fig. Q.27.1 Overview of kerberos

Q.28 What is Kerberos Realms ?

Ans. : • The constituents of a full-service Kerberos environment are

a) A Kerberos server b) Clients

c) Number of application server.

- Requirements of Kerberos sever :

a) Kerberos server should have user ID.

b) Hashed password for all users.

c) All users should be registered with Kerberos server.

d) Kerberos server should have secret key with each server.

e) All servers should be registered with Kerberos server.

- A **Kerberos realm** is referred as is the environment where,
  - All nodes share same secured database.
  - Changing and accessing the Kerberos database requires Kerberos master password.
  - A read only copy of Kerberos database resides in computer system.
- Networks have different realms under different administrative organizations. The users of one realm may access the servers in other realm provided the users are authenticated. The interoperating Kerberos shares a secret key with the server in other realm.

Q.29 Compare Kerberos version 4 and Kerberos version 5.

Ans. :

Parameters	Kerberos Versions 4	Kerberos Versions 5
Encryption algorithms used	DES only	DES and other encryptions
Ticket lifetime	5 min units, Maximum = 1280 minutes	Start and end time is arbitrary
Message byte ordering	Tagged message with ordering	Abstract syntax notation on basis encoding rules.
Password attack	Initial request in clear and use it for offline attack.	Need to send pre-authentication data
Two times encryption	Supported	Not supported
Session Keys	Replay risk using repeated ticket	Sub session key once only
Hierarchy of Realms	Limits to pairs	Transition allowed

Q.30 Explain strength and weakness of Kerberos.

Ans. :

1. Passwords are never sent across the network unencrypted. This prevents those unscrupulous people from being able to read the most important data sent over the network.
2. Clients and applications services mutually authenticate. Mutual authentication allows for both ends to know that they truly know whom they are communicating with.
3. Tickets have a limited lifetime, so if they are stolen, unauthorized use is limited to the time frame that the ticket is valid.
4. Authentication through the AS only has to happen once. This makes the security of Kerberos more convenient.
5. Shared secret keys between clients and services are more efficient than public-keys.
6. Many implementations of Kerberos have a large support base and have been put through serious testing.
7. Authenticators, created by clients, can only be used once. This feature prevents the use of stolen authenticators.

Weakness of Kerberos

1. Kerberos only provides authentication for clients and services.
2. Kerberos 4 uses DES, which has been shown to be vulnerable to brute-force-attacks with little computing power.
3. The principal-key database on the KDC has to be hardened or else bad things can happen.
4. Like any security tool, it is also vulnerable to users making poor password choices.
5. Kerberos doesn't work well in a time-sharing environment.
6. Kerberos requires a continuously available Kerberos Server. If the Kerberos Server goes down, the Kerberos network is unusable.

7. Kerberos does not protect against modifications to system software like Trojan horses.

3.9 : X.509 Authentication Service

Q.31 What is X.509 authentication service ? Draw and explain X.509 format of certificate.

Ans. : • X.509 is part of X.500 recommandations for directory service i.e. set of servers which maintains a database of information about users and other attributes.

- X.509 defines authentication services e.g. certificate structure and authentication protocols. Also X.509 also defines alternative authentication protocols base on use of public-key certificates. The X.509 certificate format is emplied in S/MIME, IP security, SET and SSL/TLS.
- X.509 standard uses RSA algorithm and hash function for digital signature. Fig. Q.31.1 shows generation of public key certificate.

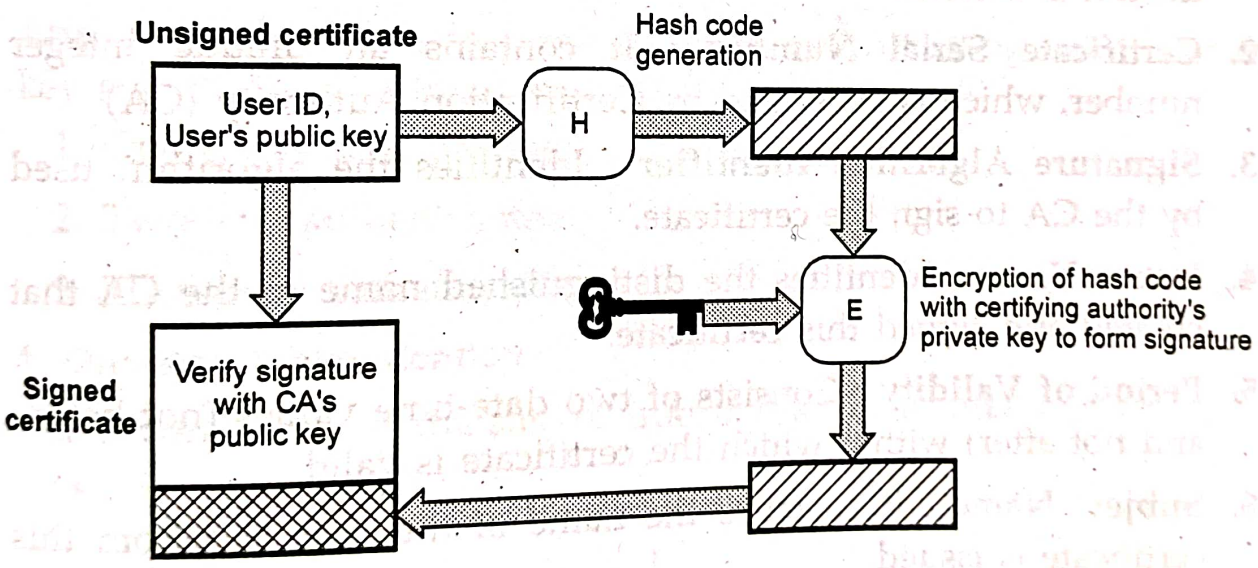


Fig. Q.31.1 Public key certificate

X.509 Format of Certificate

- The current version of the standard is version 3, called as X.509V3. The general format of digital certificate X.509V3 is shown in Fig. Q.31.2.

1	Version
2	Certificate Serial Number
3	Signature Algorithm Identifier
4	Issuer Name
5	Period of Validity
6	Subject Name
7	Subject's Public Key Info.
8	Issuer Unique Identifier
9	Subject Unique Identifier
10	Extensions
11	Signature

Fig. Q.31.2 X.509 Digital certificate format version 3

1. **Version** : Identifies successive versions of certificate format the default is version.
2. **Certificate Serial Number** : It contains an unique integer number, which is generated by Certification Authority (CA).
3. **Signature Algorithm Identifier** : Identifies the algorithm used by the CA to sign the certificate.
4. **Issuer Name** : Identifies the distinguished name of the CA that created and signed this certificate.
5. **Period of Validity** : Consists of two date-time values (not before and not after) within which the certificate is valid.
6. **Subject Name** : It specifies the name of the user to whom this certificate is issued.
7. **Subject's Public Key Information** : It contains public key of the subject and algorithms related to that key.
8. **Issuer Unique Identifier** : It is an optional field which helps to identify a CA uniquely if two or more CAs have used the same Issuer Name.

9. **Subject Unique Identifier** : It is an optional field which helps to identify a subject uniquely if two or more subjects have used the same Subject Name.
10. **Extensions** : One or more fields used in version 3. These extensions convey additional information about the subject and issuer keys.
11. **Signature** : It contains hash code of the fields, encrypted with the CA's private key. It includes the signature algorithm identifier.

Standard notations for defining a certificate

$CA\langle\langle A\rangle\rangle = CA\{V, SN, AI, CA, T_A A, A_P\}$

where,

$CA\langle\langle A\rangle\rangle$ indicates the certificate of user A issued by certification authority CA.

$CA\{V \ldots\ldots A_P\}$ indicates signing of $V \ldots\ldots A_P$ by CA.

Q.32 Describe authentication procedures of X.509.

Ans. : • X.509 supports three types of authenticating using public key signatures. The types of authentication are,

1. One-way authentication
2. Two-way authentication
3. Three-way authentication.

1. One-way authentication

• It involves single transfer of information from one user to other as shown in Fig. Q.32.1.

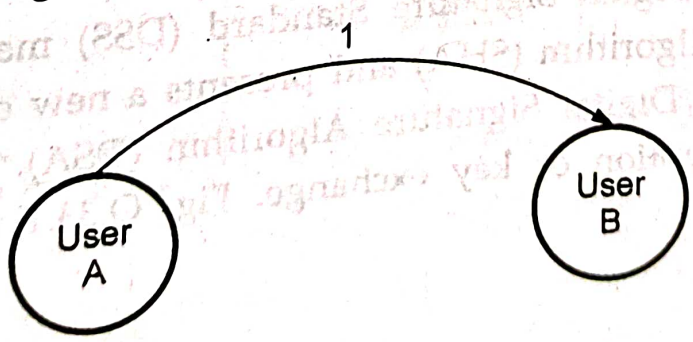


Fig. Q.32.1 One way authentication

2. Two-way authentication

- Two-way authentication allows both parties to communicate and verify the identity of the user.

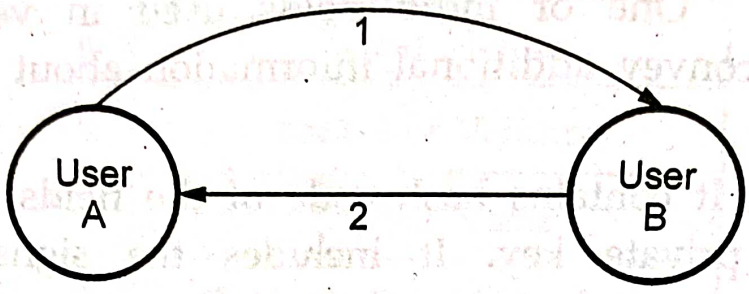


Fig. Q.32.2 Two-way authentication

3. Three-way authentication

- Three-way authentication is used where synchronized clockes are not available Fig. Q.32.3 shows three-way authentication.

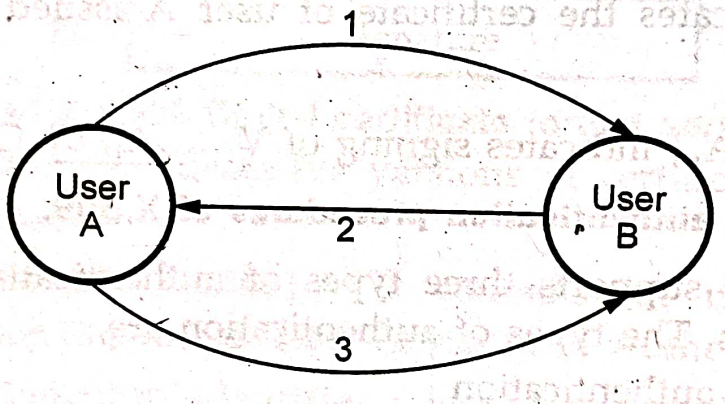


Fig. Q.32.3 Three-way authentication

3.10 : Digital Signatures : Implementation, Algorithms, Standards (DSS)

Q.33 Explain digital signature standard.

Ans. : • The Digital Signature Standard (DSS) makes use of the Secure Hash Algorithm (SHA) and presents a new digital signature technique, the Digital Signature Algorithm (DSA). DSS cannot be used for encryption or key exchange. Fig. Q.33.1 shows the DSS approach.

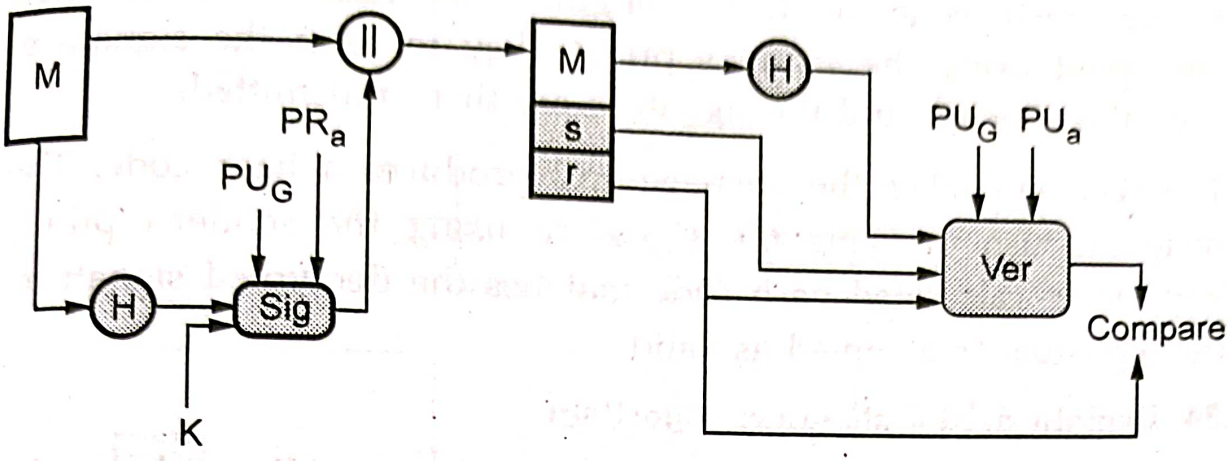


Fig. Q.33.1 DSS approach

- It uses a hash function. The hash code is provided as input to a signature function along with a random number K generated for this particular signature.
- The signature function also depends on the sender's private key (PR_a) and a set of parameters known to a group of communicating principles.
- The result is a signature consisting of two components, labeled s and r.
- At the receiving end, the hash code of the incoming message is generated. This plus the signature is input to a verification function.
- Fig. Q.33.2 shows the RSA approach. In the RSA approach, the message to be signed is input to a hash function that producs a

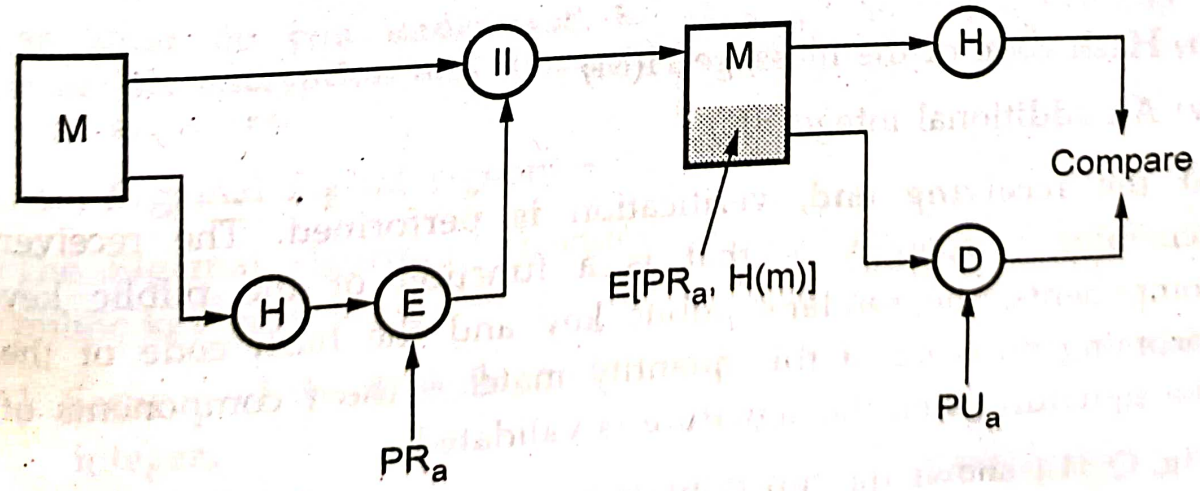


Fig. Q.33.2 RSA approach

secure hash code of fixed length. This hash code is then encrypted using the sender's private key to form the signature. Both the message and the signature are then transmitted.

- The recipient takes the message and produces a hash code. The recipient also decrypts the signature using the sender's public key. If the calculated hash code matches the decrypted signature, the signature is accepted as valid.

Q.34 Explain digital signature algorithm.

Ans. : • There are three parameters that are public and can be common to a group of users. **Prime number q** is chosen and it is **160-bit**. A **prime number p** is selected with a length between **512** and **1024 bits** such that q divides (p – 1).

- g is chosen to be of the form $h^{(P-1)/q}$ mod p where h is an integer between 1 and (p – 1)
- With these number, user selects a private key and generate a public key. The private key x must be a number from 1 to (q – 1) and should be chosen randomly or pseudorandomly.
- The public key is calculated from the private key as $y = g^x$ mod p.
- To create a signature, a user calculates two quantities, **r and s**, that are functions of

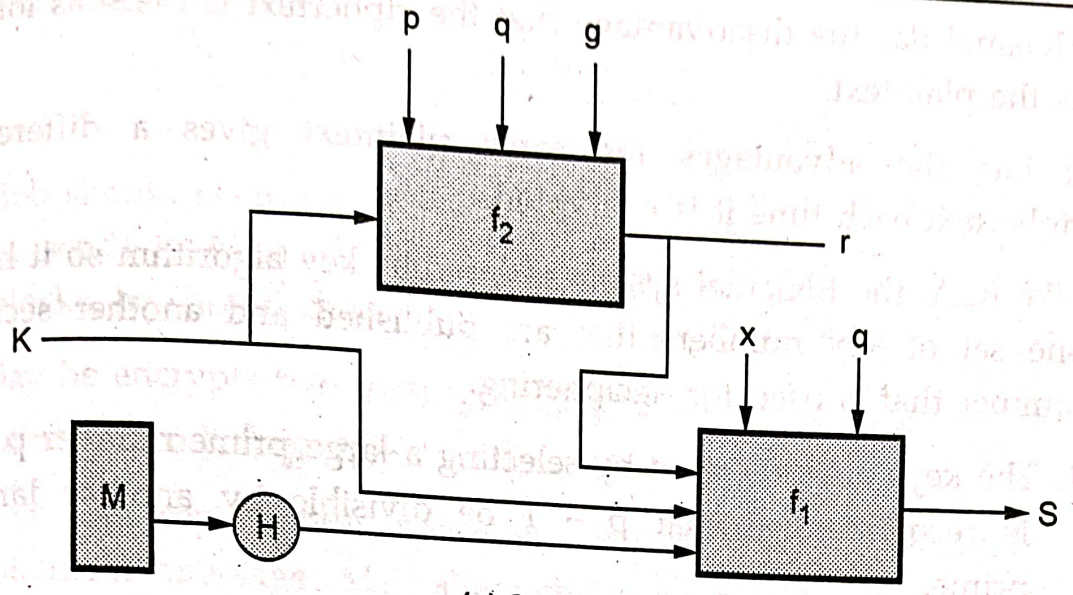
  i) Public key components (p, q, g)

  ii) User's private key (x)

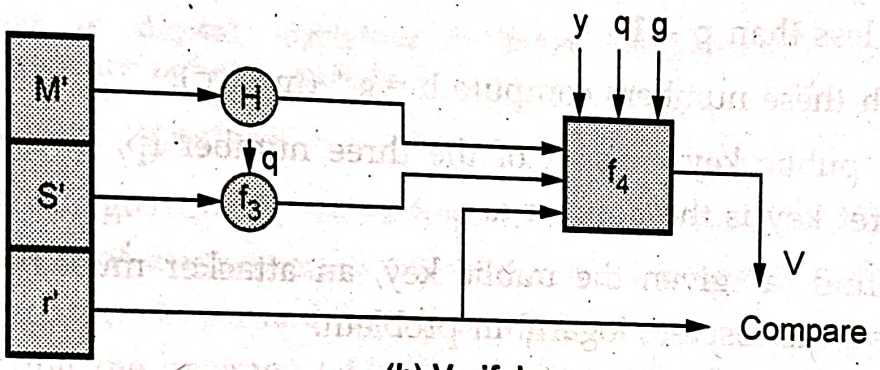
  iii) Hash code of the message H(M)

  iv) An additional integer (K)

- **At the receiving end**, verification is performed. The receiver generates a quantity V that is a function of the public key components, the sender's public key and the hash code of the incoming message. If this quantity matches the r components of the signature, then the signature is validated.
- Fig. Q.34.1 shows the functions of signing and verifying.



(a) Signing



(b) Verifying

Fig. Q.34.1 Signing and verifying

Q.35 What is digital signature ? Explain digital signature standard.

Ans. : Refer Q.33 and Q.34.

Q.36 What do you understand by Elgamel encryption system ? Explain its encryption and decription ? What do you understand by digital signature.

Ans. : Elgamal digital signature

- The Elgamal algorithm provides an alternative to the RSA for public key encryption.

1. Security of the RSA depends on the difficult of factoring large integers.
2. Security of the ElGamal algorithm depends on the difficulty of computing discrete logs in a large prime modulus.

- EIGamal has the disadvantage that the ciphertext is twice as long as the plaintext.
- It has the advantages the same plaintext gives a different ciphertext each time it is encrypted.
- Like RSA, the EIGamal system is a public key algorithm so it has one set of key numbers that are published and another secret number that is used for deciphering.

1. The keys are generated by selecting a large prime number p. It is recommended that p – 1 be divisible by another large prime.
2. Compute a generator number g and select a random integer "a" less than p – 1.
3. With these numbers compute $b = g^a \pmod p$.
4. The public key consists of the three number (p, g, b) and the secret key is the number a.
5. To find "a" given the public key, an attacker must be able to solve the discrete logarithm problem.

Encryption :

- If Bob wants to send a message to Alice he begins by looking up her public key (p, g, b) and representing the message as an integer m in the range 0 to p – 1.
- He then selects a random key, k that is less than p – 1.
- Using these numbers, Bob computes two numbers :

$$c_1 = g^k \quad \text{and} \quad c_2 = mb^k$$

- He sends (c_1, c_2) to Alice.

Decryption :

- When Alice receives the cipher-text, she will recover the plaintext using her secret key, "a" to compute :

$$m = c_2 c_1^{-a} \bmod p$$

- This works because :

$$c_2 c_1^{-a} = mb^k (g^k)^{-a} mb^k (g^a)^k (g^k)^{-a}$$
$$= mg^{ak} g^{-ak} = m \pmod p$$

- Bob should choose a different random integer k for each message he sends to Alice. If M is a longer message, so it is divided into blocks, he should choose a different k for each block.
- Say he encrypts two messagers (or blocks) M_1 and M_2, using the same k, producing cipher-texts.
- Eve intercepts both cipher-text messages and discovers one plaintext message M_1, she can compute the other plaintext message M_2.

Q.37 What is digital signature ? What requirements should a digital signature scheme satisfy ?

Ans. : Digital signature

- A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key.

Requirements

- Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other.
- In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature. The digital signature is analogous to the handwritten signature.
- It must have the following properties,
  1. It must verify the author and the date and time of the signature.
  2. It must to authenticate the contents at the time of the signature.

3. It must be verifiable by third parties, to resolve disputes.

- The digital signature function includes the authentication function. On the basis of these properties, we can formulate the following requirements for a digital signature.
- Must be a bit pattern depending on the message being signed.
- Signature must use some information unique to the sender to prevent forgery and denial.
- Computationally easy to produce a signature.
- Computationally easy to recognize and verify the signature.
- Computationally infeasible to forge a digital signature,
  a) Either by constructing a new message for an existing digital signature.
  b) Or by constructing a fraudulent digital signature for given message.
- Practical to retain a copy of the digital signature in storage.

Two general schemes for digital signatures,

1) Direct 2) Arbitrated.

3.11 : Authentication Protocol

Q.38 What do you mean by MAC ? Explain what characteristics are needed in a secure hash function.

Ans. : MAC is also known as a cryptographic check. The MAC is generated by a function C.

MAC = C(K, M)

where M = Variable length message

K = Secret key shared only by sender and receiver

C(K, M) = Fixed length authenticator

Calculated MAC and message are transmitted to the receiver. The receiver performs the same calculation on the received message.

Received MAC is compared with the calculated MAC. If both are matches, then

1. The receiver is assured that the message has not been altered.
2. The receiver is assured that the message is from the alleged sender.
3. If the message includes a sequence number, then the receiver can be assumed of the proper sequence because an attacker cannot successfully alter the sequence number.

Characteristics are needed in a secure hash function (H)

1. H can be applied to a block of data at any size.
2. H produces a fixed length output.
3. H(x) is easy to compute for any given x.
4. For any given block x, it is computationally infeasible to find x such that H(x) = h.
5. For any given block x, it is computationally infeasible to find with H(y) = H(x).
6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).

Q.39 What are the requirements of a message authentication code ?

Ans. : The requirements for message authentication code (MAC) :

1. **Disclosure :** Release of message contents to any person or process not possessing the appropriate cryptographic key.
2. **Traffic analysis :** Discovery of the pattern of traffic between parties.
3. **Masquerade :** Insertion of messages into the network from a fraudulent source.
4. **Sequence modification :** Any modification to a sequence of messages between parties, including insertion, deletion and reordering.
5. **Content modification :** Changes to the contents of a message, including insertion, deletion, transposition and modification.

6. **Timing modification :** Delay or replay of messages.
7. **Source repudiation :** Denial of transmission of message by source.
8. **Destination repudiation :** Denial of receipt of message by destination.

- Message authentication is a procedure to verify that received messages come form the alleged source and have not been altered.

Q.40 Explain Needham Schroeder protocol.

Ans. : • The Needham Schroeder protocol refers to two methods of communication protocols through an insecure network.

1. Needham Schroeder symmetric key protocol, which is based on symmetric encryption algorithm to establish a session key between two parties in a network.
2. Needham Schroeder public-key protocol, based on the public key cryptography to provide mutual authentication between two communication parties over a network.

Needham Schroeder public key authentication protocol

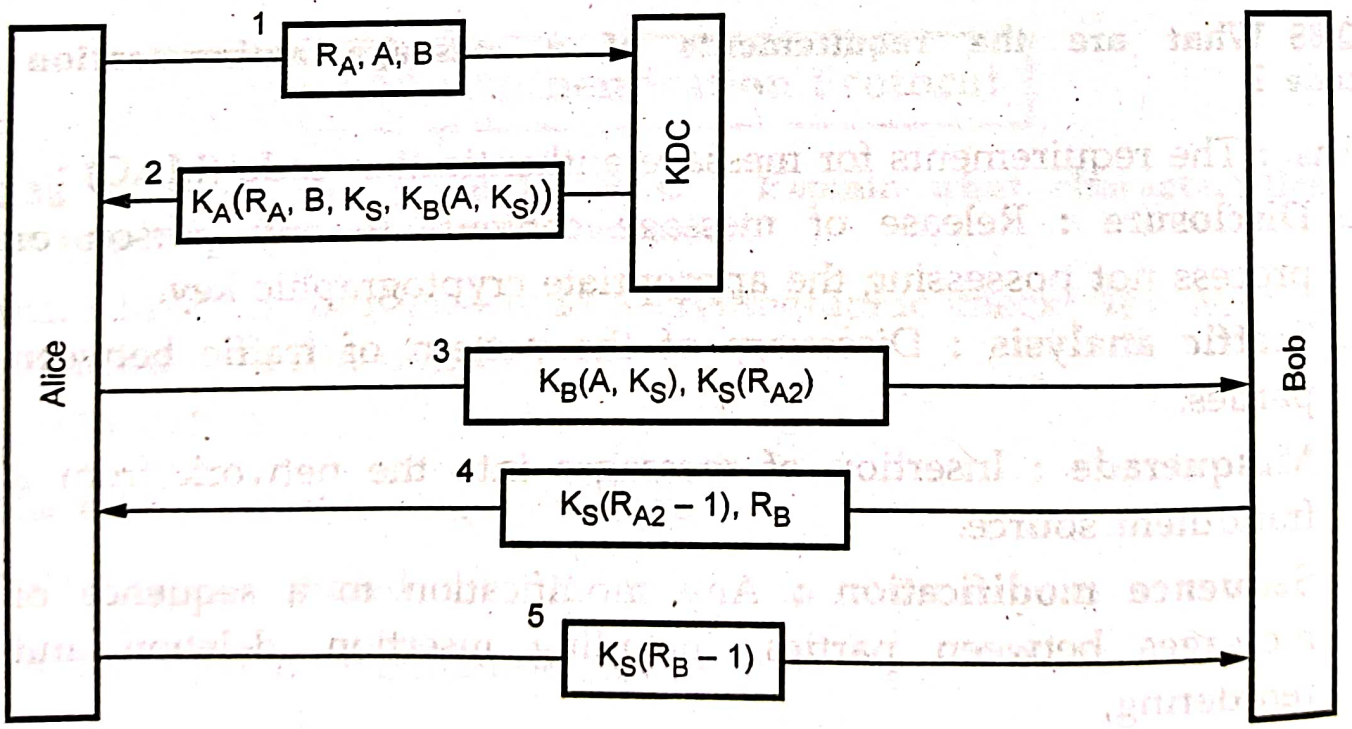


Fig. Q.40.1 Needham Schroeder authentication protocol

- The Needham Schroeder public key authentication protocol aims to provide a mutual authentication between two parties Alice (A) and Bob (B).
- Both parties want to insure each other identity before starting to communicate. The protocol is as follows :

a. K_A and K_B are Alice's public key and Bob's public key respectively,

b. N_A and N_B are nonces generated by A and B respectively.

1. $A \rightarrow B : \{N_A , A\}_{K_B}$ (Init)

Alice generates a nonce N_A and sends it to Bob with her identity. Everything is encrypted using Bob's public key.

2. $B \rightarrow A : \{N_A , N_B\}_{K_A}$ (Challenge)

Bob generates a nonce N_B, and sends it to Alice with N_A he has just received. It is a way to prove that he is really the owner of the private key corresponding to K_B. In other word, this mechanism is implemented in order to authenticate Bob. Sending back to Alice N_A is also a way to avoid a replay of this message.

3. $A \rightarrow A : \{N_B\}_{K_B}$ (Response)

Alice decrypts the message and check if it contains the right value of N_A. Then, she sends back N_B to Bob to prove her ability to decrypt with her private key, and so to authenticate herself.

END...

Unit IV

4 Security Requirements

4.1 : IP Security : Introduction, Architecture, IPv4 and IPv6

Q.1 What is IPv4 protocol ? Explain in detail IPv4 header format.

Ans. : IPv4 : • IP corresponds to the network layer in the OSI reference model and provides a connectionless best effort delivery service to the transport layer. An Internet Protocol (IP) address has a fixed length of 32 bits.

- IPv4 addresses are unique. Two devices on the internet can never have the same address at the same time.
- The address structure was originally defined to have a two level hierarchy : Network ID and host ID.
- The network ID identifies the network the host is connected to. The host ID identifies the network connection to the host rather than the actual host.
- IP addresses are usually written in dotted decimal notation so that they can be communicated conveniently by people.
- The IP address structure is divided into five address classes : Class A, Class B, Class C, Class D and Class E, identified by the most significant bits of the addresses.

IPv4 Header Format

- Packets in the IPv4 layer are called datagrams. A datagram is a variable length packet consisting of two parts : Header and data.
- Fig. Q.1.1 shows IPv4 header format.

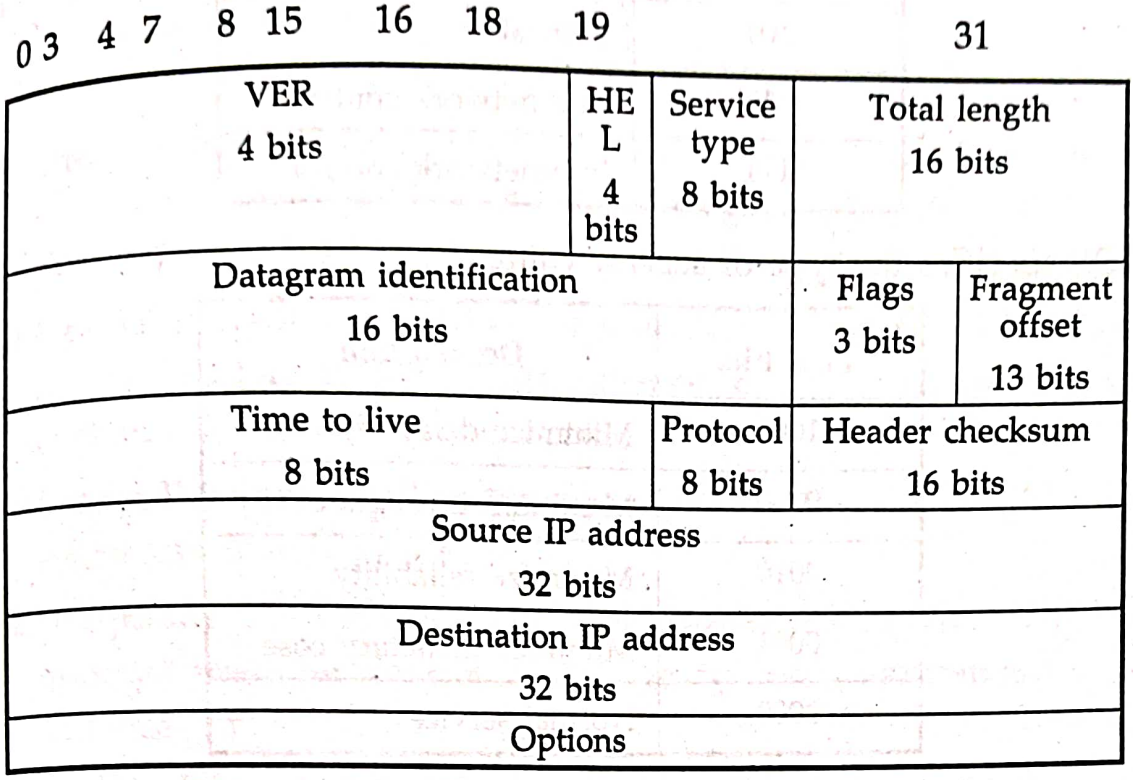


Fig. Q.1.1 IPv4 header format

1. **VER** is the field that contains the IP protocol version. The current version is 4.5 is an experimental version. 6 is the version for IPv6.
2. **HLEN** is the length of the IP header in multiples of 32 bits without the data field.The minimum value for a correct header is 5 (i.e. 20 bytes), the maximum value is 15 (i.e., 60 bytes).
3. **Service type** The service type is an indication of the quality of service requested for this IP datagram. It contains the following information.

Precedence	Types of service	R

Precedence specifies the nature / priority :

000	Routine
001	Priority
010	Immediate
011	Flash

100	Flash override
101	Critical
110	Internetwork control
111	Internetwork control

TOS specifies the type of service value :

TOS bits	Description
1000	Minimize delay
0100	Maximum throughout
0010	Maximize reliability
0001	Minimize monetary cose
0000	Normal service

The last bit is reserved for future use.

4. **Total length** specifies the total length of the datagram, header and data, in octets.
5. **Identification** is a unique number assigned by the sender used with fragmentation.
6. **Flags** contain control flags :
   a. The first bit is reserved and must be zero;
   b. The 2^{nd} bit is DF (Do not Fragment), 0 means allow fragmentation;
   c. The third is MF (More Fragments), 0 means that this is the last fragment.
7. **Fragment offset** is used to reassemble the full datagram. The value in this field contains the number of 64-bit segments (header bytes are not counted) contained in earlier fragments. If this is the first (or only) fragment, this field contains a value of zero.

8. **TTL** (Time To Live) specifies the time (in seconds) the datagram is allowed to travel. In practice, this is used as a hop counter to detect routing loops.

9. **Protocol number** indicates the higher level protocol to which IP should deliver the data in this datagram. E.g., ICMP = 1; TCP = 6; UDP = 17.

10. **Header checksum** is a checksum for the information contained in the header. If the header checksum does not match the contents, the datagram is discarded.

11. **Source/Destination IP addresses** are the 32-bit source/destination IP addresses.

12. **IP options** is a variable-length field (there may be zero or more options) used for control or debugging and measurement instance :

    a. The **loose source routing** option provide a means for source of an IP datagram to supply explicit routing information;

    b. The **timestamp** option tell the routers along the route to put timestamps in the option data.

13. **Padding** is used to ensure that the IP header ends on a 32 bit boundary. The padding is zero.

Q.2 What is IPv6 protocol ? Explain in detail IPv6 header format.

Ans. : IPv6

- IPv6 addresses are 128 bits in length. Addresses are assigned to individual interface on nodes, not to the node themselves.
- A single interface may have multiple unique unicast addresses. The first field of any IPv6 address is the variable length format prefix, which identifies various categories of addresses.
- A new notation has been devised for writing 16-byte addresses. They are written as eight groups of four hexadecimal digits with colons between the groups, like this 8000 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF.

- IPv6 allows three types of addresses : 1. Unicast 2. Anycast 3. Multicast.

Packet Format

- The IPv6 packet is shown in Fig. Q.2.1. Each packet is composed of a mandatory base header followed by the payload. The payload consists of two parts : Optional and data.

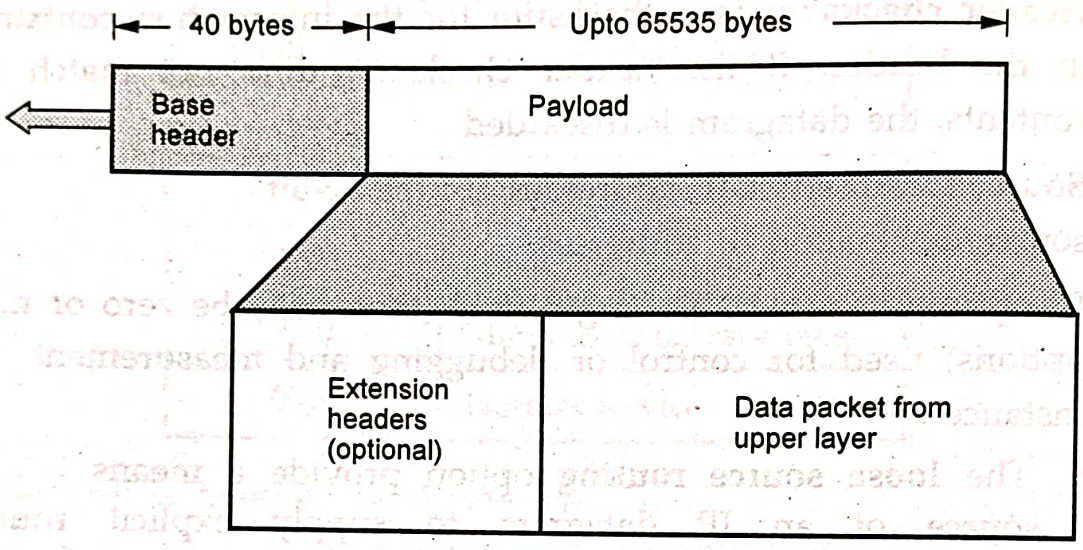


Fig. Q.2.1 IPv6 datagram header of payload

- Fig. Q.2.2 shows the IPv6 datagram header format.

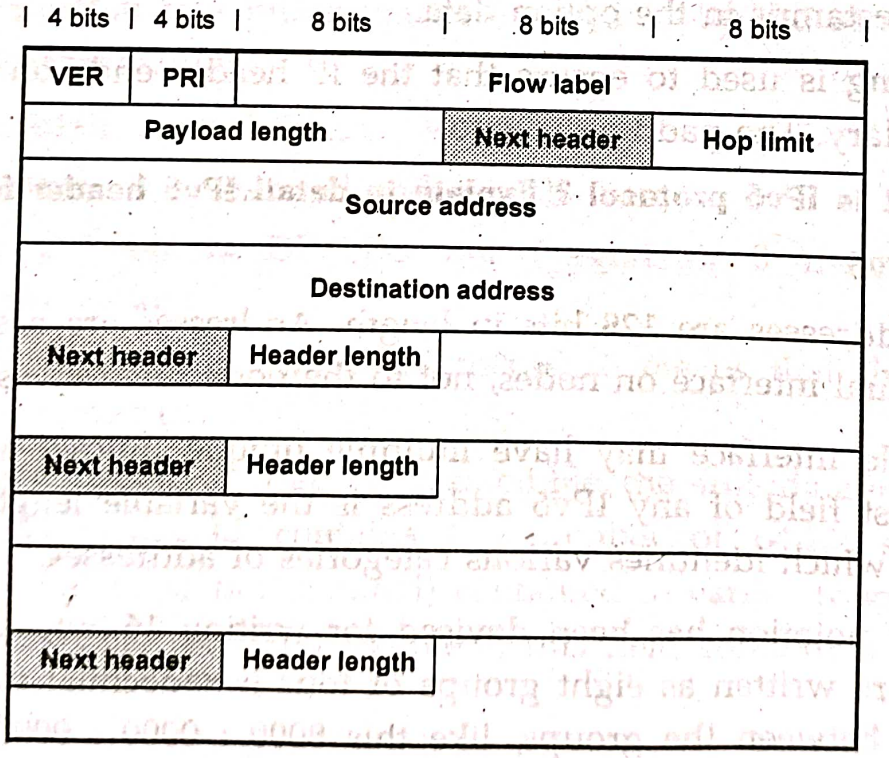


Fig. Q.2.2 IPv6 header

1. **Versions :** This 4 bits field defines the version number of the IP. The value is 6 for IPv6.
2. **Priority :** The 4 bits priority field defines the priority of the packet with respect to traffic congestion.
3. **Flow label :** It is 24 bits field that is designed to provide special handling for a particular flow of data.
4. **Payload length :** The 16 bits payload length field defines the length of the IP datagram excluding the base header.
5. **Next header :** It is an 8 bits field defining the header that follows the base header in the datagram.
6. **Hop limit :** This 8 bits hop limit field serves the same purpose as the TTL field in IPv4.
7. **Source address :** The source address field is a 128 bits internet address that identifies the original.
8. **Destination address :** It is 128 bits Internet address that usually identifies the final destination of the datagram.

- Next header codes for IPv6

Code	Next header
0	Hop by hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null
60	Destination option

Priority

- The priority field defines the priority of each packet with respect to other packets from the same source. IPv6 divides traffic into two broad categories

1. Congestion controlled 2. Noncongestion controlled

- If a source adapts itself to traffic slowdown when there is congestion, the traffic is referred to as congestion controlled traffic. congestion controlled data are assigned priorities from 0 to 7.

Priority	Meaning
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

- A priority of 0 is the lowest; a priority of 7 is the highest.
- Noncongestion controlled traffic refers to a type of traffic that excepts minimum delay. Discarding of packets is not desirable. Retransmission in most cases is impossible. Real time audio and video are examples of this type of traffic.
- Priority numbers from 8 to 15 are assigned to noncongestion controlled traffic.

Q.3 Differentiate between IPv4 and IPv6.

Ans. :

Sr. No.	IPv4	IPv6
1.	Header size is 32 bits.	Header size is 128 bits.
2.	It cannot support autoconfiguration.	Supports autoconfiguration.
3.	Cannot support real time application.	Supports real time application.
4.	No security at network layer.	Provides security at network layer.
5.	Throughput and delay is more.	Throughput and delay is less.

4.2 : IPSec Protocols and Operations

Q.4 Describe IPsec protocol with its components and security services.

OR List and explain components of IPSec protocol.

Ans. : • Different application specific security mechanisms are developed such as electronic mail (PAG, S/MIME), client/server (Kerberos), web access (secure sockets layer). An IP level security can ensure secure networking not only for applications with security mechanisms but also for many security ignorant applications.

- IP Security (IPSec) is the capability that can be added to present versions of Internet Protocol (IPv4 and IPv6) by means of additional headers for secure communication across LAN, WAN and Internet.
- IPSec is a set of protocols and mechanism that provide confidentiality, authentication, message integrity and replay detection at IP layer. The device (firewall or gateway) on which the IPSec mechanism reside is called as **security gateway.**
- IPSec has two modes of operation.
  1. Transport mode
  2. Tunnel mode

- IPSec uses two protocols for message security.
  1. Authentication Header (AH) protocol.
  2. Encapsulating Security Payload (ESP) protocol.

IP Security Architecture

- IPSec mechanism uses Security Policy Database (SPD) which determines how a messages are to handle also the security services needed and path the packet should take.
- Various documents are used to define complex IPSec specification. The overall architecture of IPSec is constituted by three major components.
  1. IPSec documents 2. IPSec services
  3. Security Associations (SA)

IPSec Documents

- IPSec specifications are described in various documents. Few important documents and specifications described are as under -

Sr. No.	Documents	Specifications
1.	RFC 2401	Overview of security architecture.
2.	RFC 2402	Packet authentication extension to IPv4 and IPv6.
3.	RFC 2406	Packet encryption extension to IPv4 and IPv6.
4.	RFC 2408	Key management capabilities.

- All above specifications are essentially supported by IPv6 and are optional for IPv4. The security features are incorporated as extension header to the main IP header for both IPv4 and IPv6.
- The extension header for authentication is called as Authentication Header (AH) and the extension header for

encryption is called as Encapsulating Security Payload (ESP) header.

- Besides RFC various other documents are published by Internet Engineering Task Force (IETF). These documents can be divided into seven groups.
- IPSec protocol consists of seven different groups of document as shown in Fig. Q.4.1.

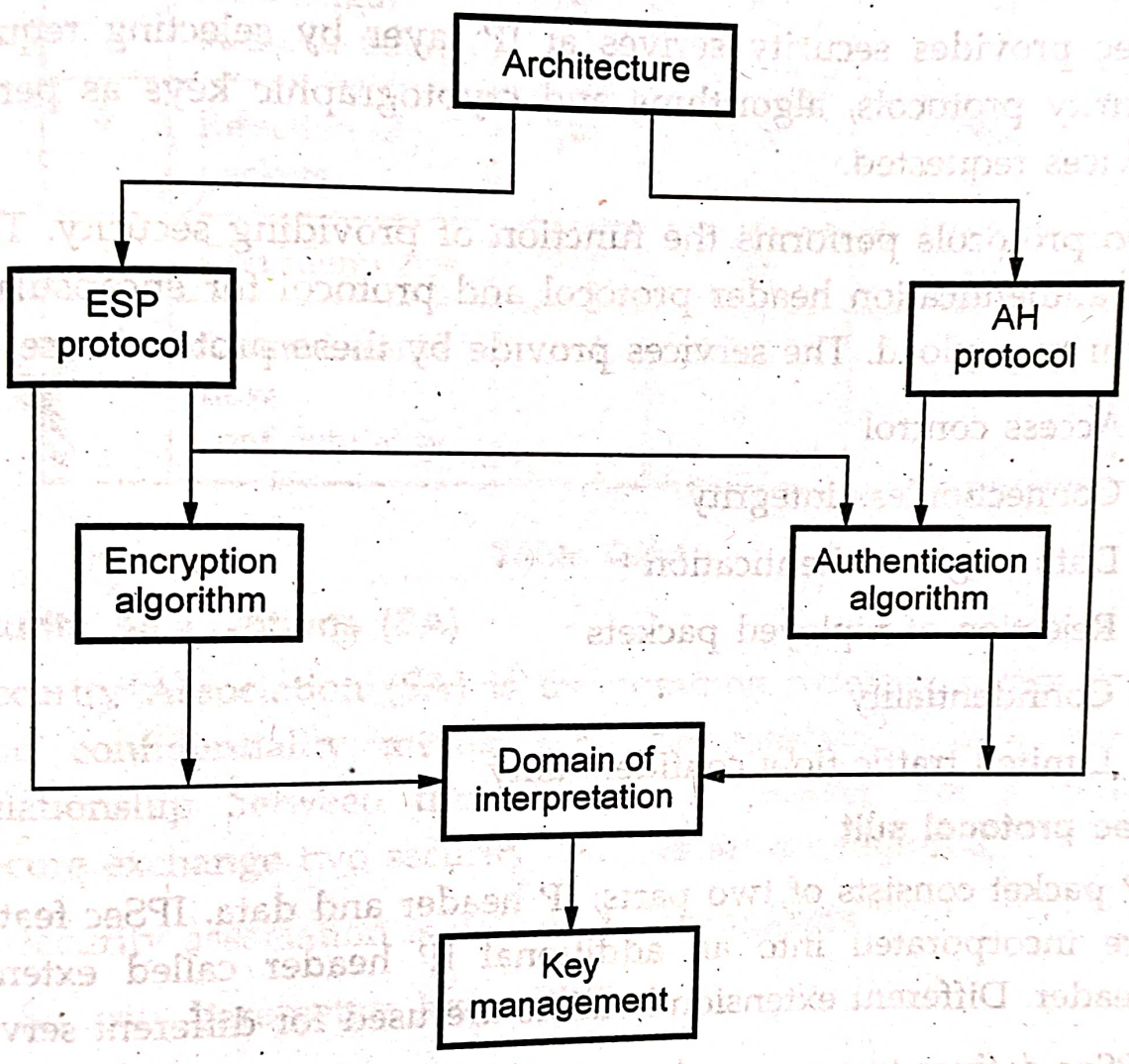


Fig. Q.4.1 IPSec document

1. **Architecture :** Covers security requirements, definitions, IPSec technology.
2. **Encapsulating Security Payload (ESP) :** Covers packet format, packet encryption authentication.

3. **Authentication Header (AH)** : Covers packet format, general issues.
4. **Authentication algorithm :** Encryption algorithms used for ESP.
5. **Key management :** Key management schemes.
6. **Domain of Interpretation (DoI) :** Values to relate documents with each other.

IPSec Services

- IPSec provides security serives at IP layer by selecting required security protocols, algorithms and cryptographic keys as per the services requested.
- Two protocols performs the function of providing security. These are authentication header protocol and protocol for encapsulating security payload. The services provide by these protocols are -
  a. Access control
  b. Connectionless integrity
  c. Data origin authentication
  d. Rejection of replayed packets
  e. Confidentiality
  f. Limited traffic flow confidentiality

IPSec protocol suit

- IP packet consists of two parts; IP header and data. IPSec features are incorporated into an additional IP header called extension header. Different extension headers are used for different services.
- IPSec defines two protocols : 1. AH 2. ESP
- The services provided by ESP protocol is possible with and without authentication option. Various services by AH and ESP protocols are summarized in Table Q.4.1.

Sr. No.	Service	AH protocol	ESP protocol	
			Encryption only	Encryption + Authentication
1.	Access control	Yes	Yes	–
2.	Connectionless integrity	Yes	–	Yes
3.	Data origin authentication	Yes	–	Yes
4.	Rejection of packets	Yes	Yes	Yes
5.	Confidentiality	Yes	Yes	Yes
6.	Limited traffic flow confidentiality	–	Yes	Yes

Table Q.4.1

Security Associations (SA)

- Security Association (SA) is the common between authentication and confidentiality mechanisms. An association is a one-way relationship between transmitter and receiver. For a two-way secure exchange two security associations are required.
- A security association is defined by parameters.
  1. Security Parameters Index (SPI)
  2. IP destination address
  3. Security protocol identifiers

1. Security Parameters Index (SPI) : SPI is a string of bit assigned to this SA and has local significance only. SPI is located in AH and ESP headers. SPI enables the receiving system under which the packet is to process.

2. IP destination address : It is the end point address of SA which can be end user system or a network system (firewall / router).

3. Security protocol identifiers : Security protocol identifier indicates whether the association is an AH or ESP security association.

Q.5 Explain transport mode and tunnel mode operation.

Ans. : Transport Mode

- AH and ESP can support two modes of operation.
  1. Transport mode
  2. Tunnel mode
- Transport mode mainly provide protection for upper layer protocols. The protection extends to the payload of an IP packet. For example, TCP or UDP segment or ICMP packet.
- The transport mode is suitable for end-to-end communication between two workstations.
- In transport mode, ESP encrypts the IP payload excluding IP header. Authentication of IP payload is optional.
- AH authenticates the IP payload and specific portions of IP header.

Tunnel Mode

- Tunnel mode provides protection to entire IP packets. Security fields are added to IP packets and entire packet (AH or ESP packet + Security packet) is new IP packet with a new IP header.
- Entire new IP packet travels through a tunnel from one point to other over IP network. No router over the network are able to detect inner IP header. Since original packet is encapsulated by new larger packet having different source and destination address.

- Tunnel mode is preferred when one or both ends of an SA a security gateway such as a firewall or router that implements IPSec.
- In tunnel mode, number of hosts on network with firewalls may engage in secure transmission without IPSec. The unsecured packets generated are tunneled through external networks by tunnel mode SAs or IPSec in firewall or router.
- ESP encrypts and optionally authenticates the entire inner IP packet including IP header.
- AH authenticates the entire inner IP packet and selected portion of outer IP header.
- The tunnel mode and transport mode functionality is summarized in Table Q.5.1.

Protocol	Transport mode	Tunnel mode
AH	Authenticates IP paylaod and selected portion of IP header.	Authenticates entire IP packet and selected portion of outer IP header.
ESP	Encrypts IP payload and IPv6 extension headers.	Encrypts entire inner IP packet.
ESP with Authentication	Authenticates IP payload and not IP header. Encrypts IP payload and IPv6 header.	Authenticates inner IP packet. Encrypts entire inner IP packet.

Table Q.5.1

Q.6 Discuss the working of IPSec. What are the benefits of IPSec.

Ans. : IP Security Scenario

Fig. Q.6.1 shows an IP security scenario.

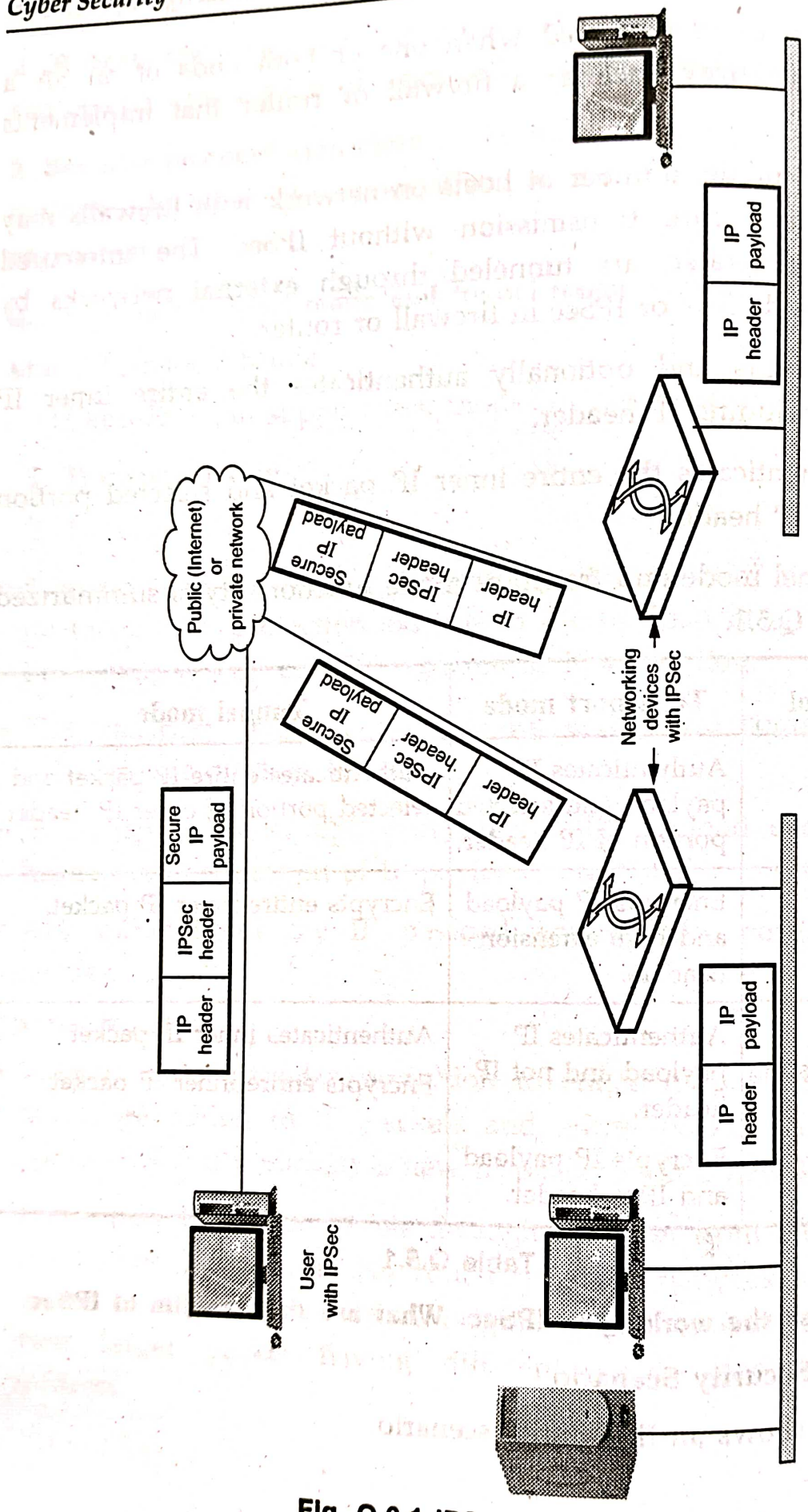


Fig. Q.6.1 IPSec scenario

- Many organizations have LAN at multiple places. The IPSec protocols are used which operates in networking devices e.g. router or firewall.
- The IPSec networking encrypt and compress the outgoing traffic while it decrypt and decompress all incoming traffic. These processes are transparent to workstations and servers on LAN.

Benefits of IPSec

1. IPSec provides strong security within and across the LANs.
2. IPSec in a firewall avoids bypass if all traffic from the outside must use IP.
3. No need to change software for implementing IPSec.
4. IPSec is below transport layer and hence is transparent to applications.
5. IPSec is transparent to end users also.
6. If required IPSec can provide security to individual users.

4.3 : AH and ESP Protocol

Q.7 Explain IPSec Authentication Header (AH) format.

Ans. : • It provides support for data integrity and authentication of IP packets.

- Data integrity service insures that data inside IP packets is not altered during the transit.
- Authentication service enables and end user to authenticate the user at the other end and decides to accept or reject packets accordingly.
- Authentication also prevents the IP spoofing attack.
- AH is based on the MAC protocol, i.e. two communication parties must share a secret key.
- AH header format is shown in Fig. Q.7.1.

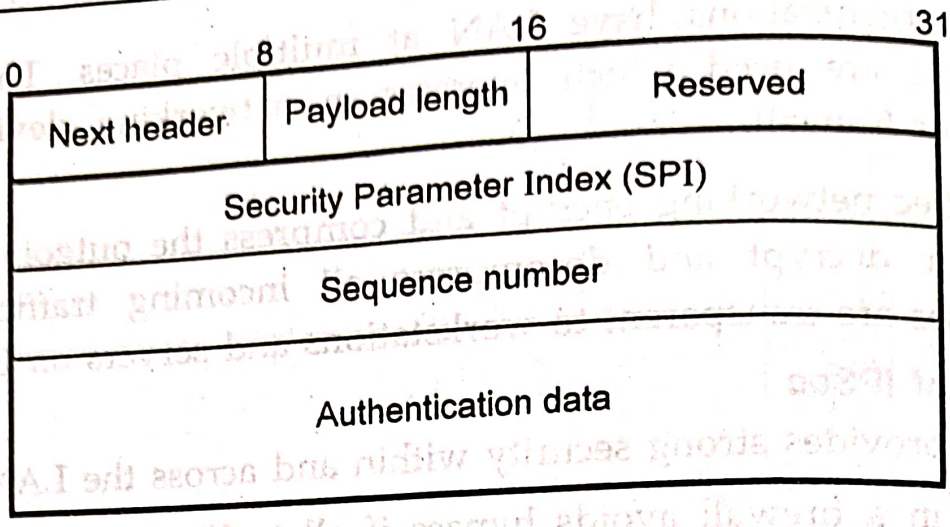


Fig. Q.7.1 IPSec authentication header format

1. **Next header** - This is 8-bits field and identifies the type of header that immediately follows the AH.
2. **Payload length** - Contains the length of the AH in 32-bit words minus 2. Suppose that the length of the authentication data field is 96-bits (or three 32-bit words) with a three word fixed header, then we have a total of 6-words in the header. Therefore this field will contain a value of 4.
3. **Reserved** - Reserved for future use (16-bit).
4. **SPI** - Used in combination with the SA and DA as well as the IPSec protocol used (AH or ESP) to uniquely identify the security association for the traffic to which a datagram belongs.
5. **Sequence number** - To prevent replay attack.

Replay attack

1. Suppose user A wants to transfer some amount to user C's bank account.
2. Both user A and C have the accounts with bank B.
3. User A might send an electronic message to bank B requesting for the funds transfer.
4. User C could capture this message and send a second copy of the message to bank B.

5. Band B have no idea that this is an unauthorized message.
6. User C would get the benefit of the funds transfer twice.

Authentication data : Also called Integrity check value for the datagram. This value is the MAC used for authentication and integrity purposes.

Q.8 Explain ESP protocol format.

Ans. : ESP

- Encapsulating Security Payload (ESP) provides confidentiality services and limited traffic flow confidentiality. An authentication service is optional feature.

ESP Format

- Fig. Q.8.1 shows IPSec ESP format.

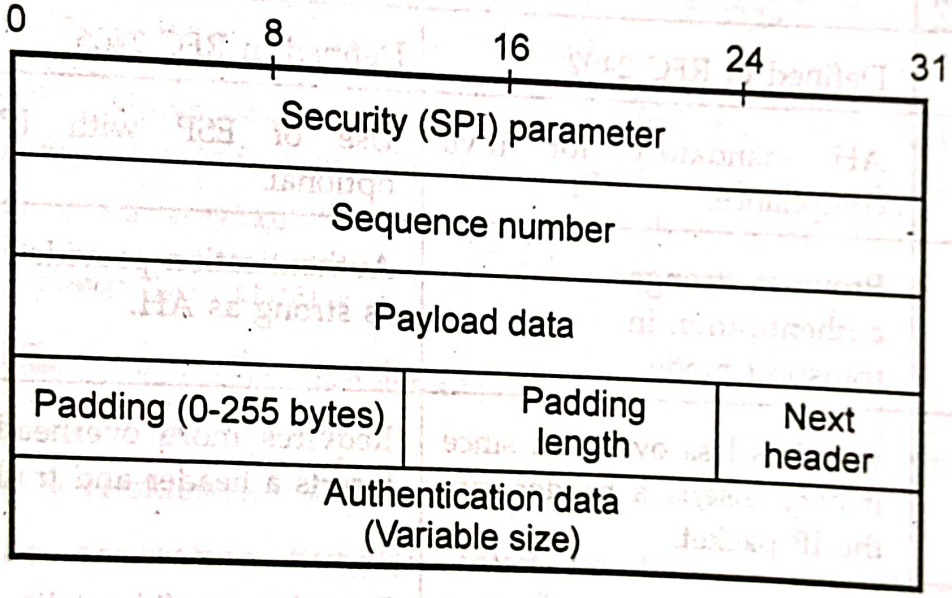


Fig. Q.8.1 ESP format

1. **SPI** - It is 32-bits field used in combination with the source and destination address. It identifies a security association.
2. **Sequence number** - This 32-bit field is used to prevent replay attacks.
3. **Payload data** - This is a transport level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.

4. **Padding** - It contains the padding bits.
5. **Padding length** - Indicates the number of pad bytes immediately preceding this field.
6. **Next header** - It identifies the type of encapsulated data in the payload.
7. **Authentication data** - It is variable length field contains the authentication data called as the integrity check value for the datagram.

Q.9 Compare AH and ESP.

Ans. :

Sr. No.	AH	ESP
1.	Defined in RFC 2402	Defined in RFC 2406
2.	AH mandatory for IPv6 compliance.	Use of ESP with IPv6 is optional.
3.	Provides stronger authentication in transport mode.	Authentication provided is not as strong as AH.
4.	Requires less overhead since it only inserts a header into the IP packet.	Requires more overhead as it inserts a header and trailer.
5.	Provides connectionless integrity and data origin authentication for IPv4 and IPv6.	Provides confidentiality, data origin authentication, connectionless integrity, an anti-reply service and limited traffic flow confidentiality.
6.	Protects as much of the IP header as possible as well as upper level protocol data.	It only protects those IP header fields that it encapsulates.
7.	It provides a packet authentication service.	It encrypts and /or authenticates data.

4.4 : ISAKMP

Q.10 Explain OAKLEY key determination protocol.

OR What is the role of OAKLEY protocol in communication ?

Ans. : • Key management is related to determination and distribution of secret keys. Four keys for communication between two applications : Transmitter and receiver pairs for both AH and ESP.

- Oakley is a refinement of the Diffe-Hellman key exchange algorithm. Two users A and B agree on two global parameters : q, a large prime number and a primitive root of q.
- Secret keys created only when needed. Exchange requires no preexisting infrastructure. This algorithm is simple to use and did not require to much computational time.
- Authentication is used as part of the identity protection and since the oakley protocol uses the users public key we see a hash function used to retain the certification of these keys.
- Cookie generation criteria :

1. Must depend on the specific parties.
2. Must not be possible for anyone other than the issuing entity to generate cookies that will be accepted by that entity.
3. Cookie generation function must be fast to thwart attacks intended to sabotage CPU resources.
4. A hash over the IP source & destination address, the UDP source and destination ports and a locally generated secret random value.

Q.11 Explain ISAKMP protocol for IPsec.

Ans. : • ISAKMP provides a framework for Internet key management and provides protocol support and format for negotiation of security attributes.

- ISAKMP defines payloads for exchanging key generation and authentication data. The payload format provide a consistent

framework independent of exchange protocol, encryption algorithm, authentication mechanism.

ISAKMP header format

- Fig. Q.11.1 shows header format for ISAKMP.

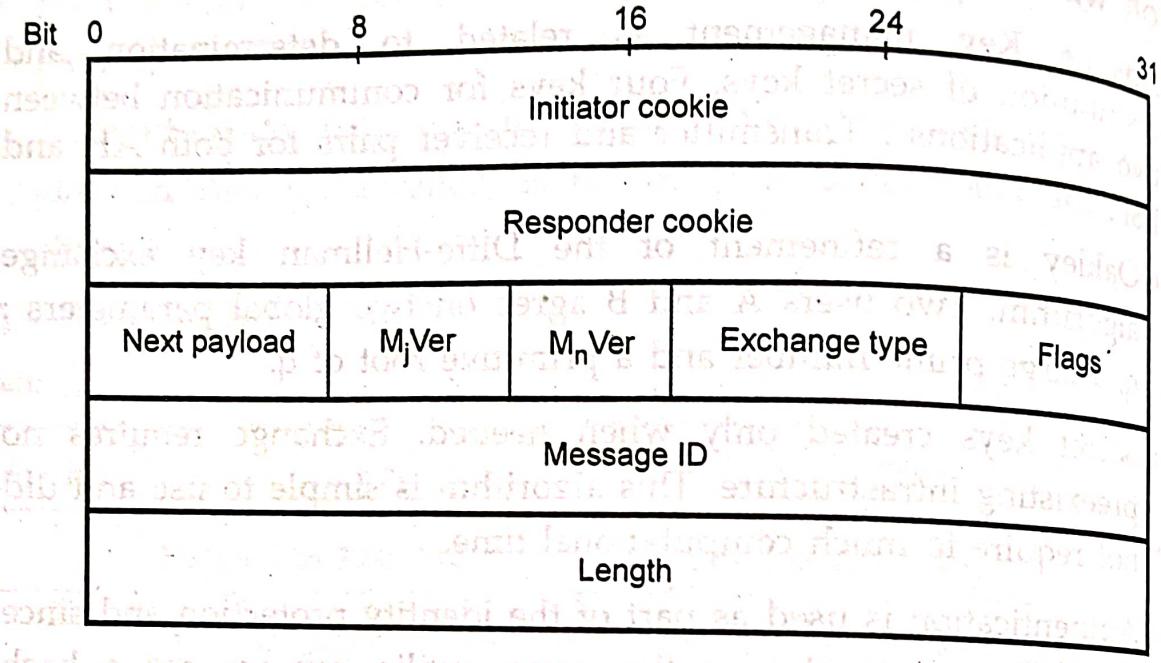


Fig. Q.11.1 ISAKMP header format

Initiator cookie (64-bits) : Cookie of entity that initiated SA establishment, SA notification or SA deletion.

Responder cookie (64-bits) : Cookie of responding entity.

Next payload (8-bits) : Indicates the type of first payload in the message.

Major version (4-bits) / M_j Ver : Indicates major version of ISAKMP in use.

Minor version (4-bits) / M_n Ver : Indicates minor version of ISAKMP in use.

Exchange type (8-bits) : Indicates the type of exchange.

Flags (8-bits) : Indicates specific options set for ISAKMP exchange.

Message ID (32-bits) : Unique ID for the message.

Length (32-bits) : Length of total message in octets.

4.5 : VPN

Q.12 What is VPN ? Explain types of VPN.

Ans. : • Virtual Private Networks (VPN) provide an encrypted connection between a user's distributed sites over a public network (e.g., the Internet). By contrast, a private network uses dedicated circuits and possibly encryption.

- Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users. To counter this problem, a VPN is needed.
- VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.
- VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends.
- The encryption may be performed by firewall software or possibly by routers. The most common protocol mechanism used for this purpose is at the IP level and is known as IPsec.

Types of VPN :

- Types of VPNs are PPTP VPN, Site-to-Site VPN, L2TP VPN, IPsec, SSL, MPLS VPN and Hybrid VPN.
- PPTP VPN stands for Point-to-Point Tunneling Protocol. It creates a tunnel and captures the data. It is used by remote users to connect them to the VPN network using their existing internet connection. This is a useful VPN for both business users and home users. To access the VPN, users log into the VPN using an approved password.
- A Site-to-Site VPN is also called a Router-to-Router VPN and is mostly used in corporate based operations. The fact that many companies have offices located both nationally and internationally, a Site-to-Site VPN is used to connect the network

of the main office location to multiple offices. This is also known as an Intranet based VPN.

- L2TP stands for Layer to Tunneling Protocol that was developed by Microsoft and Cisco. L2TP VPNs are VPNs that are typically combined with another VPN security protocol to establish a more secure VPN connection.

Q.13 State security measure applied by VPN for security.

Ans. : • VPN uses encryption to provide data confidentiality. Once connected, the VPN makes use of the tunneling mechanism described above to encapsulate encrypted data into a secure tunnel, with openly read headers that can cross a public network.

- Packets passed over a public network in this way are unreadable without proper decryption keys, thus ensuring that data is not disclosed or changed in any way during transmission.
- VPN can also provide a data integrity check. This is typically performed using a message digest to ensure that the data has not been tampered with during transmission.

1. VPN connections can be strengthened by the use of firewalls.
2. An IDS / IPS is recommended in order to monitor attacks more effectively.
3. Anti-virus software should be installed on remote clients and network servers to prevent the spread of any virus / worm if either end is infected.
4. Unsecured or unmanaged systems with simple or no authentication should not be allowed to make VPN connections to the internal network.
5. Logging and auditing functions should be provided to record network connections, especially any unauthorised attempts at access. The log should be reviewed regularly.
6. Security policies and guidelines on the appropriate use of VPN and network support should be distributed to responsible parties to control and govern their use of the VPN.

7. Placing the VPN entry point in a Demilitarised Zone (DMZ) is recommended in order to protect the internal network.

4.6 : Web Security

Q.14 Write short note on : Web security threats.

Ans. : • The Web is very visible. The WWW is widely used by businesses, government agencies and many individuals. But the Internet and the Web are extremely vulnerable to compromises of various sorts, with a range of threats.

- Complex software hides many security flaws. Web servers are easy to configure and manage. Users are not aware of the risks.
- These can be described as passive attacks including eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted.
- Active attacks including impersonating another user, altering messages in transit between client and server and altering information on a Web site. The Web needs added security mechanisms to address these threats.

Web Traffic Security Approaches

- Various approaches are used for providing security to the Web. One of the examples is IP security.
- Following table shows the comparison of threats on the web.

Parameters	Threats	Consequences	Countermeasures
Integrity	1. Modification of user data 2. Trojan horse browser 3. Modification of memory 4. Modification of message traffic in transit	1. Loss of information 2. Compromise of machine 3. Vulnerability to all other threats	Cryptographic checksums

Confidentiality	1. Eavesdropping on the Net 2. Theft of information from server 3. Theft of data from client 4. Information about network configuration 5. Information about which client talks to server	1. Loss of information 2. Loss of privacy	Encryption, Web proxies
Denial of Service	1. Killing of user threads 2. Flooding machine with bogus requests 3. Filling up disk or memory 4. Isolating machine by DNS attacks	1. Disruptive 2. Annoying 3. Prevent user from getting work done	Difficult to prevent
Authentication	1. Impersonation of legitimate users 2. Data forgery	1. isrepresentation of user 2. Belief that false information is valid	Cryptographic techniques

- Fig Q.14.1 shows the relative location of security facilities in the TCP/IP protocol stack.

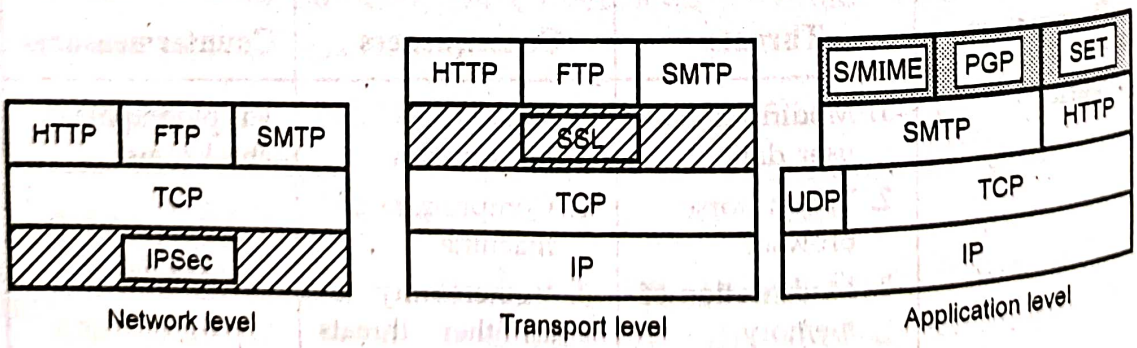


Fig. Q.14.1 Relative locations of security facilities in TCP/IP

Q.15 Compare TLS and IPSec.

Ans. :

Sr. No.	IPSec	TLS
1.	Type of security is device to device.	Type of security is application to application.
2.	It provides network segment protection.	It does not provides network segment protection.
3.	Application modification is required.	Application modification is not required.
4.	Traffic protected with data authentication and encryption is for all protocol.	Traffic protected with data authentication and encryption is only for TCP protocol.
5.	It controlled by using IPSec policy.	It controlled by using TLS policy.
6.	Scope of protection is for single connection for all traffic protocol.	Scope of protection is for single connection for TLS session.

Q.16 Explain TLS handshake protocol.

Ans. : • Handshake protocol is responsible for negotiating security, authenticating the server to the browser and (optionally) defining other communication parameters.

- The TLS handshake protocol allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.
- Fig. Q.16.1 shows the TLS handshake protocol.

1. Browser sends a hello message that includes TLS version and some preferences.
2. Server sends a certificate message that includes the public key of the server. The public key is certified by some certification authority, which means that the public key is encrypted by a CA private key. Browser has a list of CAs and their public keys. It uses the corresponding key to decrypt the certification and finds the server public key. This also authenticates the server because the public key is certified by the CA.

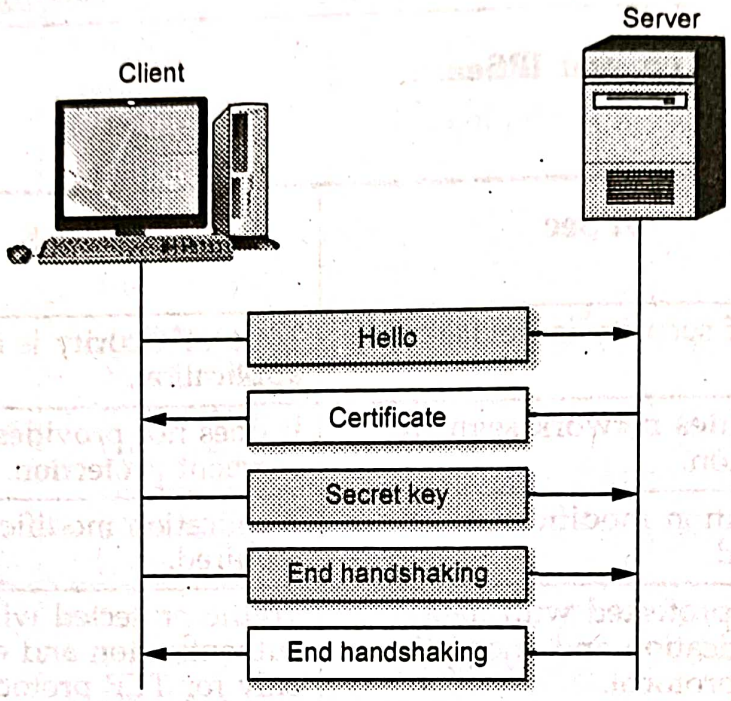


Fig. Q.16.1 TLS handshake protocol

3. Browser sends a secret key, encrypts it with the server public key and sends it to the server.
4. Browser sends a message, encrypted by the secret key to inform the server that handshaking is terminating from the browser key.
5. Server decrypts the secret key using it private key and decrypts the message using the secret key. It then sends a message, encrypted by the secret key, to inform the browser that handshaking is terminating from the server side.

4.7 : SSL

Q.17 Explain secure socket layer handshake protocol in brief.

OR Describe the operation of secure socket layer in detail.

Ans. : • Handshake protocol allows the server and client to authenticate each other and to negotiate an encryption before transmitting application data various massages are used in protocol. Table Q.17.1 enlist these messages and there associated function.

Phase	Message type	Function
1.	Hello - request Client - hello Server - hellow	Null Version, session id, cipher, compression Version, session id, cipher, compression.
2.	Certificate Server - key - exchange Certificate - request Server - done	Chain of X.509 V3 certificates. Parameters, signature. Type, authorities. Null
3.	Certificate - verify	Signature
4.	Client - key - exchange finished.	Parameters, signature hash value.

Table Q.17.1 SSL handshake protocol message types

- Fig. Q.17.1 shows handshake protocol action

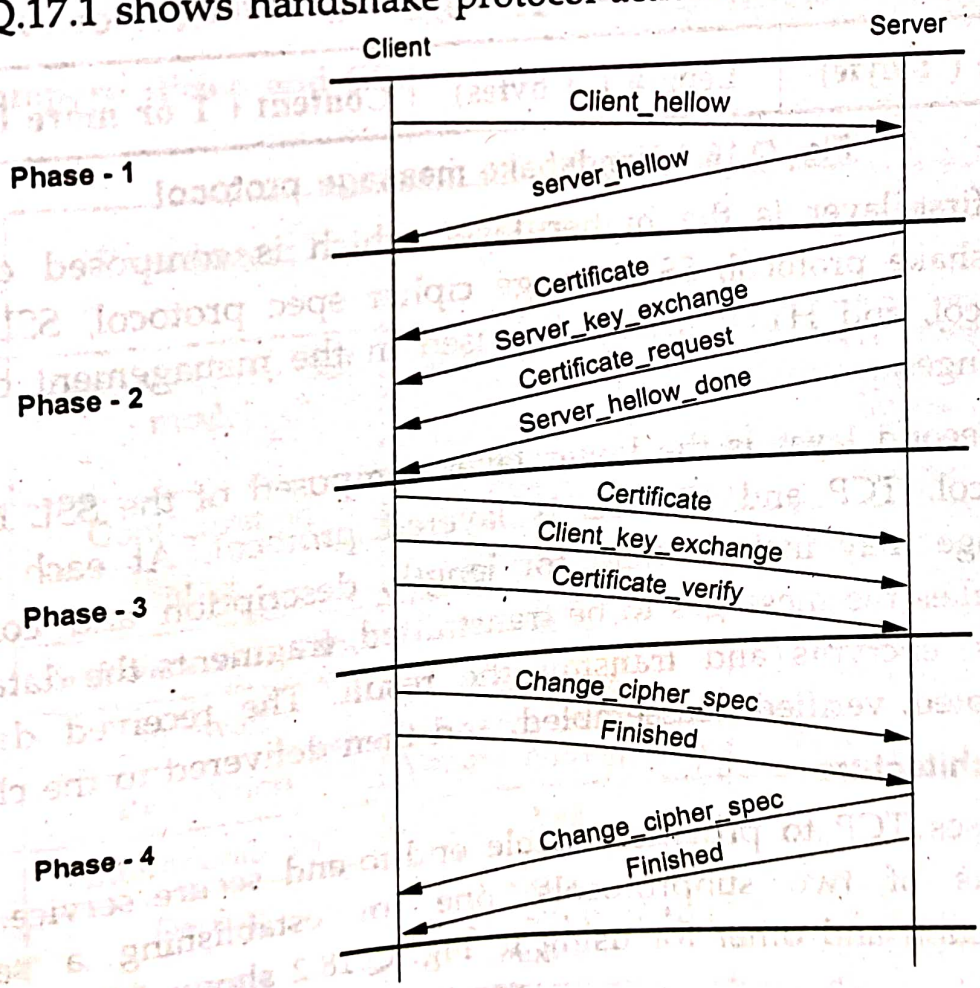


Fig. Q.17.1 Handshake protocol action

Q.18 Describe operation of Secure Socket Layer (SSL) protocol in detail.

Ans. : • Secure Socket Layer (SSL) is a protocol developed by netscape for transmitting private documents via the Internet. SSL is a communications protocol layer which can be placed between TCP/IP and HTTP.

- SSL is built into all major browsers and web servers. It intercepts web traffic and provides security between browser and server. Encryption is used to guarantee secure communication in an insecure environment. All security operations are transparent at both ends of the communication.
- SSL uses public-key cryptography. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
- The SSL Protocol Stack is composed of two layers.

Type (1 byte)	Length (3 bytes)	Content (1 or more bytes)

Fig. Q.18.1 Handshake message protocol

- The first layer is the higher layer which is composed of SSL handshake protocol, SSL change cipher spec protocol, SSL alert protocol, and HTTP, which are used in the management of SSL exchanges.
- The second layer is the lower layer composed of the SSL record protocol, TCP and IP. SSL is layered protocol. At each layer, message may include field for length, description and content. SSL takes the messages to be transmitted, fragments the data into blocks, encrypts and transmit the result. The received data is decrypted, verified, reassembled, and then delivered to the client.

SSL Architecture

- SSL uses TCP to provide reliable end-to-end secure service. SSL consists of two subprotocols, one for establishing a secure connection and other for using it. Fig. Q.18.2 shows SSL protocol stack.

SSL handshake protocol	SSL change cipher protocol	SSL alert protocol	HTTP
SSL record protocol			
TCP			
IP			

Fig. Q.18.2 SSL protocol stack

SSL record protocol : It provides basic security services to various higher layer protocols

HTTP : Provides the transfer service for web client/server interaction.

SSL Handshake protocol,

SSL Change cipher protocol,

SSL Alert protocol. : Management of SSLexchanges.

Q.19 Compare IPSec and SSL.

Ans. :

Sr. No.	Parameters	IPSec	SSL
1.	Position in the OSI model	Internet Layer	Between transport and application layers
2.	Configuration	Complex	Simple
3.	NAT	Problematic	No Problem
4.	Software Location	Kernel Area	User Area
5.	Firewall	Not Friendly	Friendly
6.	Installation	Vender Non-specific	Vender Specific
7.	Interoperability	Yes	No
8.	Deploy	More expensive to deploy, support and maintain.	Less costly to deploy and maintain

Q.20 Compare SSL and TLS.

Ans. :

SSL	TLS
In SSL the minor version is 0 and the major version is 3.	In TLS, the major version is 3 and the minor version is 1.
SSL use HMAC algorithm except that the padding bytes concatenation.	TLS makes use of the same algorithm the padding bytes concatenation.
SSL supports 12 various alert codes.	TLS supports all of the alert codes defined in SSL 3 with the exception of no certificate.

4.8 : Electronic Mail Security

Q.21 What is backdoors and key escrow in PGP ?

Ans. : • **Backdoor** means that based on ciphertext it is possible to find out used key. A backdoor is a "feature" in the software of PGP. It allow an outside user to decrypt the encrypted message.

- How does the sender know whether someone has intentionally planted their own security hole in PGP ?
- If the government induced the PGP Corporation to insert a "backdoor" that allows the police and CBI to decrypt our messages and files with ease ?
- Suppose the one company owned the PGP product, the source-code was unavailable and outside inspection became impossible. As a result, experienced users of PGP lost confidence in newer versions of the product. This situation has been reversed by the PGP Corporation in an attempt to restore confidence.
- PGP Corporation signs its executable programs with a key that can be traced back to that company. Anyone who downloads a

Q.20 Compare SSL and TLS.

Ans. :

SSL	TLS
In SSL the minor version is 0 and the major version is 3.	In TLS, the major version is 3 and the minor version is 1.
SSL use HMAC algorithm except that the padding bytes concatenation.	TLS makes use of the same algorithm the padding bytes concatenation.
SSL supports 12 various alert codes.	TLS supports all of the alert codes defined in SSL 3 with the exception of no certificate.

4.8 : Electronic Mail Security

Q.21 What is backdoors and key escrow in PGP ?

Ans. : • **Backdoor** means that based on ciphertext it is possible to find out used key. A backdoor is a "feature" in the software of PGP. It allow an outside user to decrypt the encrypted message.

- How does the sender know whether someone has intentionally planted their own security hole in PGP ?
- If the government induced the PGP Corporation to insert a "backdoor" that allows the police and CBI to decrypt our messages and files with ease ?
- Suppose the one company owned the PGP product, the source-code was unavailable and outside inspection became impossible. As a result, experienced users of PGP lost confidence in newer versions of the product. This situation has been reversed by the PGP Corporation in an attempt to restore confidence.
- PGP Corporation signs its executable programs with a key that can be traced back to that company. Anyone who downloads a

copy of a PGP program can thus check the authenticity of its source.

- Try to avoid installing any version of PGP that does not include signature files for each component. User must check the downloaded files against their signatures after verifying the authenticity of the PGP Corporation's public key. In this manner, try to protect userself from a tampered version of PGP that could have a backdoor.
- **Key Escrow** is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys.
- In general, key escrow means that a copy of the secret key needed to decrypt something is stored with a third party. This can be a notary or a bank, who will keep it safely for you, in case you lose your key.
- It is also common in business. When an employee has encrypted material on his company computer and he leaves, gets fired or dies unexpectedly, the company might not be able to decrypt the material. This can cost them a lot of money, especially when the employee was working on something very important. For this reason, a copy of the secret key is usually kept by one or more supervisors, who can then decrypt the material if necessary. To ensure that a supervisor does not abuse this power, the key can be split amongst several persons, who have to work together to restore the key.
- The US Clipper initiative this term and now more or less synonymous with government key escrow, where the government keeps a copy of all the secret keys in the country. This allows them to read all encrypted messages being sent, usually for reasons of national security. Many people object to this type of key escrow, as it can be used to invade people's privacy very easily.

Q.22 Explain working of PGP in detail.

Ans. : • PGP is a complete e-mail security package that provides privacy, authentication, digital signatures and compression all in an easy to use form.

- PGP encrypts data by using a block cipher called IDEA, which uses 128-bit keys. IDEA is similar to DES and AES. Key management uses RSA and data integrity uses MD5.
- Suppose user A wants to send a message (P) to user B in a secure way. Both the user have private and public RSA keys. Each user knows the other's user public key.
- User A uses PGP program for security purpose. At sender side i.e. at user A, PGP apply the hash function to the plain text message using MD5 and that message is encrypted.
- After encrypting again apply hash function using own private RSA key. Fig. Q.22.1 shows this process.

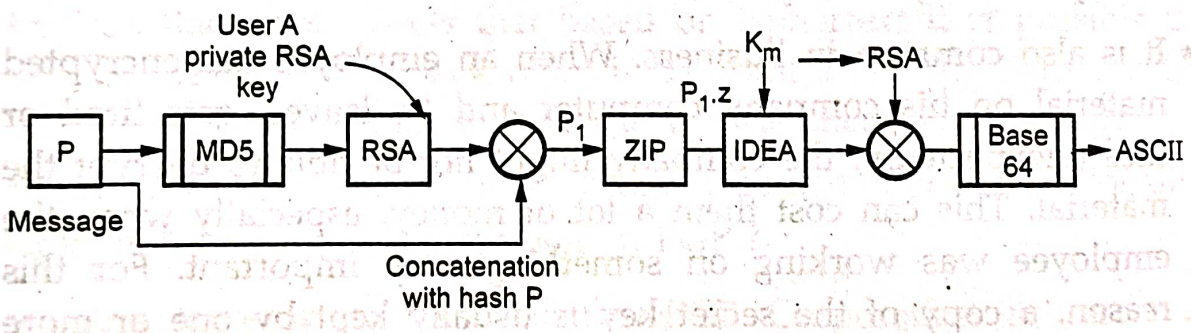


Fig. Q.22.1 PGP process

- When message is received by user B, he decrypts the hash with user A public key and verifies that the hash is correct. MD5 is the difficult to break.
- The encrypted hash and original message are concatenated into a single message P1 and compressed using the ZIP program (P_1. Z).
- Using 128 - bit IDEA message key (K_m), the ZIP program is encrypted with IDEA. Also K_m is encrypted with user B's public key (B_p). These two components are then concatenated and coverted to base 64.

- When this is received by user B, he reverses the base 64 encoding and decrypts the IDEA key using his private RSA key. Using this key, user B decrypts the message to get P_1 Z. After decompressing P_1 Z, user B gets the plaintext message.
- For getting correct message, user B separates the plaintext from hash and decrypts the hash using user A public key. If the plaintext hash agrees with his own MD5 computation, user B knows that P is the correct message and that message came from user A.

Q.23 What are the security services provided by PGP ?

Ans. : PGP operation : • PGP operation involves five different services.

1. Authentication
2. Confidentiality
3. Compression
4. E-mail compatibility
5. Segmentation.

1. Authentication

- Signatures are attached to the message or file are detached signatures are also supported and are stored and transmitted separately from the message it signs.
- The digital signature is generated by either

  i) SHA-1 and RSA

  ii) DSS/SHA-1

- Sender authentication consists of the sender attaching his/her digital signature to the email and the receiver verifying the signature using public-key cryptography. Here is an example of authentication operations carried out by the sender and the receiver :

  1. At the sender's end, the SHA-1 hash function is used to create a 160-bit message digest of the outgoing email message.

2. The message digest is encrypted with RSA using the sender's private key and the result prepended to the message. The composite message is transmitted to the recipient.
3. The receiver uses RSA with the sender's public key to decrypt the message digest.
4. The receiver compares the locally computed message digest with the received message digest.

- The description was based on using a RSA/SHA based digital signature. PGP also support DSS/SHA based signature. DSS stands for Digital Signature Standard. PGP also supports datached signatures that can be sent separately to the receiver. Detached signatures are also useful when a document must be nultiple individuals.
- Fig. Q.23.1 shows an authentication only.

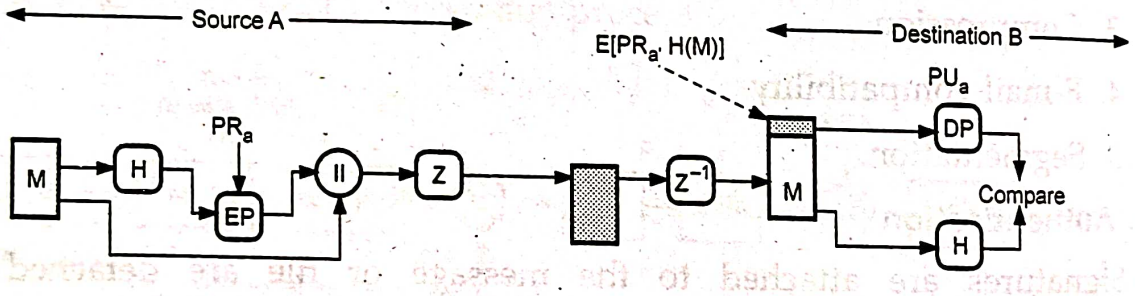


Fig. Q.23.1 Authentication

2. Confidentiality

- Confidentiality is provided by encrypting messages to be transmitted. The algorithms used for encrypties are CAST-128, IDEA, 3DES with multiple keys.
- Only a portion of plaintext is encrypted with each key and there is no relationship with keys. Hence, the public key algorithm is secure.
- This service can be used for encrypting disk files. As you'd expect, PGP uses symmetric-key encryption for confidentiality. The user has the choice of three different block-cipher algorithms

for this purpose : CAST-128, IDEA or 3DES, with CAST-128 being the default choice.

1. Sender generates message and random 128-bit number to be used as session key for this message only.
2. Message is encrypted, using CAST-128 / IDEA/3DES with session key.
3. Session key is encrypted using RSA with recipient's pulic key, then attached to message.
4. Receiver uses RSA with its private key to decrypt and recover session key.
5. Session key is used to decrypt message.

- Fig. Q.23.2 shows a confidentiality operation.

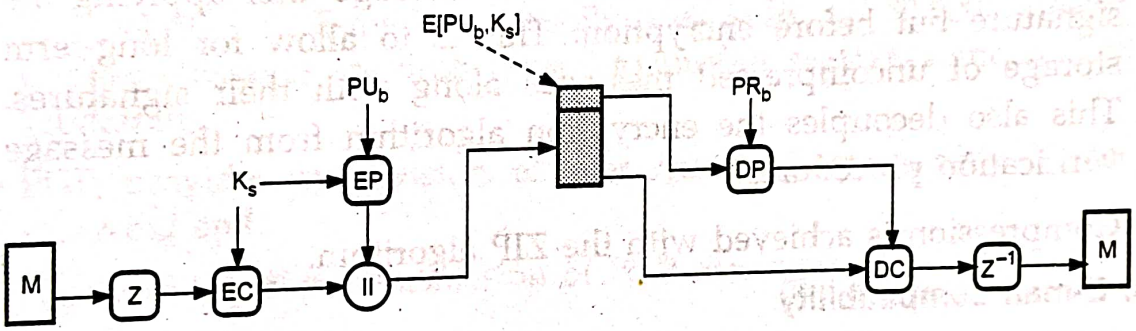


Fig. Q.23.2 Confidentiality

Confidentiality and Authentication

- May be both services used same message
  a. Create signature for plain text and attach to message
  b. Encrypt both message and signature using CAST - 128 or IDEA or TDEA
  c. Attach RSA encrypted session key
- Fig. Q.23.3 shows confidentiality and authentication
- When both services are used, the sender first signs the message with its own private key, then encrypts the message with a session key and then encrypts the session key with the recipient's public key.

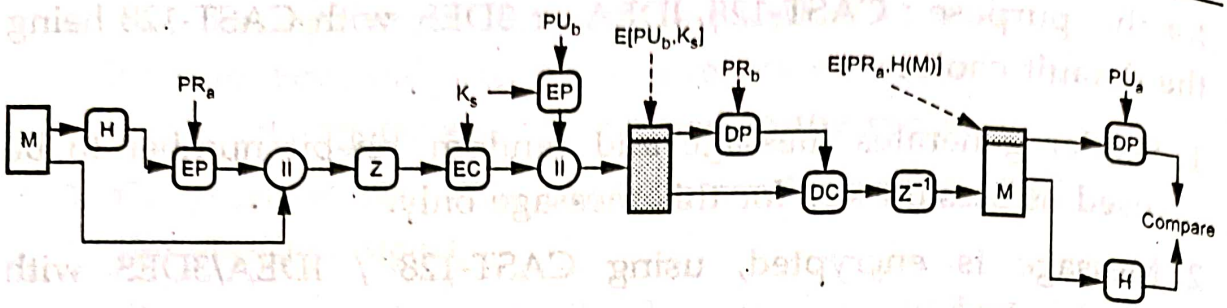


Fig. Q.23.3 Confidentiality and authentication

3. Compression

- Before encryption, the message alongwith signature is compressed. Compression of message saves space and ease of transmission. PGP makes use of a compression package called ZIP. Another algorithm lampd-ZIV LZ77 is also used in zip compression scheme.
- By Default PGP compresses the email message after applying the signature but before encryption. This is to allow for long-term storage of uncompressed messages along with their signatures. This also decouples the encryption algorithm from the message verification procedures.
- Compression is achieved with the ZIP algorithm.

4. E-mail compatibility

- PGP encrypts the block of transmitted message. Some system uses ASCII text, PGP converts it into raw 8-bit binary stream to a stream of printable ASCII characters. The scheme is called radix-64 conversion.
- After receiving, the incoming data is converted into binary by radix-64. Then the encrypted message is recovered by using session key and then decompressed.
- Since encryption, even when it is limited to the signature, results in arbitrary binary strings, and since many email systems only permit the use of ASCII characters, we have to be able to represent binary data with ASCII strings.
- PGP uses radix-64 encoding for this purpose.
- Radix-64 encoding, also known as Base-64 encoding has emerged as probably the most common way to transmit binary data over a

network. It first segments the binary stream of bytes (the same thing as bytes) into 6-bit words.

- The 2^6 = 64 different possible 6-bit words are represented by printable characters as follows : The first 26 are mapped to the uppercase letters A through Z, the next 26 to the lowercase a through z, the next 10 to the digits 0 through 9 and the last two to the characters / and +. This causes each triple of adjoining bytes to be mapped into four ASCII characters.
- The Base-64 character set includes a 65^{th} character, '=', to indicate how many characters the binary string is short of being an exact multiple of 3 bytes. When the binary string is short one byte, that is indicated by terminating the Base-64 string with a single '='. And when it is short two bytes, the termination becomes '=='.

5. Segmentation and reassembly

- The length of E-mail is usually restricted to 50,000 octecks. Longer messages are broken-up into smaller segments and mailed separately.
- PGP provides subdivision of messages and reassembly at the receiving end.
- Fig. Q.23.4 shows transmission of PGP messages

Transmission of PGP message

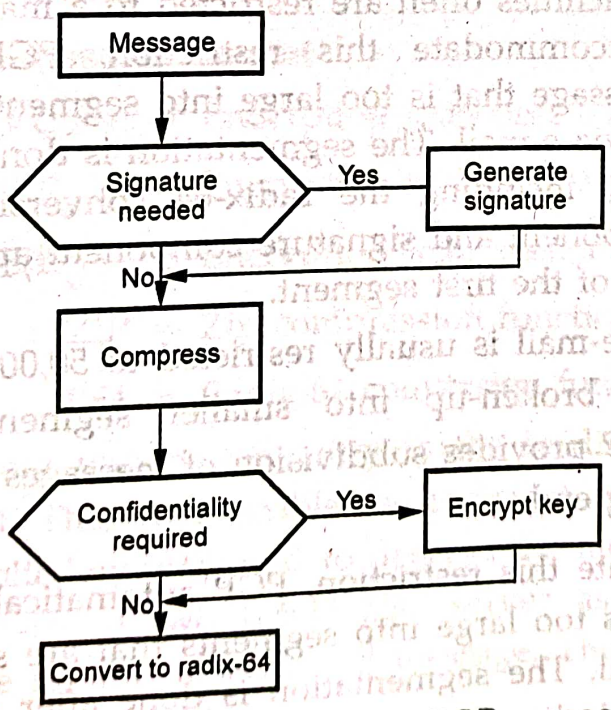


Fig. Q.23.4 Transmission of PGP message

Reception of PGP message

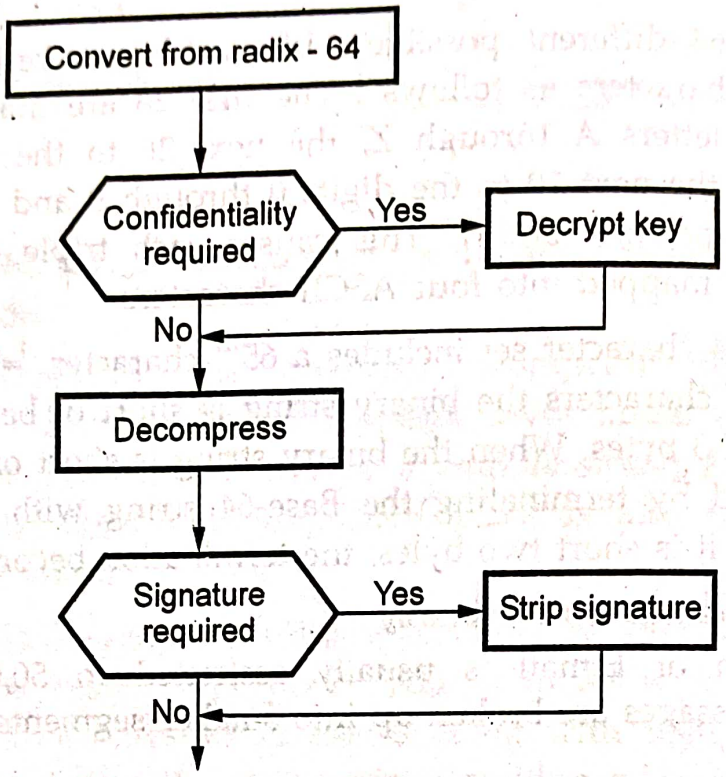


Fig. Q.23.5 Reception of PGP message

Q.24 Why is the segmentation and reassembly function in PGP needed ? How does PGP use the concept of trust ?

Ans. : • E-mail facilities often are restricted to a maximum message length. To accommodate this restriction, PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail. The segmentation is done after all of the other processing, including the radix-64 conversion. Thus, the session key component and signature component appear only once, at the beginning of the first segment.

- The length of e-mail is usually restricted to 50,000 octets. Longer messages are broken-up into smaller segments and mailed separately. PGP provides subdivision of messages and reassembly at the receiving end.
- To accommodate this restriction, PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail. The segmentation is done after all of the other processing, including the radix-64 conversion. Thus, the session

key component and signature component appear only once, at the beginning of the first segment. At the receiving end, PGP must strip off all e-mail headers and reassemble the entire original block.

PGP use the concept of trust :

- PGP provide a convenient means of using trust, associating trust with public keys and exploiting trust information. Each entry in the public-key ring is a public key certificate.
- Associated with each such entry is a key legitimacy field that indicates the extent to which PGP will trust that this is a valid public key for this user; the higher the level of trust, the stronger is the binding of this user ID to this key.

Q.25 Give a general format of PGP message. Why does PGP generate a signature before applying compression ?

Ans. : Message Format

- The Fig. Q.25.1 shows the general format of a PGP message. As the figure shows, a PGP message consists of three components :

a) Session key component b) Signature component

c) Actual email message

Notation used in message format

$E(PU_b, \bullet)$ = Encyrption with user b's public key

$E(PR_a, \bullet)$ = Encryption with user a's private key

$E(K_s, \bullet)$ = Encryption with session key

ZIP = Zip compression function

R64 = Radix-64 conversion function

- Perhaps the only unexpected entry is the leading two bytes of message digest. This is to enable the recipient to determine that the correct public key was used to decrypt the message digest for authentication. These two octets also server as a 16-bit frame check sequence for the actual email message. The message digest itself is calculated using SHA-1.

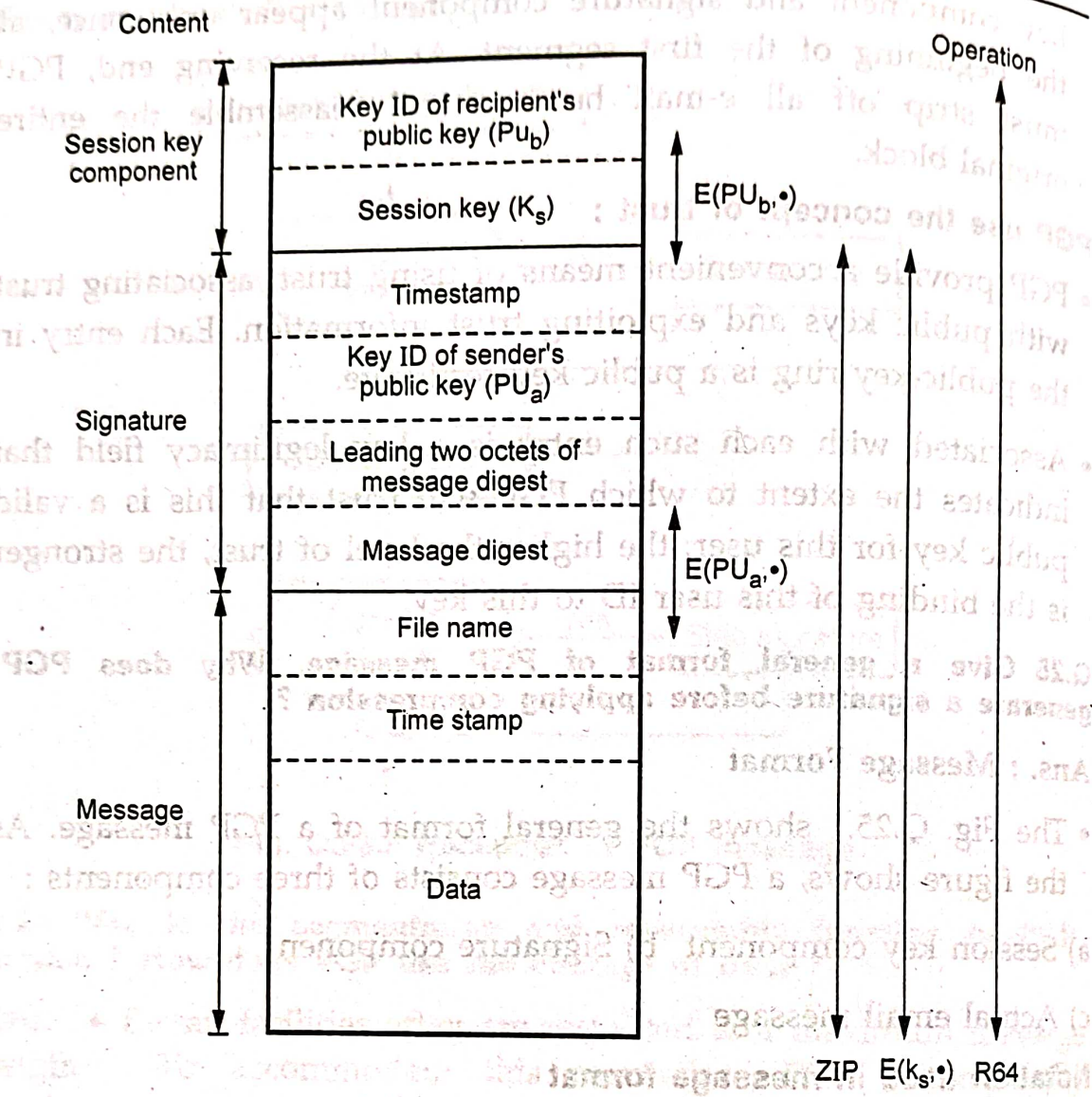


Fig. Q.25.1 General format of PGP message

- **Message component** includes the actual data to be stored or transmitted, as well as a filename and a timestamp that specifies the time of creation.
- Signature component consists of

a) **Timestamp :** The time at which the signature was made.

b) **Key ID of sender's public key :** Identifies the public key that should be used to decrypt the message digest.

c) **Leading two octets of message digest :** To enable the recipient to determine if the correct public key was used to decrypt the

message digest for authentication, by comparing this plain text copy of the first two octets with the first two octets of the decrypted digest.

d) **Message digest :** The 160-bit SHA-1 digest encrypted with the sender's private signature key.

- Session key component includes the session key and the identifier of the recipient's public key that was used by the sender to encrypt the session key.
- In the table, each row represents one the public / private key pairs owned by this user. Each row contains the following entries :
  1. **Timestamp :** The date or time when this key pair was generated.
  2. **Key ID :** The least significant 64 bits of the public key for this entry.
  3. **Public key :** The public key portion of the pair.
  4. **Private key :** The private key portion of the pair; this field is encrypted.
  5. **User ID :** This will be the user's e-mail address or to reuse the same user ID more than one.
- The private key itself is not stored in the key ring. Rather, this key is encrypted using CAST-128. The procedure is as follows :
  1. The user select a passphrases to be used for encrypting private keys.
  2. When the system generates a new public / private key pair using RSA, it ask the user for the passphrases. A 160-bit hash code is generated from the pass-phrase using SHA-1.
  3. The system encrypts the private key using CAST-128 with the 128-bits of the hash code as the key.
- PGP will retrieve the encrypted private key, generate the hash code of the pass-phrase and decrypt the encrypted private key using CAST-128 with the hash code.

PGP Message Generation

- Fig. Q.25.2 shows PGP message generation.

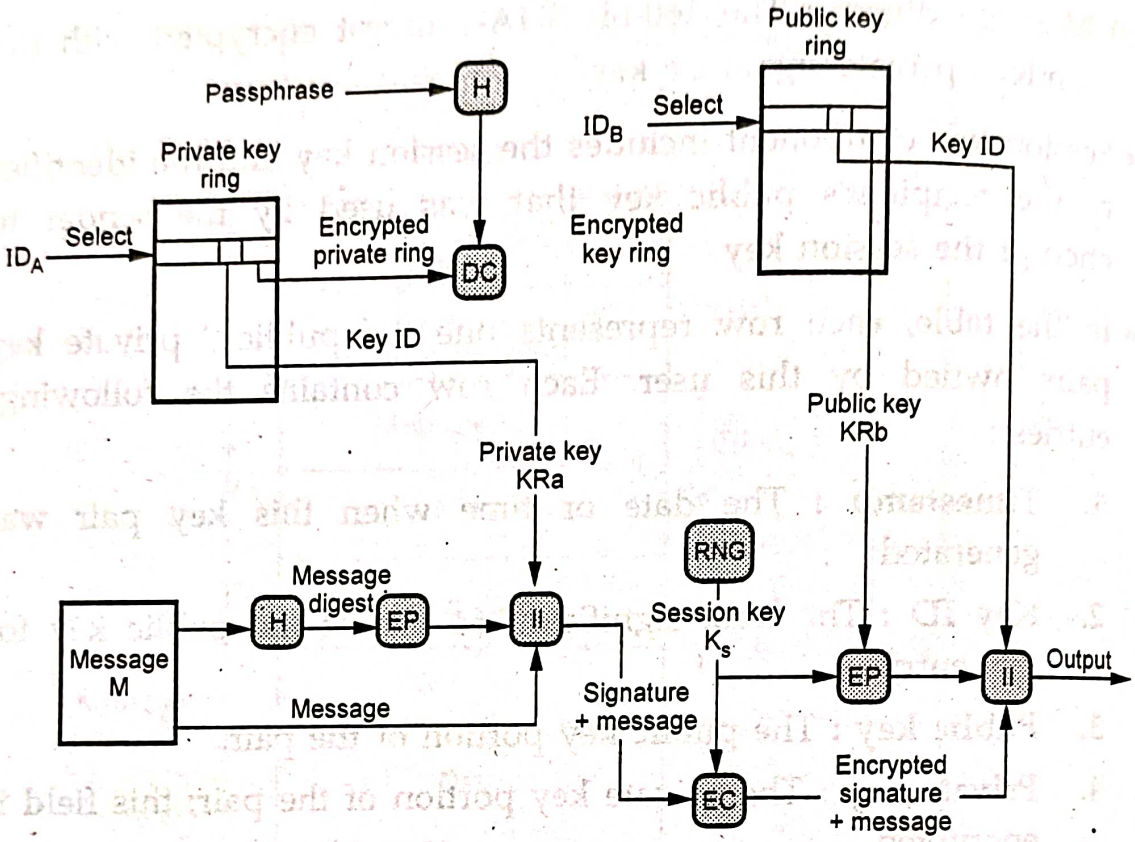


Fig. Q.25.2 PGP message generation

- The sending PGP entity performs the following steps :

a) Signs the message :

i. PGP gets sender's private key from key ring using its user id as an index.

ii. PGP prompts user for pass-phrase to decrypt private key.

iii. PGP constructs the signature component of the message.

b) Encrypts the message :

i. PGP generates a session key and encrypts the message.

ii. PGP retrieves the receiver public key from the key ring using its user id as an index.

iii. PGP constructs session component of message.

- It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification.
- If one signed a compressed document, then it would be necessary either to store a compressed version of the message for later verification or to recompress the message when verification is required. b. Even if one were willing to generate dynamically a recompressed message for verification, PGP's compression algorithm presents a difficulty.
- The algorithm is not deterministic; various implementations of the algorithm achieve different tradeoffs in running speed versus compression ratio and, as a result, produce different compressed forms. However, these different compression algorithms are interoperable because any version of the algorithm can correctly decompress the output of any other version.
- Applying the hash function and signature after compression would constrain all PGP implementations to the same version of the compression algorithm.

Q.26 What is S/MIME ? State operation of S/MIME in detail.

OR Explain working of S/MIME with secrecy and authentication.

Ans. : • S/MIME is a Secure/Multipurpose Internet mail extension. It is a security enhancement to the MIME Internet e-mail format standard. S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP.

- S/MIME incorporates three public-key algorithms, DSS for digital signatures, Diffie-Hellman for encrypting session keys or RSA. It uses SHA1 or MD5 for calculating digests and three-key triple DES for message encryption.
- In an ideal situation, a S/MIME sender has a list of preferred decrypting capabilities from an intended recipient, in which case it chooses the best encryption. Otherwise, if the sender has

received any previous mail from the intended recipient, it then chooses the same encryption mechanism.

- To secure a MIME entity (e.g. the entire message with exception of the RFC 822 header), S/MIME produces a PKCS object. The PKCS object is then treated as the message object and encoded with MIME. Since the result of encryption is typically in binary, it needs to be transferred in a more secure way, such as in base64 mode.
- **S/MIME Functionality :** Functions are as follows

1. Enveloped data consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.
2. A singed data message can only be viewed by a recipient with S/MIME capability. Base64 encoding method is used for encoding content and signature.
3. In clear signed data, a digital signature of the content is formed. Here only the digital signature is encoded using base64. Recipients without S/MIME capability can view the message content, although they cannot verity the signature.
4. Signed and enveloped data : Signed only and encrypted only entities may be nested, so that encrypted data may be signed and signed data or clear signed data may be encrypted.

Q.27 Compare PGP, MME and S/MIME.

Ans. : PGP : • PGP stands for Pretty Good Privacy.

- PGP encrypts data by using a block cipher called IDEA, which uses 128-bit keys.
- PGP is a complete e-mail security package that provides privacy, authentication, digital signatures and compression all in an easy to use form.
- Diffie-Hellman signature is used.
- Also used in virtual private network.

MIME :

- Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through SMTP.
- MIME defined by IETF to allow transmission of non-ASCII data via e-mail.
- It allows arbitary data to be encoded in ASCII for normal transmission.
- All media types that are sent or received over the world wide web (www) are encoded using different MIME types.

S/MIME :

- S/MIME is a Secure / Multipurpose Internet Mail Extension. It is a security enhancement to the MIME Internet e-mail format standard.
- Elgamal digital signature is used.
- Digital certificate standard uses X.509.
- Only used for email services.

4.9 : Secure Electronic Transaction (SET)

Q.28 What is secure electronic transaction ?

OR Explain operation of secure electronic transaction protocol.

OR Explain the operation of secure electronic transaction protocol in brief.

Ans. : • SET is an encryption and security specification develop to protect credit card transactions through Internet SET is not a payment system but a set of security protocols for secured way for payment transactions.

- SET provides a secure communication channel among all parties.
- The participants of SET system are Card holder, Merchant, Issuer, Acquirer, Payment gateway and Certification authority.

- Dual signature is needed for linking two messages that are intended for two different receiver Order Information and Payment Information (OI and PI).

Purchase Request

- Browsing, selecting, and ordering is done.
- Purchasing involves four messages :

i) Initiate request ii) Initiate response

iii) Purchase request iv) Purchase response

i) Initiate Request

- Basic requirements :
  - Cardholder must have copy of certificates for merchant and payment gateway.
- Customer requests the certificates in the initiate request message to merchant.
  - Brand of credit card
  - ID assigned to this request/response pair by customer

ii) Initiate Response

- Merchant generates a response
  - Signs with private signature key
  - Include customer nonce
  - Include merchant nonce (returned in next message)
  - Transaction ID for purchase transaction
- In addition ...
  - Merchant's signature certificate
  - Payment gateway's key exchange certificate

iii) Purchase Request

- Cardholder verifies two certificates using their CAs and creates the OI and PI

- Message includes :
  - Purchase-related information
  - Order-related information
  - Cardholder certificate
- The cardholder generates a one-time symmetric encryption key KS

(Refer Fig. Q.28.1)

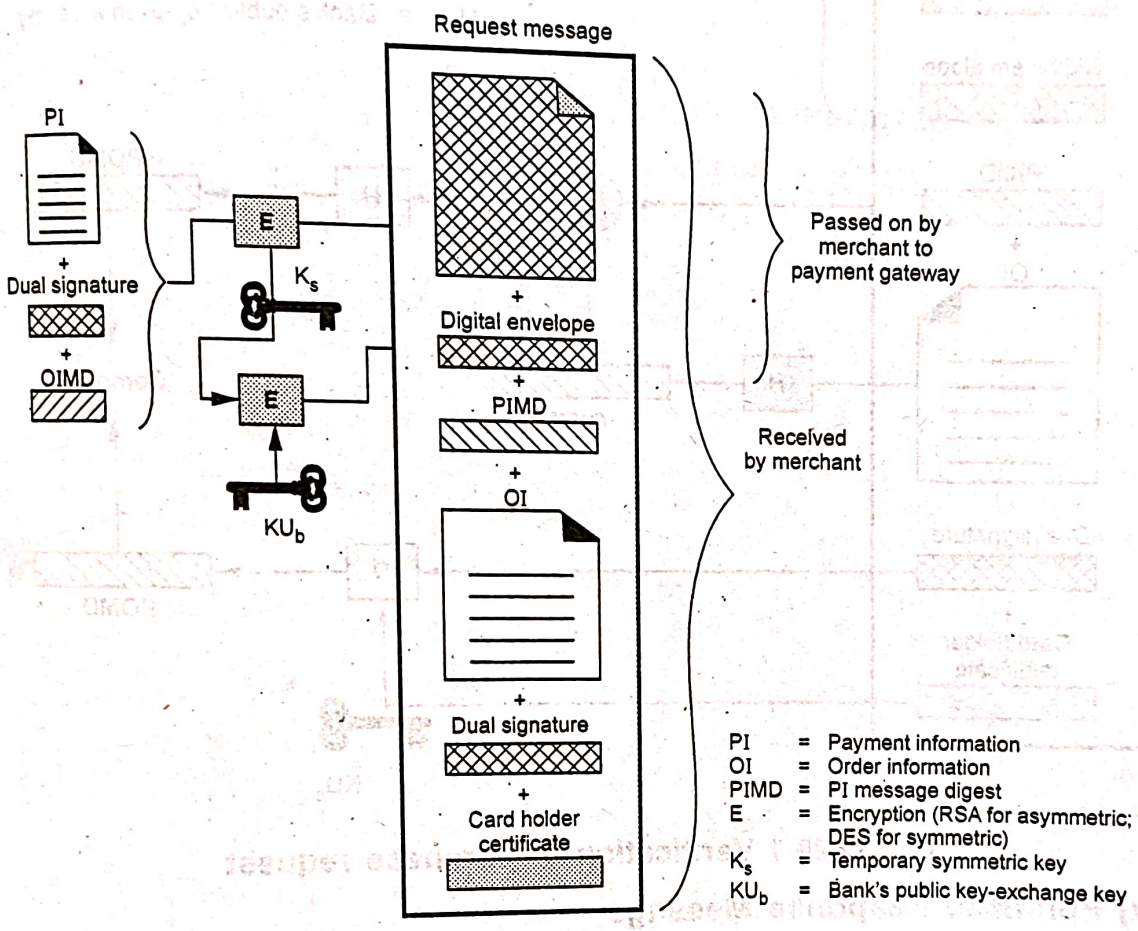


Fig. Q.28.1 Purchase request message generation

Merchant Verifies Purchase Request

- When the merchant receives the purchase request message, it performs the following actions :
  - Verify the cardholder certificates by means of its CA signatures.
  - Verifies the dual signature using the customer's public key signature.

Processes the order and forwards the payment information to the payment gateway for authorization.

Sends a purchase response to the cardholder. (Refer Fig. Q.28.2)

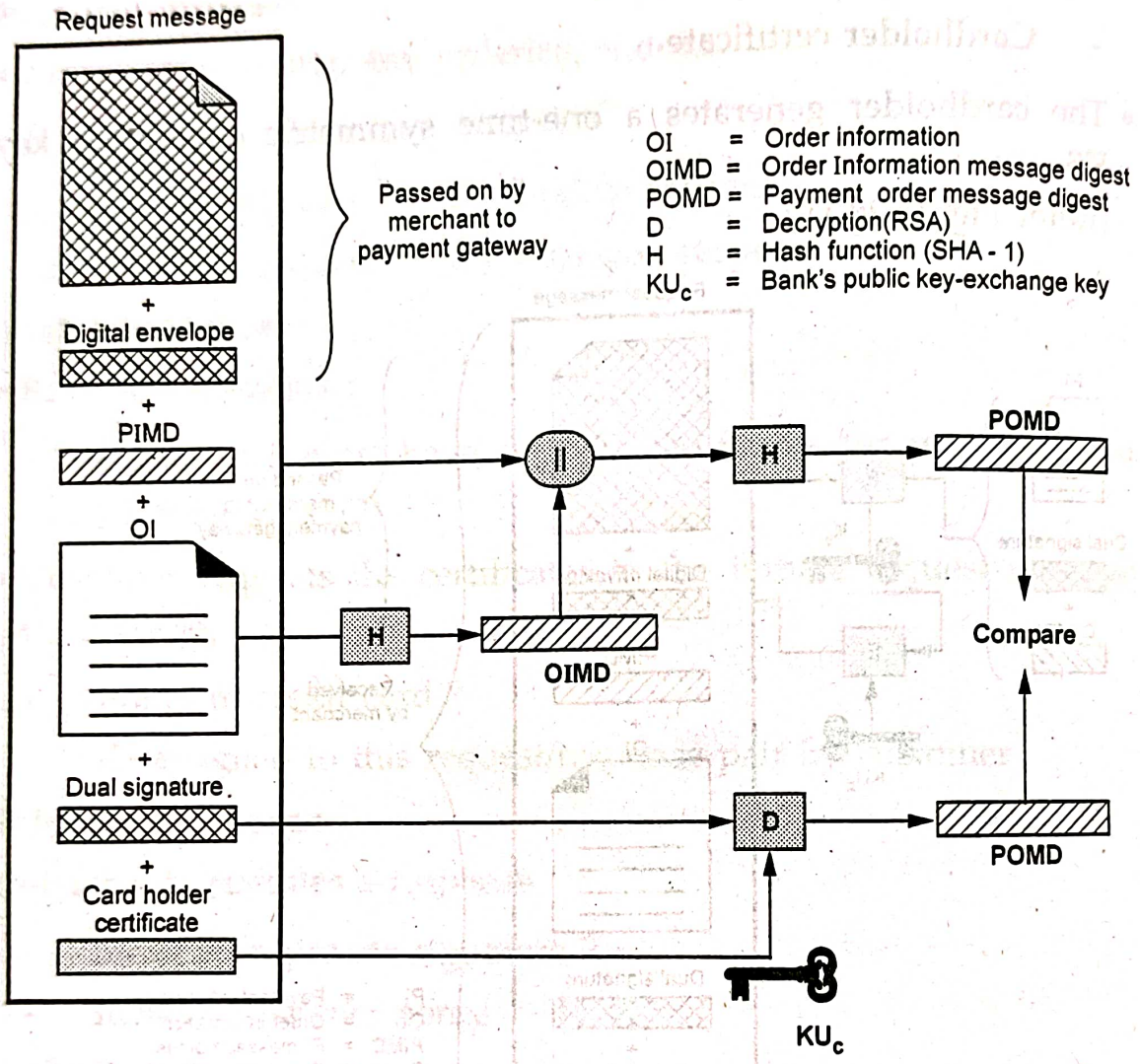


Fig. Q.28.1 Verification of purchase request

iv) Purchase Response Message

- Message that acknowledges the order and references corresponding transaction number.
- Block is,
  - Signed by merchant using its private key
  - Block and signature are sent to customer along with merchant's signature certificate

- Upon reception
  - Verifies merchant certificate
  - Verifies signature on response block
  - Takes the appropriate action

Q.29 What is dual signature ? How it is used in SET ?

Ans. : • Dual signature is needed for linking two messages that are intended for two different receiver Order Information and Payment Information (OI and PI).

• The operation of dual signature can be summarized as,

$$DS = E(PRc, [H(H(PI) \| (OI)])$$

where,

PRc, is customer's private signature key

PI is payment information

OI is order information

H is Hash function

|| is concatenation

E is encryption (RSA)

• Dual signature limit the information on need to know basis i.e. merchant does not need credit card number and bank does not need details of customer order. This provides extra protection interms of privacy.

• Fig. Q.29.1 shows implementation of dual signatures.

Why Dual Signature ?

• Suppose that customer send the merchant two messages :

1. The signed Order Information (OI)
2. The signed Payment Information (PI)

• In addition, the merchant passes the Payment Information (PI) to the bank. If the merchant can capture another Order Information (OI) from this customer, the merchange could claim this order

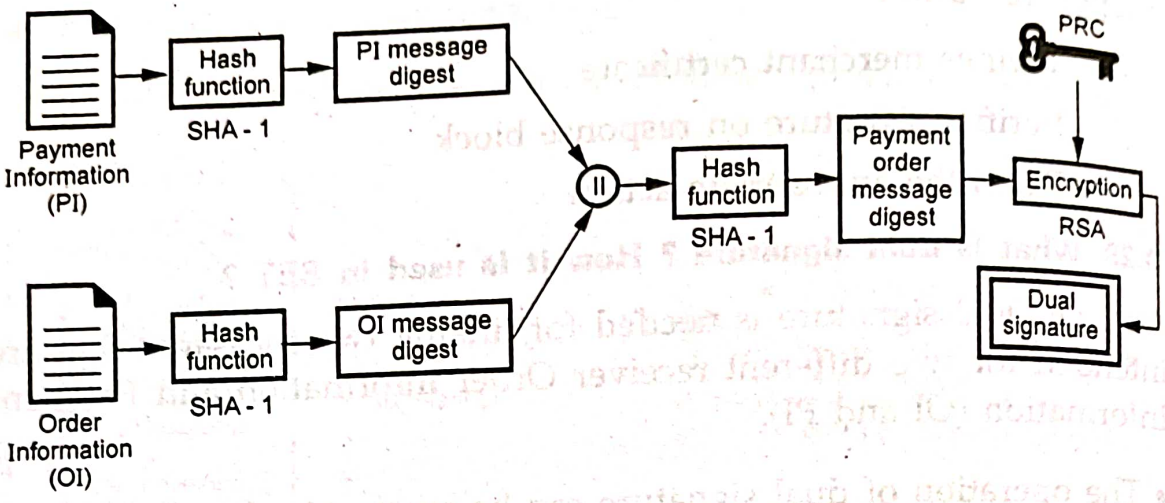


Fig. Q.29.1 Generation of dual signature

goes with the Payment Information (PI) rather than the original. Dual signature confirms the payment is made for specific order.

A] DS Verification by Merchant

- The merchant has the public key of the customer obtained from the customer's certificate.
- Now, the merchant can compute two values :

  H(PIMD || H(OI)

  DKUC[DS]

- Should be equal.

B] DS Verification by Bank

- The bank is in possession of DS, PI the message digest for OI [OIMD] and the customer's public key, then the bank can compute the following :

  H(H(PI) || OIMD)

  DKUC[DS]

Q.30 List and explain various participants involved in Secure Electronic Transaction (SET).

Ans. : • Following are the participants of SET system.

a) Card holder

b) Merchant

c) Issuer

d) Acquirer

e) Payment gateway

f) Certification authority

- The sequence of event in SET system is as follows :

1. Customer opens an account
2. Customer receives a certificate
3. Merchant's certificate
4. Customer places an order
5. Verification of merchant
6. Order and payment sent
7. Request for payment authorization by merchant
8. Merchant confirms order
9. Merchant provides goods or service
10. Merchant requests payment

END...

Unit V

5 Firewall and Intrusion

5.1 : Computer Intrusions

Q.1 What is an intruder ? Explain different classes of intruders and intrusion techniques.

Ans. : • An intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.

- Three classes of intruders are Masquerader, Misfeasor, and Clandestine user.

1. **Masquerader :** An unauthorized user who penetrates a computer system's access control and gains access to user accounts.
2. **Misfeasor :** A legitimate user who accesses resources he is not authorized to access. Who is authorized such access but misuses his privileges.
3. **Clandestine user :** A user who seizes the supervisory control of the system and uses it to evade auditing and access control.

Intrusion techniques

- **Objective :** An intruder wants to gain access to a system.
- Access is generally protected by passwords. System maintains a file that associates a password with each authorized user.
- Password file can be protected with : **One-way encryption and access control**

1. **One way function :** A system stores passwords only in encrypted form. When user presents a password, the system

transforms that password and compares it with the stored value.

2. **Access control :** Access to the password file is limited to very few people.

Techniques for guessing passwords

1. Try default passwords. (Used with standard accounts that is shipped with systems.)
2. Try all short words, 1 to 3 characters long.
3. Try all the words in an electronic dictionary.
4. Collect information about the user's hobbies, family names, birthday, etc.
5. Try user's phone number, social security number, street address, etc.
6. Try all license plate numbers (AP 12 AA 4453).
7. Use a trojan horse.
8. Tap the line between a remote user and the host system.

5.2 : Firewall

Q.2 Explain architecture of firewall.

Ans. : • A firewall is inserted between the Internet and LAN for security purpose. The firewall protects the LAN from Internet-based attacks and also provides security and audits.

- A firewall may be a hardware or a software program running on a secure host computer. A firewall is placed at junction or gateway between the two networks.
- A firewall must have at least two network interfaces one for the network it is intended to protect and one for the network and other for the network it is exposed to.
- A firewall placed between a private or corporate network and a public network is shown in Fig. Q.2.1.

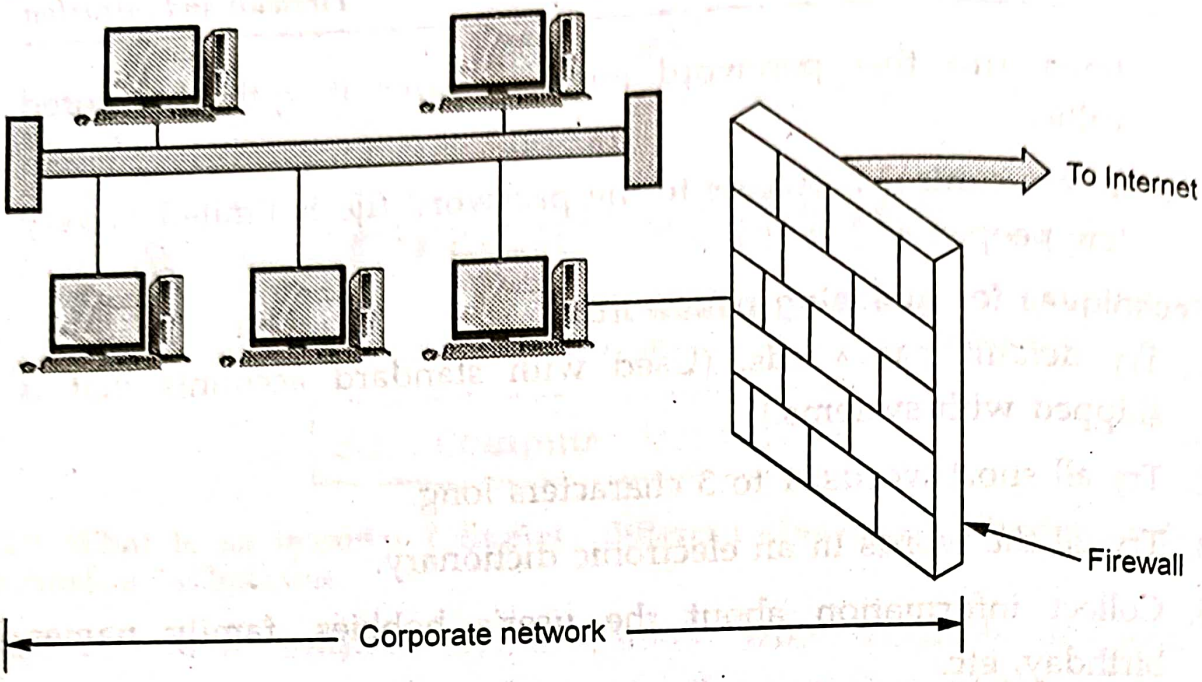


Fig. Q.2.1 Firewall

- A firewall examines all traffic routed between the two networks to see if it meets the certain criteria. If it does, it is routed between the networks, otherwise it is stopped.
- A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted.
- Firewalls can filter packets based on their source and destination addresses and port numbers. This known as address filtering.
- Firewalls can also filter specific types of network called protocol filtering because the decision to forward or reject traffic is dependent upon the protocol used. For example, HTTP,FTP, Telnet.
- Firewalls can also filter traffic by packet attribute or state

Q.3 What are the various characteristics of firewall ?

Ans. : Firewall characteristics :

1. All traffic from inside to outside, and vice-versa, must pass through the firewall.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.
3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system.
4. A firewall can serve as the platform for IPsec.
5. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
6. A firewall is a convenient platform for several Internet functions that are not security related

Q.4 Describe types of firewall in detail.

OR Explain the firewall types with its operation.

OR Describe operation of packet filtering firewall.

Ans. : Types of firewall :

1. Packet filtering router
2. Application level gateways
3. Circuit level gateways

Packet filtering router

- Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP. They are usually part of a router.
- Packet filtering router applies rule to each incoming and outgoing IP packet, according forward or discards it. Fig. Q.4.1 shows packet filtering router.
- A router is a device that receives packets from one network and forwards them to another network.

- In a packet filtering firewall each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it or send a message to the originator.

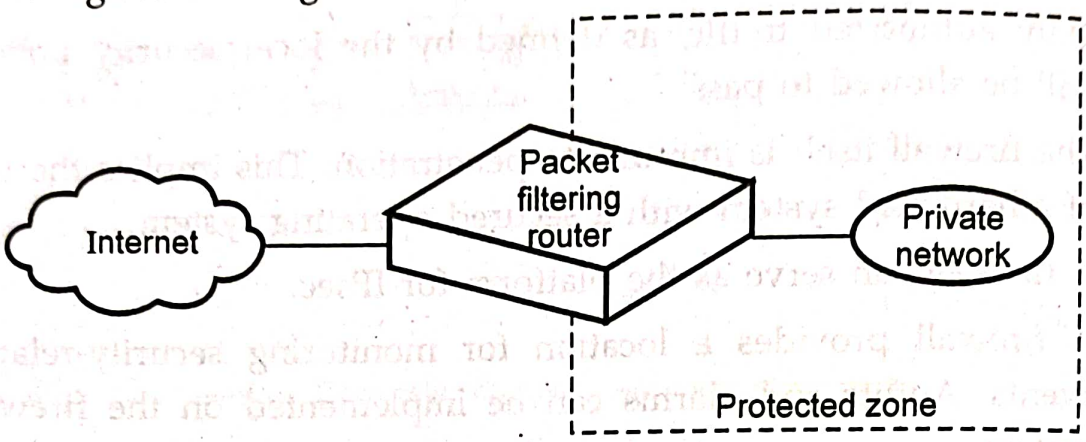


Fig. Q.4.1 Packet filtering router

- Rules can include source and destination IP address, source and destination port number and protocol used.
- Packet filtering provides a useful level of security at low cost. The type of router used in packet filtering is a screening router.
- Packet filters work by dropping packets based on their source and destination addresses or ports. Configuring a packet filter is a three step process.
- First of course, one must know what should and what should not be permitted. Next, the allowable types of packets must be specified, in terms of local expression on packet fields.
- Finally the expression should be rewritten in whatever syntax your vendor supports.

Application Level Gateways

- Application level gateways, also called proxies, are similar to circuit level gateways except that they are application specific. They can filter packets at the application layer of the OSI model.
- Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, an application level gateway that is configured to be a web proxy will not allow any FTP, gopher, Telnet or other traffic through.

- Because they examine packets at application layer, they can filter application specific commands such as http:post and get, etc.
- This cannot be accomplished with either packet filtering firewalls or circuit level neither of which know anything about the application level information.
- Fig. Q.4.2 shows application level gateway.

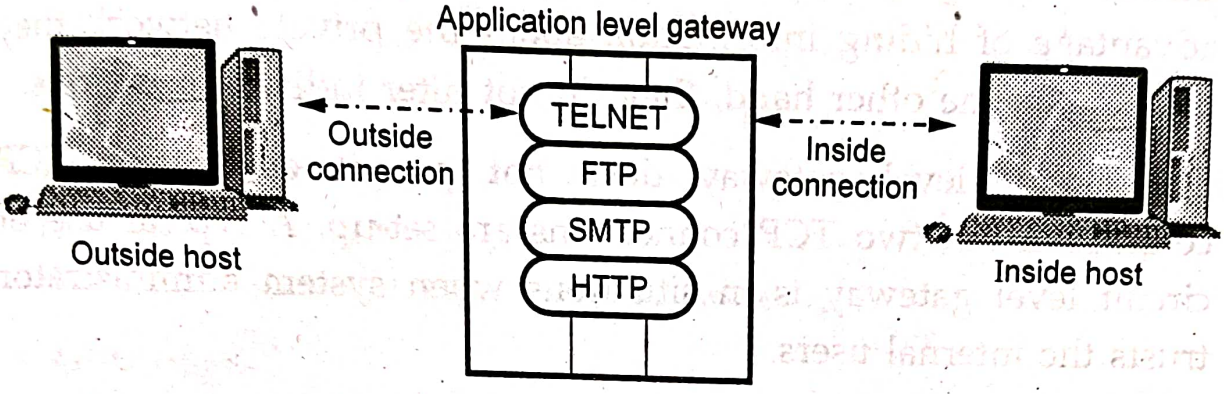


Fig. Q.4.2 Application gateway

- Application level gateways can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on network performance.
- This is because of context switches that slow down network access dramatically. They are not transparent to end users and require manual configuration of each client computer.

Circuit level gateways

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. They monitor TCP handshaking between packets to determine whether a requested session is legitimate.
- Information passed to remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks.
- Fig. Q.4.3 shows circuit gateway.

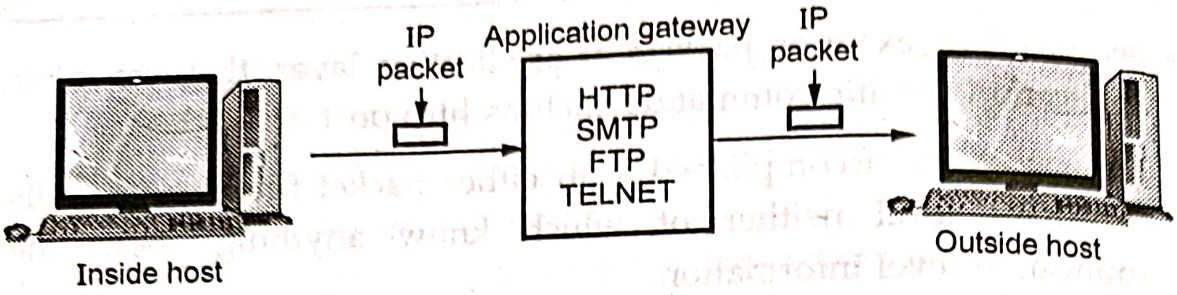


Fig. Q.4.3 Circuit gateway

- Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.
- The circuit level gateway does not permit end-to-end TCP connection but two TCP connections are set-up. A typical use of circuit level gateway is in situations when system administrator trusts the internal users.

Q.5 Describe screened subnet firewall architecture.

Ans. : • Fig. Q.5.1 shows screened subnet firewall architecture.

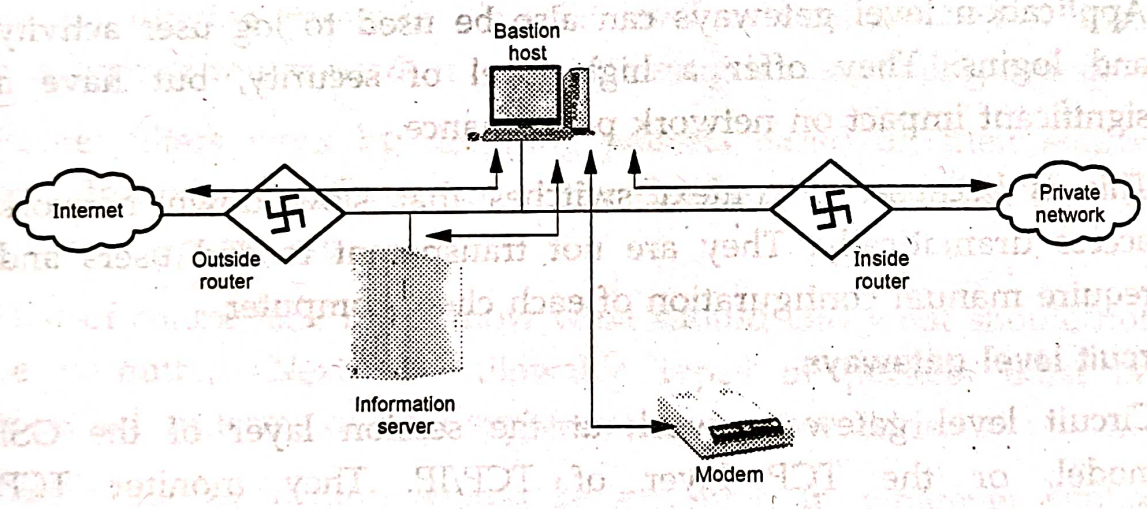


Fig. Q.5.1 Screened subnet

- This configuration creates an isolated subnetwork which may consists of simply the bastion host but may also include one or more information servers and modems for dial-up capability.
- The architecture of a screened subnet firewall provides a DMZ. The DMZ can be a dedicated port on the firewall device linking a single bastion host, or it can be connected to a screened subnet.

- Until recently, servers providing services through an untrusted network were commonly placed in the DMZ.
- Examples of these include Web servers, File Transfer Protocol (FTP) servers, and certain database servers. More recent strategies using proxy servers have provided much more secure solutions.
- A common arrangement finds the subnet firewall consisting of two or more internal bastion hosts behind a packet filtering router, with each host protecting the trusted network.
- There are many variants of the screened subnet architecture. The first general model consists of two filtering routers, with one or more dual-homed bastion hosts between them.
- Advantages
  1. There are now three levels of defense to thwart intruders.
  2. Internal network is invisible to the Internet.
  3. The systems on the inside network cannot construct direct routes to the internet.

5.3 : Trusted System

Q.6 What is trusted system ?

OR What is trusted system ? Explain in brief.

Ans. : • Another widely applicable requirement is to protect data or resources on the basis of levels of security, as is commonly found in the military where information is categorized as Unclassified (U), Confidential (C), Secret (S), Top Secret (TS) or Higher.

- Here subjects have varying rights of access to objects based on their classifications. This is known as multilevel security. A system that can be proved to enforce this is referred to as a **trusted system.**
- The general statement of the requirement for multilevel security is that a subject at a high level may not convey information to a

subject at a lower or incompatible level unless that flow accurately reflects the will of an authorized user. This can be implemented using the **Bell LaPadula Model,** in which a multilevel secure system must enforce :

1. **No read up :** A subject can only read an object of less or equal security level - Simple Security Property.
2. **No write down :** A subject can only write into an object of greater or equal security level - * (star) Property.

- These two rules, if properly enforced, provide multilevel security.

Bell LaPadula model

- The BLP model was developed in the 1970s as a formal model for access control. The model relied on the access control concept. In the model, each subject and each object is assigned a security class. In the simplest formulation, security classes form a strict hierarchy and are referred to as security levels. One example is the U.S. military classification scheme : *top secret* > *secret* > *confidential* > *restricted* > *unclassified.*
- It is possible to also add a set of categories or compartments to each security level, so that a subject must be assigned both the appropriate level and category to access an object.
- This concept is equally applicable in other areas, where information can be organized into gross levels and categories and users can be granted clearances to access certain categories of data. For example, the highest level of security might be for strategic corporate planning documents and data, accessible by only corporate officers and their staff; next might come sensitive financial and personnel data, accessible only by administration personnel, corporate officers and so on. This suggests a classification scheme such as *strategic* > *sensitive* > *confidential* > *public.*
- A subject is said to have a security clearance of a given level; an object is said to have a security classification of a given level. The

security classes control the manner by which a subject may access an object.

- The model defined four access modes

1. **READ :** The subject is allowed only read access to the object.
2. **APPEND :** The subject is allowed only write access to the object.
3. **WRITE :** Tthe subject is allowed both read and write access to the object.
4. **EXECUTE :** The subject is allowed neither read nor write access to the object but may invoke the object for execution.

5.4 : Access Control

Q.7 List and explain any two password management practices.

Ans. : • Password is a front line protection against the unauthorized access (intruder) to the system. A password authenticate the identifier (ID) and provides security to the system. Therefore almost all systems are password protected.

1] Password vulnerability

Passwords are extremely common. Passwords can often be guessed. Use of mechanisms to keep passwords secret does not guarantee that the system security can not be broken. It only says that it is difficult to obtain passwords. The intruder can always use a trial and error method. A test of only a limited set of potential strings tends to reveal most passwords because there is a strong tendency for people to choose relatively short and simple passwords that they can remember. Some techniques that may be used to make the task of guessing a password difficult are as follows :

1. Longer passwords.
2. Salting the password table.
3. System assistance in password selection.

The length of a password determines the ease with which a password can be found by exhaustion. For example, 3-digit password provides 1000 variations whereas a four digit passwords provides 10,000 variations. Second method is the system assistance. A password can be either system generated or user selected. User selected passwords are often easy to guess. A system can be designed to assist users in using passwords that are difficult to guess.

2] Encrypted passwords

Instead of storing the names and passwords in plain text form, they are encrypted and stored in cipher text form in the table. In this case, instead of directly using a user specified name and password for table lookup, they are first encrypted and then the results are used for table lookup. If the stored encoded password is seen, it can not be loaded, so the password cannot be determined. The password file does not need to be kept secret.

3] One time passwords

Set of paired passwords solve the problem of password sniffing. When a session begins, the system randomly selects and presents one part of a password pair; user must supply the other part. In this, user is challenged and must respond with the correct answer to that challenge. In this method, the password is different in each instance. One time passwords are among the only ways to prevent improper authentication due to password exposure. Commercial implementations of one time password system such as secur ID, use hardware calculators.

Password selection strategies

- Too short password is too easy to guess. If the passward is 8 random character, it is impossible to crack the password. In order to eliminate gaussable passwords four basic techniques are suggested.
  1. User education
  2. Computer generated password

3. Reactive password checking
4. Proactive password checking

Q.8 What is access control security service ?

Ans. : • Access control is an important tool of security to protect data and other resources.

- The access control mechanism refers to prevention of unauthorized use of a resource.
- Access control includes :
  1. Authentication of users
  2. Authorization of their privileges
  3. Auditing to monitor and record user actions.
- Three types of access controls system are :
  1. Discretionary access control
  2. Mandatory access control
  3. Role-based access control

Discretionary Access Control (DAC)

- When user set an access control mechanism to allow or deny access to an object (system resource), such a mechanism is a Discretionary Access Control (DAC).
- The Discretionary Access Control (DAC) is also called as an Identity-Based Access Control (IBAC).
- A Discretionary Access Control (DAC) policy is a means of assigning access rights based on rules specified by users.
- The DAC policies include the file permissions model implemented by nearly all operating systems. In Unix, for example, a directory listing might yield "... rw, xr-xr-x ... file.txt", meaning that the owner of file.txt may read, write, or execute it, and that other users may read or execute the file but not write it. The set of access rights in this example is {read, write, execute}, and the operating system mediates all requests to perform any of

these actions. Users may change the permissions on files they own, making this a discretionary policy.

- Discretionary Access Control List (DACL) determines which users and groups can access the object (system resource) for operations. It consists of a list of Access Control Entries (ACEs).

Q.9 Write short note on : Mandatory access control.

Ans. : • When a system mechanism controls access to an object and an individual user cannot alter that access, then such a control is called as Mandatory Access Control (MAC).

- Mandatory Access Control (MAC) is also called as rule-based access control.
- Mandatory access control is a more restrictive scheme that does not allow users to define permissions on files, regardless of ownership. Instead, security decisions are made by a central policy administrator.
- Each security rule consists of a subject, which represents the party attempting to gain access, an object, referring to the resource being accessed, and a series of permissions that define the extent to which that resource can be accessed.

Elements of MAC

- MAC has two key elements :

1. Labels :

- In a system using MAC, every entity is an object (laptops, files, projects, etc.) and is assigned a classification label.
- These labels represent the relative importance of the object, such as confidential, secret, and top secret. Subjects (users, processes, etc.) are assigned a privilege label (sometimes called a clearance).

2. Levels :

- A hierarchy based on the labels is also used, both for objects and subjects.

- Top secret has a higher level than secret, which has a higher level than confidential.

MAC Implementations

- Major implementations of MAC are :

1. **Lattice model :** Security levels for objects and subjects are ordered as a lattice.
2. **Bell-LaPadula confidentiality model :** Advanced version of the lattice model (actually this uses a mix of MAC and DAC).

Q.10 Write short note on : Role based access control.

Ans. : • A user is an entity that wishes to access resources of the organization to perform a task. Usually, users are actual human users, but a user can also be a machine or application.

- A role is defined as a collection of users with similar functions and responsibilities in the organization. Examples of roles in a university may include "student," "alum," "faculty," "dean," "staff," and "contractor." In general, a user may have multiple roles.
  - Roles and their functions are often specified in the written documents of the organization.
  - The assignment of users to roles follows resolutions by the organization, such as employment actions (e.g. hiring and resignation) and academic actions (e.g., admission and graduation).
- Role-Based Access Control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.
- In RBAC, the rights and permissions are assigned to roles instead of individual users.
- RBAC is also called as Non-Discretionary Access Control (NDAC).

- This added layer of abstraction permits easier and more flexible administration and enforcement of access controls.
- The RBAC framework provides administrators with the capability to regulate who can perform what actions, when, from where, in what order, and in some cases under what relational circumstances.
- RBAC is important because it provides customers a greater degree of control over cloud resource utilization with the added layer of system security.
- RBAC should be implemented in the following situations :

1. In an effort to minimize downtime and accidental changes to the cloud resources, the account owner would like to restrict access to the accounts to only a few people.
2. In an effort to synchronize cloud product access to the functions of an employee's job, the account owner would like to grant access to employees based on the nature of their position.
3. In an effort to help prevent unauthorized access to cloud products through the sharing of admin credentials, the account owner would like each user of the cloud accounts to have their own credentials.

5.5 : Intrusion Detection System (IDS)

Q.11 What are the challenges of intrusion detection ?

Ans. : Challenges of intrusion detection :

- Runtime limitations
- Specification of detection signatures
- Dependency on environment

- A good intrusion detection system alert should produce a corresponding response.
- Network-based IDS sensors must be deployed in areas where they can "see" network traffic packets. However, in switched networks this is not possible because by their very nature, sensors in switched networks are shielded from most of the network traffic. Sensors are allowed to "see" traffic only from specified components of the network.
- The technology is not yet ready to handle a large-scale attack. Because of its very nature it has to literally scan every packet, every contact point, and every traffic pattern in the network. For larger networks and in a large-scale attack, it is not possible that the technology can be relied on to keep working with acceptable quality and grace.

Q.12 Explain anomaly based intrusion detection system.

OR Explain operation of anomaly based intrusion detection system in detail.

Ans. : Anomaly detection

- An anomaly based intrusion detection system is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.
- It examines ongoing traffic, activity, transactions, and behaviour in order to identify intrusions by detecting anomalies.
- For instance, anomaly-based IDS will detect that an IP packet is malformed. It does not detect that it is malformed in a specific way, but indicates that it is anomalous.
- The classification is based on heuristics or rules, rather than patterns or signatures, and will detect any type of misuse that falls out of normal system operation.
- Anomaly detectors construct profiles representing normal behavior of users, hosts, or network connections. These profiles are constructed from historical data collected over a period of normal operation.

- The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the norm.
- Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.
- The measures and techniques used in anomaly detection include : Threshold detection, statistical measures, and rule-based measures.

Advantages of anomaly detection

1. IDSs based on anomaly detection detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details.
2. Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.

Disadvantages of anomaly detection

1. Anomaly detection approaches usually produce a large number of false alarms due to the unpredictable behaviors of users and networks.
2. Anomaly detection approaches often require extensive "training sets" of system event records in order to characterize normal behavior patterns.

Q.13 Explain types of intrusion detection system.

OR List and explain types of intrusion detection system.

OR Explain the operation of misused based intrusion detection system.

Ans. : Types of intrusion detection system are as follows :

1. Anomaly detection
2. Signature-based detection
3. Network based System
4. Host-based IDSs

Signature based detection

- A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from

known malicious threats. This is similar to the way most antivirus software detects malware.

- A common strategy for IDS in detecting intrusions is to memorize signatures of known attacks. The inherent weakness in relying on signatures is that the signature patterns must be known first.
- New attacks are often unrecognizable by popular IDS. Signatures can be masked as well. The ongoing race between new attacks and detection systems has been a challenge.
- It is also called misuse detection.

Network based system

- A Network Intrusion Detection System (NIDS) is tries to detect malicious activity such as denial of service attacks; port scans or even attempts to crack into computers by network security monitoring of network traffic.
- Network intrusion detection systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.
- Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, there by protecting those hosts.
- Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network.
- These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console.
- As the sensors are limited to running the IDS, they can be more easily secured against attack.
- Many of these sensors are designed to run in stealth mode, in order to make it more difficult for an attacker to determine their presence and location.

Host-based IDSs (HIDS)

- Host based monitors system logs for evidence of malicious or suspicious application activity in real time.
- It requires small programs or agents to be installed on individual systems to be monitored. The agents supervise the OS and write data to log files and activate alarm.
- Host-based IDSs operate on information collected from within an individual computer system.
- Host-based IDSs normally utilize information sources of two types, operating system audit trails, and system logs.
- Operating system audit trails are usually generated at the innermost (kernel) level of the operating system, and are therefore more detailed and better protected than system logs.
- System logs are much less obtuse and much smaller than audit trails, and are furthermore far easier to comprehend.

Q.14 Explain method for intrusion detection system.

Ans. : • Intrusion detection techniques are as follows :

1. **Threshold detection :** It records each occurrence of suspicious events and compares it with a threshold number. Threshold detection involves counting no occurrences of a specific event type over an interval of time, if count surpasses a reasonable number, then intrusion is assumed establishing threshold number is difficult.
2. **Anomaly detection :** It requires little knowledge of the actual system beforehand. Usage patterns are established automatically by means of neural networks.
3. **Rule based detection :** Observe events on system and apply rules to decide if activity is suspicious or not. Analyze historical audit records to identify usage patterns and auto-generate rules for them. Then observe current behavior and match against rules to see if conforms. Like statistical anomaly detection does not require prior knowledge of security flaws.

END...

Unit VI

6 Cyber Forensic, Hacking & its Countermeasures

6.1 : Personally Identifiable Information (PII)

Q.1 Explain with example PII.

Ans. : Introduction to Personally Identifiable Information (PII)

- Personally Identifiable Information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for anonymous data can be considered PII.
- It consists of a broad range of information that can identify individuals, including dates of birth, addresses, driver's license numbers, credit card numbers, bank account numbers, health and insurance records and much more.
- Privacy concerns exist wherever personally identifiable information or other sensitive information is collected and stored - in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as :

1. Healthcare records
2. Criminal justice investigations and proceedings
3. Financial institutions and transactions
4. Biological traits, such as genetic material
5. Residence and geographic records
6. Ethnicity

7. Privacy breach
8. Location-based service

- Privacy rules set out obligations in respect of two classes of information: "Personal Information", which includes any information that relates to a natural person, which directly or indirectly, is capable of identifying a person; and a smaller subset of Personal Information known as SPDI (Sensitive Personal Data or Information), which is information relating to passwords, financial information, health information, sexual orientation, medical records and biometric information. This accounts to the sensitive data which needs to be protected.
- For example, in a hospital, the patient records which is private information should be accessed only by the Doctor who is treating the patient and the Nurse who is on duty with the patient. Any other nurse or doctor in the hospital should not have access to those medical records.
- Any collection, processing, storage, use or transfer of personal information or SPDI which takes place through a computer or computer network located in India would have to comply with the IT Act and Privacy Rules.
- Protecting PII example scenario: A HR manager needs to provide important papers to a pension company.The company's network security solution must provide :
  1. Encryption that will keep the data safe if the manager's laptop is lost or stolen.
  2. Threat protection to keep his PC safe from viruses, phishing and other threats.
  3. Data loss prevention that will warn him he is about to send a file with PII.
  4. Policy compliance that will block him from using a browser with a known security vulnerability or stop him from saving the file to an unencrypted USB stick.

5. Blocking of anonymous proxies for web searches, because they allow personal information to be accessed by administrators of the proxy server.

6.2 : Cyber Stalking

Q.2 Explain cyber stalking.

Ans. : Cyber Stalking

Definition of stalking : *Threatening behavior or unwanted advances directed at another using the Internet and other forms of online and computer communications.*

- Cyber stalking is defined as the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals.
- Stories of criminal intimidation, harassment, fear, and suggestive violence where individuals use the Internet as a tool to stalk another person.
- Stalkers use victim information like mobile numbers, telephone numbers, addresses, and personal preferences to impinge upon their normal life. Some time cyber stalkers can learn what sorts of things upset their victims and can use this knowledge to harass the victims further.
- Stalkers target victims through chat rooms, WhatsApp, Hangouts, e-mail, facebook etc.
- Different forms of cyber stalking : Threatening e-mails, spam, and online verbal abuse, inappropriate messages on message boards, computer viruses, tracing internet activity, and identity theft.
- Effects of cyber stalking on person :
  1. Changes in sleeping and eating patterns
  2. Nightmares
  3. Hyper vigilance

4. Anxiety
5. Helplessness
6. Fear for safety
7. Shock and disbelief

- Cyber stalking damages multiple aspects of victims' lives, from study to professional activity to their relationships with others. Survey respondents reported changing or losing jobs, isolating themselves by giving up social activities, and having important relationships break up.
- The Delhi police registered India's first case of cyber stalking. A case was registered under section 509 of the Indian Penal Code. One Mrs. Neha (Name changed) complained to the police against a person who was using her identity to chat over the Internet. She also complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was giving her telephone number to other chatters encouraging them to call her at odd hours.
- Stalkers usually make harassing phone calls, leave written messages or objects, or vandalize a person's property. Cyber stalkers meet or target their victims by using different search engines, bulletin and discussion boards, and online forums.
- Cyber stalkers use different social network sites and self publishing media such as Facebook, Twitter, Friendster, Bebo, Myspace and Indymedia etc. They try to damage the reputation of their victims by posting false information on websites, blogs or user pages. Many cyber stalkers use third parties to encourage them to join in their pursuit.
- They may order pornographic materials and sex toys, having them sent to their victim's address. Some cyber stalkers may arrange to meet their victims, especially young people who are at high risk of becoming their victims.

- Most stalking behavior is not a crime, at least not by itself. Calling someone over and over, texting numerous messages and leaving gifts are common behaviors that, on their own, do not constitute a crime.
- Section 354D says that anyone who monitors an individual's electronic communication and causes fear or distress is guilty of stalking, just as they are if they follow or attempt to contact them in the real world. The offender could get a fine and three years in jail.
- India is finally waking up to cyber stalking with the Criminal Law (Amendment) Bill, 2013, saying that stalking includes monitoring of a person's use of internet, email and electronic communication.
- Section 66A of the IT Act deals with cyber stalking. "A person who repeatedly sends emails can be booked under 66A, but not many know this,"
- Two different kinds of cyber stalking situations which can occur.
  1. Online harassment and cyber stalking that occurs and continues on the internet.
  2. Online harassment and stalking that begins to be carried on offline too. This is when a stalker may attempt to trace a telephone number or a street address. Always be careful what details you give out over the web and to whom.
- The increasing use of the Internet and the ease with which it allows others unusual access to personal information, have made this form of stalking ever more accessible. Potential stalkers may find it easier to stalk via a remote device such as the Internet rather than to confront an actual person. You cannot stop the contact with a request. In fact, the more you protest or respond, the more rewarded the cyber stalker feels. The best response to cyber stalking is not to respond to the contact.

Q.3 Explain types of cyber stalkers.

Ans. : Types of Stalkers

- There are three main types of stalkers :

1. Simple obsessional 2. Delusional 3. Vengeful

Simple obsessional stalkers or domestic

- This is the most common type of stalker.
- Stalker, usually male, knows victim as an ex-spouse, ex-lover, or former boss, who they attempt to establish a relationship with and when rebuffed begin a campaign of harassment.
- This category represents 70 - 80 % of all stalking cases and is distinguished by the fact that some previous personal or romantic relationship existed between the stalker and the victim before the stalking behavior began.
- This kind of stalker may or may not have psychological disorders, all clearly have personality disorders. They refuse to believe that the relationship is over despite being told several times. They may have a history of other criminal behaviors.
- The love-obsessional stalker, who is typically a psychotic stalker targeting famous people or total strangers; and, most common. Stalker is a stranger to the victim but is obsessed with the victim and when rejected mounts a campaign of harassment to make the victim aware of the stalker's feelings.

Delusional stalkers

- Often have little contact with their victims
- Could have a mental disorder
- Often are unmarried, socially immature, isolated loners
- Typically choose a victim that is unattainable or who has shown them kindness in some way...a therapist, celebrity, clergy, teacher, doctor, etc.
- Can be dangerous and usually the rarest category of stalker.

- False belief that the victim shares the stalker's feelings and desire for a relationship.
- Here relationship based on stalker's psychological fixation. It also based on idealized love or spiritual union rather than sexual attraction.
- Target is usually a person with high visibility and a higher status.
- The danger period for a delusional is when they are falling out of love with one victim and in love with another victim.

Vengeful stalkers

- **Vengeful stalkers** may or may not have contact with their victims. They become angry with their victims over some real or perceived event or insult.
- They are as dangerous as delusional stalkers and are violent.
- Vengeful stalkers thinks you did them wrong and they want to make you pay for it.
- These stalkers may be stalking to get even and take revenge and believe that "they" have been victimized. Ex-spouses can turn into this type of stalker.

6.3 : PII Impact Levels with Examples

Q.4 Explain three impact levels of PII.

Ans. : PII Impact Levels with Examples

- The following describe the three impact levels : low, moderate and high

1. Low

- The potential impact is LOW if the loss of confidentiality, integrity or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.

- A limited adverse effect means that, for example, the loss of confidentiality, integrity or availability might
  (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
  (ii) result in minor damage to organizational assets;
  (iii) result in minor financial loss;
  (iv) result in minor harm to individuals.

2. Moderate

- The potential impact is MODERATE if the loss of confidentiality, integrity or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- A serious adverse effect means that, for example, the loss of confidentiality, integrity or availability might
  (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
  (ii) result in significant damage to organizational assets;
  (iii) result in significant financial loss;
  (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

3. High

- The potential impact is HIGH if the loss of confidentiality, integrity or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.
- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity or availability might

i. cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

ii. result in major damage to organizational assets;

iii. result in major financial loss; or

iv. result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

6.4 : Cybercrime

Q.5 What is cyber crime ? Explain types of cyber crime.

Ans. : Cybercrime : • Cyber safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.

- There is no standard definition for "**CYBER**". This word is used to describe the virtual world of computers e.g. an object in cyberspace refers to a block of data floating around a computer system or network.
- The word "cyberspace" is credited to William Gibson, who used it in his book, Neuromancer, written in 1984.
- Cyberspace : The impression of space and community formed by computers, computer networks, and their users ; the virtual "world" that Internet users inhabit when they are online.
- The term 'cyber' is derived from the word 'cybernetics' which means science of communication and control over machine and man.
- Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world.
- Therefore, crimes committed in cyberspace are to be treated as cyber crimes. In wider sense, cyber crime is a crime on the Internet which includes hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, flowing of viruses etc.

- Over the past few years, the global cyber crime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security.
- Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent.
- Cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smart phones and tablet personal computers. In 2010, the number of malicious software programs specifically targeting mobile devices, rose 46 %, according to information technology security group McAfee.
- **Cybercrime** is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.
- **Cybercrime** is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).
- Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.

Types of Cyber Crimes

- There are many types of cyber crimes and the most common ones are explained below :

1. **Hacking :** This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed.
2. **Theft :** This crime occurs when a person violates copyrights and downloads music, movies, games and software.
3. **Cyberstalking :** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails.

4. **Identity Theft :** This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, debit card and other sensitive information to siphon money or to buy things online in the victim's name.
5. **Malicious Software :** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.
6. **Child soliciting and Abuse :** This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography.

Example of cyber crime :

a. Online banking fraud
b. Fake antivirus
c. `Stranded traveler' scams
d. `Fake escrow' scams
e. Advanced fee fraud
f. Infringing pharmaceuticals
g. Copyright-infringing software
h. Copyright-infringing music and video
i. Online payment card fraud
j. In-person payment card fraud
k. Industrial cyber-espionage and extortion
l. Welfare fraud

- The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important Cybercrimes known today.

- Stealing the significant information, data, account number, credit card number transmit the data from one place to another. Hacking and cracking are amongst the gravest Cybercrimes known till date.

Q.6 Explain Botnet.

Ans. : Botnets : A botnet is an interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals.

- They're typically used to send spam emails, transmit viruses and engage in other acts of cybercrime. Sometimes known as a zombie army, botnets are often considered one of the biggest online threats today.
- Computers in a botnet, called nodes or zombies, are often ordinary computers sitting on desktops in homes and offices around the world.
- Typically, computers become nodes in a botnet when attackers illicitly install malware that secretly connects the computers to the botnet and they perform tasks such as sending spam, hosting or distributing malware or other illegal files, or attacking other computers.
- Fig. Q.6.1 shows botnet.

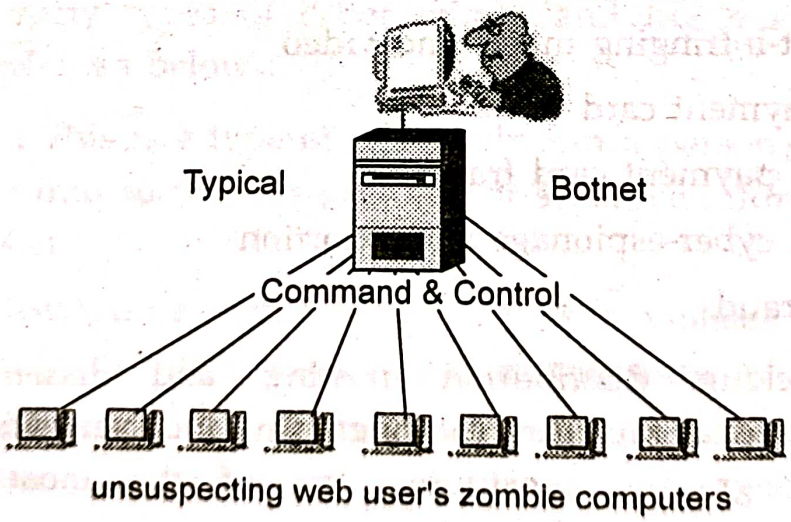


Fig. Q.6.1 Botnet

- Attackers usually install bots by exploiting vulnerabilities in software or by using social engineering tactics to trick users into installing the malware. Users are often unaware that their computers are being used for malicious purposes.
- The word Botnet is formed from the words 'robot' and 'network'. Cybercriminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all of the infected machines into a network of 'bots' that the criminal can remotely manage.
- A zombie or bot is often created through an Internet port that has been left open and through which a small Trojan horse program can be left for future activation. At a certain time, the zombie army "controller" can unleash the effects of the army by sending a single command, possibly from an Internet Relay Channel (IRC) site.
- Botnets can be used to :
  1. Send out spam emails
  2. Launch a Distributed Denial of Service Attack
  3. Commit advertising fraud
  4. Distribute malware, or spyware
- Keep phishing websites active and frequently change their domains to remain anonymous and undetected by law enforcement.

Q.7 Explain zombie compters.

Ans. : • Zombie computer is a computer connected to the Internet that has been compromised and controlled by an attacker without user's consent.

- Zombie network (Botnet) refers to a network of zombie computers under the remote control by an attacker. Attackers control their botnets through some command and control centers to perform illegal activities.

- If your computer is infected by malicious code such as Trojan Horse, your computer may be controlled by an attacker and may become a zombie.
- Types of attacks perpetrated by a zombie network include denial of service attacks, adware, spyware, spam and click fraud.
- The following steps are used to create zombie networks :
  1. A zombie network operator uses a bot to infect thousands of computers with worms or viruses that carry a deadly payload.
  2. The bot inside an infected computer logs on to an online server - usually IRC but sometimes Web.
  3. The zombie network operator leases zombie network services to a customer.
  4. The customer provides the zombie network operator with spam or any other material, which is run through the zombie network.
- Another botnet called, Gameover Zeus Botnet, allows cyber criminals to retrieve banking passwords from infected machines, or use the botnet to infect more computers.

How and why do cyber criminals use botnets ?

- The value of bots and botnets to criminals comes from aggregating massive numbers of computers they can control simultaneously to perform malicious activities.
- Cyber criminals may use the botnets to send spam, phishing emails, or other scams to trick consumers into giving up their financial information.
- Cyber criminals may also collect information from the bot-infected machines and use it to steal identities, incurring loans, and purchase charges under the user's name.
- Cyber criminals may use botnets to create denial-of-service (DoS) attacks that flood a legitimate service or network with a crushing

volume of traffic. The volume may severely slow down, or even shut down, the organization's business operations.

- Revenue from DoS attacks come through extortion and leasing botnets. The criminals will rent botnets to groups interested in inflicting damage to another entity.
- The "renters" will use the botnet for sending spam and phishing emails or attacking legitimate websites and networks.

6.5 : PII Confidentiality Safeguard

Q.8 Write a note on PII Confidentiality Safeguard.

Ans. : PII Confidentiality Safeguards

- Confidential data refers to any data pertaining to individuals or the University that is sensitive, private or of a personal nature or data that is protected under a confidentiality agreement, regulation, law or University procedure.
- The confidentiality of PII should be protected based on its impact level.
- Confidential information means any information not exempted in specific legislation and identified as personal, sensitive or confidential such as personally-identifiable information, individually-identifiable health information, education records and non-public information as specified in all applicable federal or state laws.
- Organizations should evaluate how easily PII can be used to identify specific individuals. For example, PII data composed of individuals' names, fingerprints or SSNs uniquely and directly identify individuals, whereas PII data composed of individuals' ZIP codes and dates of birth can indirectly identify individuals or can significantly narrow large datasets.
- However, data composed of only individuals' area codes and gender usually would not provide for direct or indirect

identification of an individual depending upon the context and sample size.

- Thus, PII that is uniquely and directly identifiable may warrant a higher impact level than PII that is not directly identifiable by itself.
- Organizations should evaluate the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together.
- For example, an individual's SSN, medical history, or financial account information is generally considered more sensitive than an individual's phone number or ZIP code.
- Organizations often require the PII confidentiality impact level to be set at least to moderate if a certain data field, such as SSN, is present.
- Organizations may also consider certain combinations of PII data fields to be more sensitive, such as name and credit card number, than each data field would be considered without the existence of the others.
- Data fields may also be considered more sensitive based on potential harm when used in contexts other than their intended use.
- For example, basic background information, such as place of birth or parent's middle name, is often used as an authentication factor for password recovery at many web sites.

6.6 : IT Act

Q.9 Explain IT Act, 2000. Give aims and Objectives of IT Act.

Ans. : IT Act : The present laws governing Information and Communication Technology have been derived from the Indian Telegraph Act 1885, Indian Wireless Telegraphy Act 1933, The Telegraph Wire Unlawful Possession Act 1950 and the Cable Television Networks (Regulation) Act 1995.

- In the recent past the Telecom Regulatory Authority of India Act 1997 (TRAI Act) was enacted, paving way for the constitution of the first ever telecom regulatory body in India, known as Telecom Regulatory Authority of India (TRAI).
- The TRAI apart from telecom has recently been entrusted with the task of regulating and drafting of policies relating to broadcasting sector.
- The growth of IT industry and e-commerce, lead the government to enact the Information Technology Act 2000 (IT Act 2000).
- The issues relating to cyber crimes, data security, digital signatures, electronic commerce etc are covered under the IT Act 2000.
- The IT Act 2000 grants legal sanction to e-commerce transactions and also prohibits breach of confidentiality and privacy.

Aim and Objectives of IT Act, 2000

- The important aims and objectives of the IT Act, 2000 are :

1. To suitably amend existing laws in India to facilitate e-commerce.
2. To provide legal recognition of electronic records and digital signatures.
3. To provide legal recognition to the transactions carried out by means of Electronic Data Interchange (EDI) and other means of electronic communication.
4. To provide legal recognition to business contacts and creation of rights and obligations through electronic media.
5. To establish a regulatory body to supervise the certifying authorities issuing digital signature certificates.
6. To create civil and criminal liabilities for contravention of the provisions of the Act and to prevent misuse of the e-business transactions.

7. To facilitate e-governance and to encourage the use and acceptance of electronic records and digital signatures in government offices and agencies. This would also make the citizen-government interaction more hassle free.
8. To make consequential amendments in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions.
9. To amend the Reserve Bank of India Act, 1934 so as to facilitate electronic fund transfers between the financial institutions.
10. To amend the Banker's Books Evidence Act, 1891 so as to give legal sanctity for books of accounts maintained in the electronic form by the banks.
11. To make law in tune with Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) adopted by the General Assembly of the United Nations.

Q.10 Explain the importance of IT act.

Ans. :

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects.

a) Firstly, the implication of these provisions for the e-businesses is that email is now a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

b) Companies are now able to carry out electronic commerce using the legal infrastructure provided by the Act.

c) Digital signatures have been given legal validity and sanction in the Act.

d) The Act opens the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signature Certificates.

e) The Act now allows Government to issue notification on the web thus heralding e-governance.

f) The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate. Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

g) The IT Act also addresses the important issues of security, which are critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to be passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the IT Act, 2000, it is possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding ₹ 5 crores.

Q.11 Write note on Information Protection Law : Indian perspective.

Ans. : • The Indian government has created the necessary legal and administrative framework through the enactment of Information Technology Act 2000, which combines the e-commerce transactions and computer misuse and frauds rolled into an Omnibus Act.

• While on the one hand it seeks to create the Public Key Infrastructure for electronic authentication through the digital signatures, on the other hand, it seeks to build confidence among the public that the frauds in the cyber space will not go unpunished. The Controller of Certifying Authority (CCA) has been put in place for the effective implementation of the IT Act, 2000. The Act also enables e-governance applications for the

electronic delivery of services to the public, business and government.

- The Information technology Act, 2000 has been enacted by the legislators with the prime intention of ensuring that the communication through electronic medium is facilitated and all sorts of ambiguity regarding the authenticity of the communication is fixed for once and all.

Also refer Q.9 of Chapter - 6.

6.7 : Cyber Forensic

Q.12 What are different phases of cyber forensics ? Explain with suitable diagram.

Ans. : Fig. Q.12.1 shows different phases of cyber forensics.

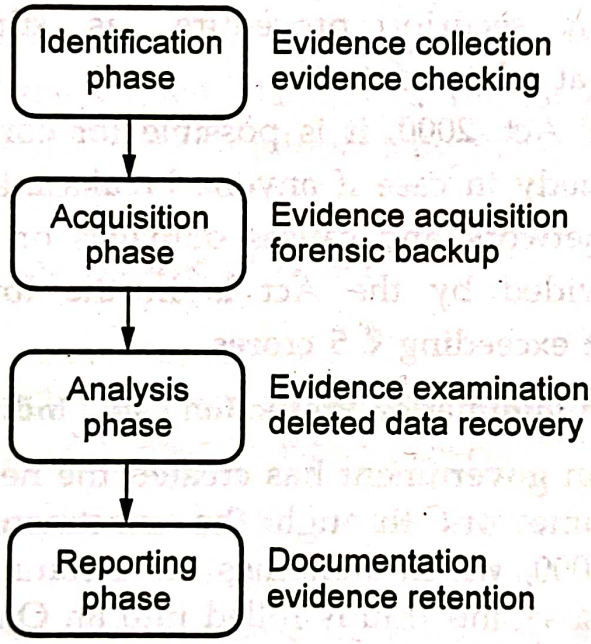


Fig. Q.12.1

1. **Identification :** It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format). Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

2. **Preservation (Acquisition) :** In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.
3. **Analysis :** In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.
4. **Documentation :** In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.
5. **Presentation :** In this last step, the process of summarization and explanation of conclusions is done. However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details

END...