May 2019

Chapter 1 : Security Basics [Total Marks - 05]

Q. 1(a) List and explain various elements of Information security. (5 Marks)

Ans. :

Elements of Information Security

- When we say information security – what exactly are we protecting? What is the asset? The asset here is "Information" or more precisely "Digital Information". The information could be about your Facebook user account, Online bank account, OS password, email or pretty much anything that touches a computer system.
- There are 3 tenets (or pillars) of security :
- These tenets in short are also called as the CIA triad or any other combination of the first letters in their words. These are also sometimes called **goals of security**.

1. Confidentiality

- **Definition :** An act of protecting information from unauthorised disclosure to an entity.
- It ensures that the protected information is kept secret throughout its lifetime and is made available only to the authorised entities as and when needed.
- The information should be
  - **Protected at Rest :** When stored on the disk
  - **Protected in Motion :** When transmitted over the network
  - Protected during Use : When processing
- In terms of digital information, confidentiality is enforced using several mechanisms :
  1. Encryption
  2. Access control
  3. Data classification

2. Integrity

- **Definition :** An act of protecting information from unauthorised modification by an entity.
- For example, during criminal investigations, any evidence that you collect is protected from touching or any modifications to ensure that those evidences can be used during court proceedings. If evidence is tampered, it is not admissible in the court and cannot be used. Another example is email. If I send you an email and someone changes it before you read it, you might get wrong information, or it could be severely damaging to our relations.
- In terms of digital information, integrity is enforced using several mechanisms :
  1. Hashing
  2. Access Control
  3. Data Classification
  4. Input and output sanitization

3. Availability

- **Definition :** An act of protecting information from unauthorised destruction by an entity.
- For example, your Windows or Linux systems track all activities done on the system via log files. If I do some mischief around your computer and then delete the log files, you would have no way to prove that I did something to your computer. The availability of log files is crucial to ensure that the system is adequately monitored and protected from any security mishaps.
- Availability is generally enforced using several mechanisms :
  1. Access control
  2. Isolation
  3. Back up
  4. Disaster Recovery
  5. Business continuity processes
- above 3 security principles summarised in Fig. 1-Q. 1(a).

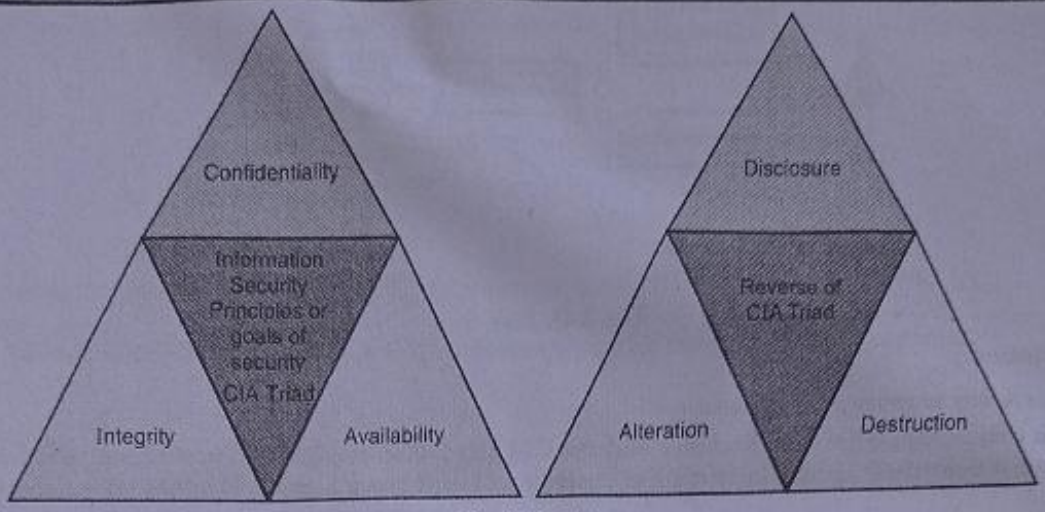


Fig. 1-Q. 1(a)

- Confidentiality, Integrity and Availability are the 3 core principles of security. Ensuring that you understand the objectives behind these principles is crucial to your success in the information and cyber security domain.

4. Identification

- **Definition :** A way to claim an entity's presence with respect to the process being carried out.
- For example, when you try to login to your Facebook account, you provide your Email or Phone number to establish your presence during the login process.

5. Authentication

- **Definition :** A way to ensure that the entity is indeed what it claims to be.
- This means that providing just the ID is not enough. You must additionally prove that the ID belongs to you. For example, even if I know your Facebook email address or phone, I cannot login as you until I also know the password.
- Thus, knowing just the ID is not enough. We need to prove that the ID belongs to us and that is what is precisely called authentication. It is for this reason that you need to additionally sign when you submit Aadhar card or PAN card as an ID proof to ensure that someone didn't just use the photocopy of those IDs without your permission (or consent). Some of the ways to authenticate an ID are passwords, biometric (like your Aadhar fingerprints or phone sensor), PIN (like for Debit Card), or OTP (SMS that you get to confirm transaction).

6. Authorisation

- **Definition :** A way to determine what resource an entity can access.
- For example, even if you have a valid voter ID card but if your name is not on the electoral list at a particular area booth, you won't be allowed to vote. Having authenticated ID is one thing and getting access to the resource is another.
- Just because you have an authenticated ID, does not mean that you have automatically access to the resources. So, authenticated ID is a must for authorisation but that does not always guarantee that you would be allowed access.

7. Accountability

- **Definition :** A way to record your actions.
- Suppose, you used a system to take print outs. That system logs this action (pretty much like you record attendance in lab or classroom) to build a trace (evidence or proof) that you used the printer.
- If you were not supposed to use the printer, the evidence can be used to find you accountable for using it without permissions and could result in particular consequences.
- Accountability is a key determinant of how securely a system is operating. The logs generated are continuously monitored and necessary alarms are raised if any entry is found to be suspicious.
- summarise the 4 access control steps with the help of Fig. 2-Q. 1(a).

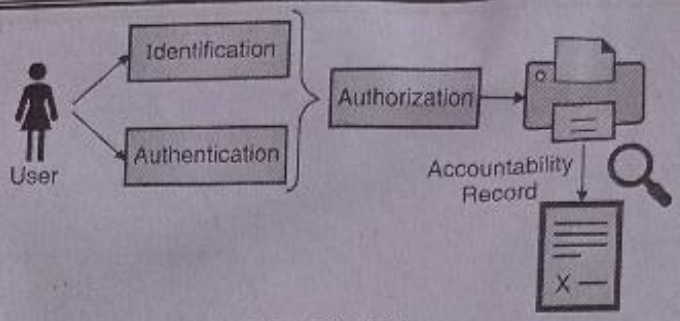


Fig. 2-Q. 1(a)

8. Non-repudiation

- **Definition :** A way to prove your actions.
- It is used in conjunction with accountability and the CIA triad. Non-repudiation provides an assurance that someone cannot deny their actions later on. For example, if I sent you an email, I cannot later deny that I did not.
- To send an email, I must have used my email ID and password and then sent it over to you over a secure network where no one could change the email body. If you can establish all of these facts truthfully, you have proven that I sent that email and thus established non-repudiation.

Chapter 2 : Data Encryption Techniques and Standards
[Total Marks - 25]

Q. 1(b) Using Hill Cipher encrypt the message 'ESSENTIAL'. The key for encryption is 'ANOTHERBZ'. (5 Marks)

Ans. :

- use the following table for forming a matrix for plaintext ESSENTIAL.

Table 1-Q. 1(b)

Alphabet	Number	Alphabet	Number
A	0	N	13
B	1	O	14
C	2	P	15
D	3	Q	16
E	4	R	17
F	5	S	18
G	6	T	19
H	7	U	20
I	8	V	21
J	9	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

- The Key ANOTHERBZ can be written in matrix form as following $\begin{bmatrix} 0 & 19 & 17 \\ 13 & 7 & 1 \\ 14 & 4 & 25 \end{bmatrix}$
- The plaintext ESSENTIAL when converted into matrix form gives $\begin{bmatrix} 4 & 4 & 8 \\ 18 & 13 & 10 \\ 18 & 19 & 11 \end{bmatrix}$
- Now, multiply the key matrix with the plaintext matrix and perform mod 26 on the resultant matrix.

$$\begin{bmatrix} 0 & 19 & 17 \\ 13 & 7 & 1 \\ 14 & 4 & 25 \end{bmatrix} \times \begin{bmatrix} 4 & 4 & 8 \\ 18 & 13 & 10 \\ 18 & 19 & 11 \end{bmatrix} = \begin{bmatrix} 648 & 570 & 187 \\ 196 & 162 & 115 \\ 578 & 583 & 387 \end{bmatrix}$$

$$\begin{bmatrix} 648 & 570 & 187 \\ 196 & 162 & 115 \\ 578 & 583 & 387 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24 & 24 & 5 \\ 14 & 6 & 11 \\ 6 & 11 & 23 \end{bmatrix}$$

- Arranging the resulting matrix back to alphabets we get encrypted text as YOGYGLFLX

Q. 2(a) What is steganography? What are the applications and limitations of steganography? (5 Marks)

Ans. :

Steganography

Definition : Steganography is the practice of concealing a message within another message, image, or file.

- The information is only hidden and not encrypted. The hiding is so non-obvious that it is difficult to discover it by anyone who is unaware of the presence of the hidden information. Only who knows what to look for and where can lookout for the hidden information.
- There are many different methods of performing steganography. The most famous of all is the one that modifies only the LSBs (Least Significant Bits). In media files such as images, audio or video, it is difficult to make out any difference between the files with modified LSBs and the files where LSBs are not modified.
- Hence, the information can be transferred hidden where generally these files are not considered harmful or are thoroughly inspected for finding information transfer. Do you see any difference between the following two images?

Fig. 1-Q. 2(a)

- That is precisely how hard it is to make out the hidden information where the variations between the two files is extremely hard to make out and not visible to the human eye.

A. Uses of Steganography

1. Leak corporate, business or personal data without being caught by firewall, IDS or other detection mechanisms.
2. Sending information in special groups without knowledge of others.
3. Attacking users with hidden malicious code in the downloaded media files.

B. Limitations of Steganography

1. Without declared algorithms, it is difficult to hide and unhide the secret message.
2. Somehow, the recipients must be told where to look for the hidden information.
3. The original image must be destroyed so that it is difficult for someone to find the difference between the images.
4. Steganography is not a real secure way of communication. It just provides security by obscurity which means that is just tries to complicate things rather than actually securing the communication.
5. Only a small amount of information can be hidden without distorting the image such that it becomes noticeable.

Q. 2(b) Use Transposition Cipher to encrypt plain text 'I Love my India' and use the key 'HEAVEN'. [Use single columnar transposition] **(5 Marks)**

Ans. :

- Arrange the unique characters in the key in a column

H	E	A	V	N
3	2	1	5	4
i	l	o	v	e
m	y	i	n	d
i	a	-	-	-

- Now, arrange the letters in the order of columns
- This gives "oilyaimiedvn" as the ciphertext.

Q. 3(b) What is block Cipher? Explain counter mode of block Cipher. **(5 Marks)**

Ans. :

Block Cipher

- In block ciphers, the information that needs to be encrypted is broken into smaller and equal block sizes. Then, the encryption operation (substitution and transposition) is applied to each block. The resultant cipher text from each block is then combined to produce the encrypted information.
- Fig. 1- Q. 3(b) illustrates simplified block diagram of how a block cipher works. The information is broken into equal size blocks and then the encryption operation is carried out on each block. If the block size has lesser number of characters than required to form a block, then padding is done to fill the block. Padding is just filling some temporary information to form a block. Finally, the resulting encrypted information from each block is combined to get the overall encrypted message.
- DES and AES are two of the examples of Symmetric Block Ciphers.

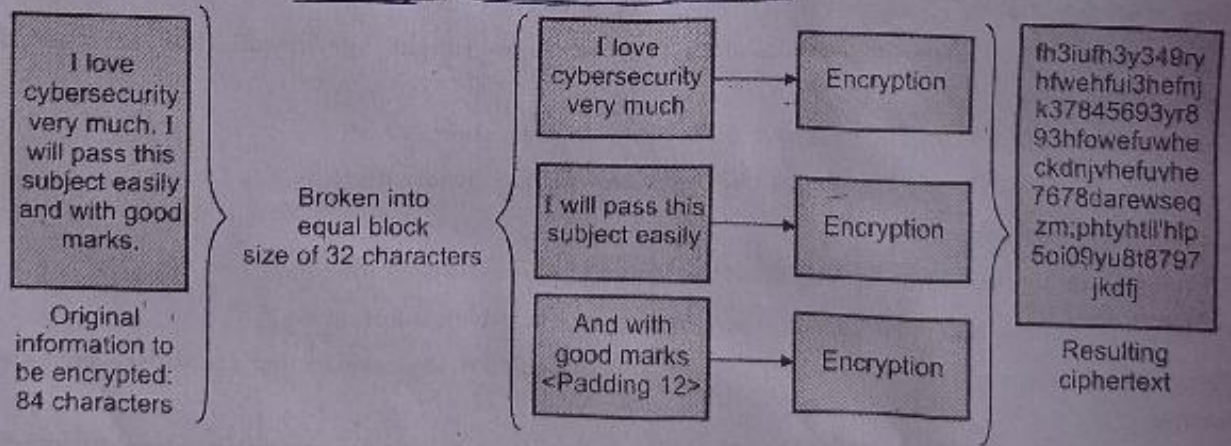


Fig. 1- Q. 3(b) : Block ciphers

Counter (CTR) Mode

– In this mode as well, the block cipher works like a stream cipher. The key is converted into keystream (as used in stream cipher) and the keystream is XORed with a counter that increases for every block.

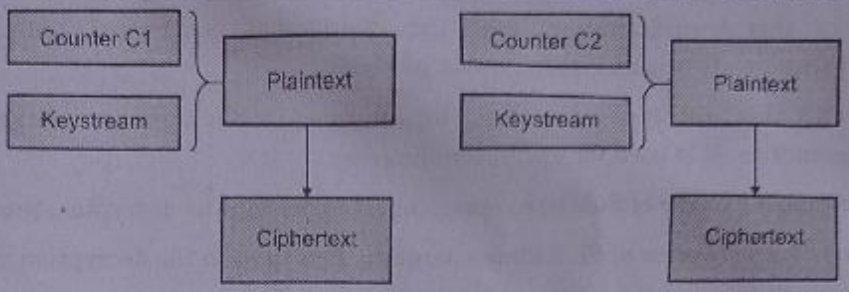
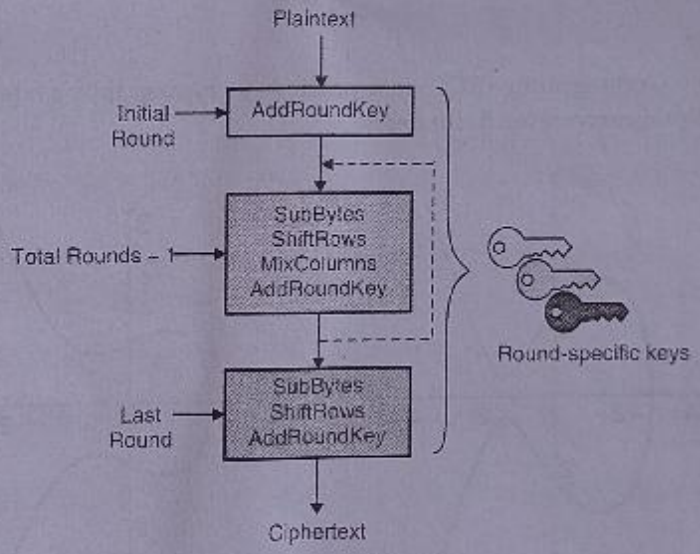


Fig. 2- Q. 3(b) : Counter (CTR) Mode

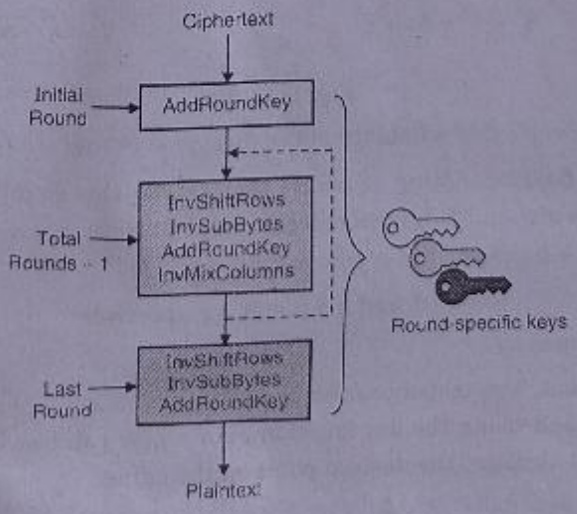
Q. 4(b) Explain working of AES in detail. **(5 Marks)**

Ans. :

Block Diagram and working of AES



(a) AES Encryption Process



(b) AES Decryption Process

Fig. 1-Q. 4(b) : Block diagram of AES

1. **AddRoundKey :** In this transformation step, a round key is generated and XORed with the intermediate (temporary) ciphertext. This block is used in both encryption as well as decryption process.
2. **SubBytes :** In this transformation step, the intermediate ciphertext undergoes various substitution operations. It is used for encryption process.
3. **ShiftRows :** In this transformation step, the intermediate ciphertext undergoes various row-wise transposition operations. It is used for encryption process.
4. **MixColumns :** In this transformation step, the intermediate ciphertext undergoes various column-wise transposition operations. It is used for encryption process.
5. **InvSubBytes :** This is inverse of SubBytes operation. It is used in the decryption process.
6. **InvShiftRows :** This is inverse of ShiftRows operation. It is used in the decryption process.
7. **InvMixColumns :** This is inverse of MixColumns operation. It is used in the decryption process.

Chapter 3 : Public Key and Management [Total Marks - 10]

Q. 3(a) Discuss elliptic curve cryptography in detail. **(5 Marks)**

Ans. :

Elliptic Curve Cryptography

Definition : Elliptic Curve Cryptography (ECC) is a public-key cryptography system which is based on discrete logarithms structure of elliptic curves over finite fields.

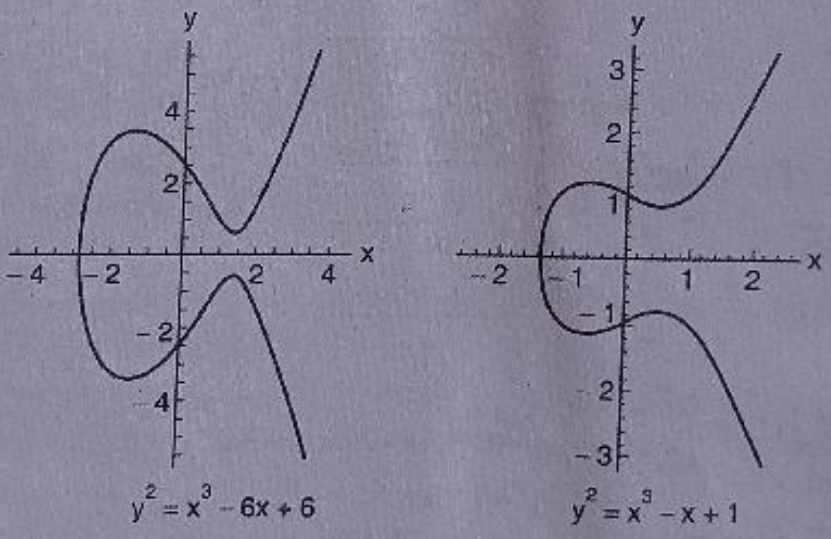


Fig. 1- Q. 3(a)

- ECC uses an elliptic curve over a finite field (p) of the form $y^2 = x^3 + ax + b \ (mod\ p)$
- The curve defines a finite field consisting of points that satisfy this equation along with infinity (∞) as the identity element. The value of a and b determines the shape of the curve. Only those curves which don't have repeated factors for $x^3 + ax + b$ are used in cryptography.
- Given are the two plots for a = – 6 and –1 and b = 6 and 1 respectively.

Working of Elliptic Curve Cryptography

- ECC uses a trapdoor function. The trapdoor function is similar to a mathematical game of pool. Start with a certain point on the curve and using the dot function , got a new point on the curve. Keep repeating the dot function from point to point until get the desired point on the curve.
- So, based on the diagram,
  - Start from point A and go to B. Reflect the point B in the opposite axis.

- It reflects at point C.
- From C go to D and reflect again cross X-axis as E
- Keep repeating it until you reach the desired point

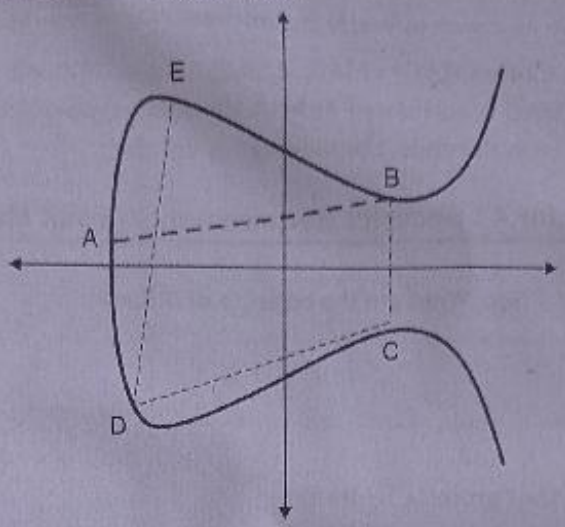


Fig. 2- Q. 3(a)

- So, if you know where on the curve is the starting point *A* and how many hops (number of dot functions needed) are required to reach the ending point *E*, it is very easy to find the ending point.
- But, if you just know that where the starting point and ending point are on the curve, it is nearly impossible to find how many hops it would take to get there. Hence, we can use these 3 information in cryptography as below :
  - **Public Key :** Coordinates of (Starting Point A, Ending Point E) on the curve
  - **Private Key :** Number of hops from A to E

Q. 4(a) What is authentication? Explain various methods of authentication. **(5 Marks)**

Ans. :

Authentication

Definition : Message authentication is a process to ensure that the received message is exactly the same as it was sent.

Types of Authentication Methods

At a high level, the message authentication can be performed using three mechanisms :

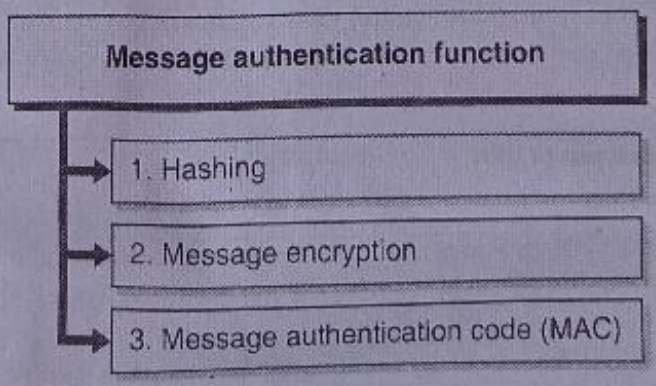


Fig. 1- Q. 4(a)

1. **Hashing :** It deals with producing a unique hash value of the message that can be computed at the sender's and the receiver's end. If the hashes match at both the ends, the message is verified.

2. **Message encryption :** In this, the ciphertext of the entire message can be used to serve as its authenticator. The message is encrypted at the sender's and the receiver's end. If they both get the same ciphertext using the same key, it verifies the message. Note here that the focus is not to encrypt the message but to get the resulting ciphertext to serve as a way to verify the authenticity of the message.
3. **Message Authentication Code (MAC) :** MAC is very similar to hash. It uses a key to calculate the hash value of the message. The MAC is calculated at both the ends (sender's and receiver's) using the same key. If the MAC value matches at both the ends, the message is verified.

Chapter 4 : Security Requirements [Total Marks - 36]

Q. 5(a) Discuss the working of IPSec. What are the benefits of IPSec? **(6 Marks)**

Ans. :

IPSec

Definition :

IPSec is a suite of protocols that protects IP traffic.

Working of IPSec

IPSec has 5 broad steps-

1. **Initiate IPSec process :** IPSec communication begins with the identification of traffic that requires IPSec security.
2. **IKE Phase 1 :** In this phase, the IKE SAs are negotiated and agreed.
3. **IKE Phase 2 :** In this phase, next set of SAs for actual data transfer are negotiated and agreed.
4. **Data Transfer :** Data is transferred between the communicating entities.
5. **Termination :** The IPSec connection is terminated once the data transfer is complete.

Benefits of IPSec

i. **Establish Virtual Private Network (VPN) :** IPSec is predominantly used to establish VPN connection. VPN connections are generally used to access private networks over the internet. For example, you can access your college or your organization's network from home over the internet.

ii. **Connecting two or more branch networks :** IPSec can be used to extend or connect branch networks. For example, if you have two branches of office each using its own network, the branches can be connected using IPSec. The network traffic then can securely move between the branches.

iii. **General security benefits :** IPSec adds general security benefits to the core IP protocol. It provides benefits such as data confidentiality, data integrity, data origin authentication and protection from several attacks on the core IP protocol.

Q. 5(b) What is VPN? Explain types of VPN. **(6 Marks)**

Ans. : Virtual Private Network (VPN)

- A Virtual Private Network (VPN) provides a solution for this scenario. It allows to establish a secure channel between the communicating parties over the public network, such as the Internet and facilitate secure connection between them.
- A Virtual Private Network (VPN) is a data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them.
- The authorised users can then securely access the private network over the public network. Physical presence within organisation premises is not required to access the private network. The entire traffic between the remote user and the private network is encrypted. IPSec can be one of the mechanisms for establishing a VPN connection.

Types of VPN

At a broad level, there are two types of VPN.

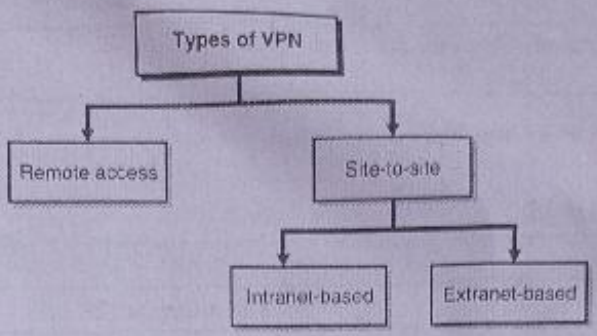


Fig. 1-Q. 5(b)

1. **Remote Access VPN :** Remote Access VPN is setup for remote users. They can access the private network securely over the public network.

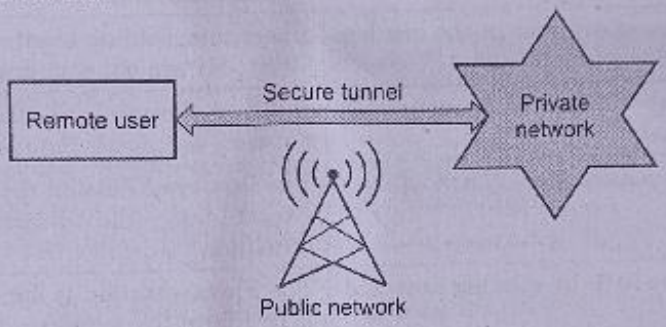


Fig. 2-Q. 5(b)

2. **Site-to-Site VPN :** This is established by the organisation for connecting its multiple sites or branch offices so that the users can access the resources across the sites.
   a. **Intranet-based site-to-site VPN** is used for organization's own sites.
   b. **Extranet-based site-to-site VPN** is used for organization and its partners.

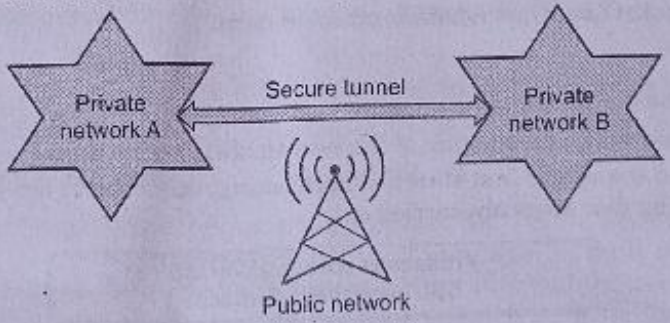


Fig. 3- Q. 5(b)

Q. 5(c) Compare PGP and S/MIME. **(6 Marks)**

Ans. : Difference between PGP and S/MIME

Mandatory features	S/MIME	PGP
Message format	Binary, based on Cryptographic Message Syntax (CMS)	Binary, based on previous PGP
Certificate format	Binary, based on X, 509v3	Binary, based on previous PGP
Symmetric encryption algorithm	Triple DES (DES EDE3 CBC)	TripleDES (DES EDE3 Ecentric CFB)
Signature algorithm	Diffie-Hellman (X9.42) with DSS or RSA	El Gamal with DSS

Mandatory features	S/MIME	PGP
Hash algorithm	SHA-1	SHA-1
MIME encapsulation of signed data	Choice of multiple/signed for CMS format	Multipart/signed with ASCII armor
MIME encapsulation of encrypted data	Application /pkcs7-mime	Miltipart/encrypted

Q. 6(a) Differentiate between IP-V4 and IP-V6. (4 Marks)

Ans. :

Comparison between IP-V4 and IP-V6

IP-v4	IP-v6
The address space is 32 bits.	The space is 128 bits.
The length of header is 20 bytes	The length of header is 40
4 bytes for each address in the header	16 bytes of each address in the header
The number of Header field 12	The number of header field 8
Checksum field, used to measure error in the header, required	Checksum field eliminated from header as error in the IP header are not very crucial
Internet Protocol Security (IPSec) with respect to network security is optional	Internet Protocol Security (IPSec) with respect to network security is mandatory
No identification to the packet flow (Lack of Qos handing).	The flow level field on the header portion identifies the packet flow and directs to router (Efficient Qos handling)
The Fragmentation is done both by sending host and routers	The Fragmentation is done both by sending host; there is no role of the routers.
No identification to the packet flow (Lack of Qos handing).	The flow level field on the header portion identities the packet flow and directs to router (Efficient Qos handling)
Clients have approach Dynamic Host Configuration server (DHCS) whenever they connect to a network.	Clients do not have to approach any server as they are given permanent addresses.

Q. 6(b) Explain Secure Socket Layer handshake protocol in detail. (7 Marks)

Ans. :

Secure Socket Layer Handshake Protocol

- **Definition :** The cryptographic parameters of the session state are produced by the SSL handshake protocol.
- When an SSL client and the server first start communicating, they need to agree upon certain parameters. At a high level, the following four steps are carried out.

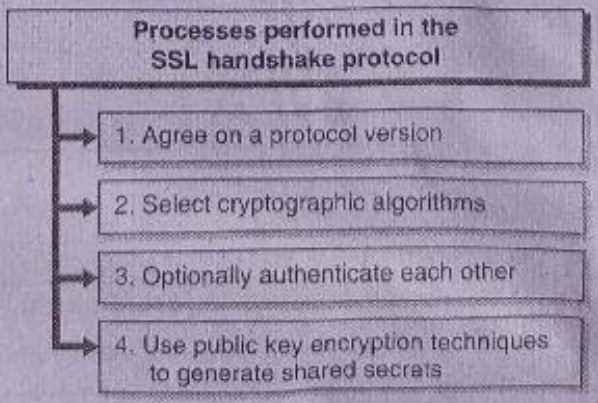


Fig. 1-Q. 6(b)

- Fig. 1-Q. 6(b) illustrates the detail steps of handshake process diagram.

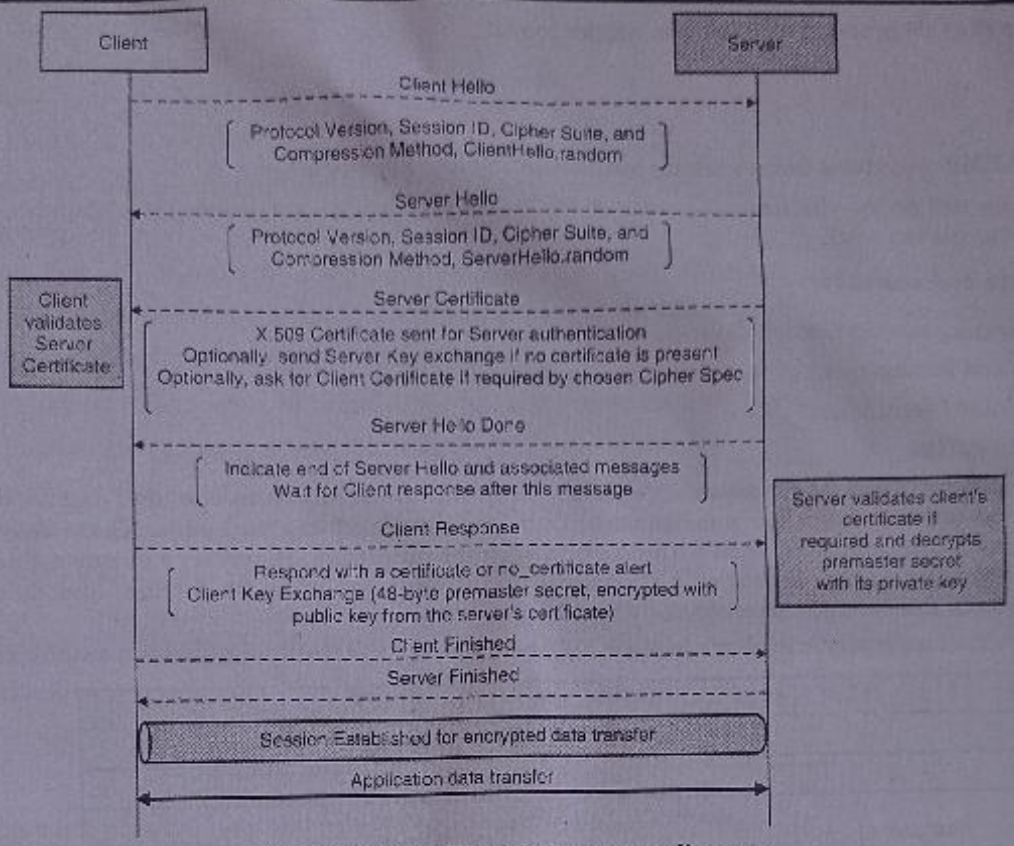


Fig. 2-Q. 6(b) : Handshake process diagram

Step 1 : Hello messages (Establish security capabilities)

The hello phase messages are used to exchange security enhancement capabilities between the client and server.

1. **Client Hello :** When a client first connects to a server it is required to send the client hello as its first message. The client can also send a client hello in response to a hello request or on its own initiative in order to renegotiate the security parameters in an existing connection. The list of parameters sent is in Fig. 2-Q. 6(b).
2. **Server Hello :** The server processes the client hello message and responds with server hello message. The list of parameters sent is in Fig. 2-Q. 6(b).

Step 2 : Server Authentication and Key Exchange

- This is the most important step. This is why you need SSL at all. Before proceeding to interact with the server you should find out "Is this really the server you want to talk to?" This is crucial. For example, if you want to do a banking transaction, before providing your account information, username and password, you MUST validate that the website you are on (server behind the website) is legitimate.
- In this step, the client validates the server certificate. Any certificate related errors are highlighted.

Step 3 : Client authentication and Key exchange

If the certificate is found valid, client exchanges the keying material that would be subsequently used to encrypt the messages. The client generates a 48-byte premaster secret, encrypts it using the public key from the server's certificate and sends the result in an encrypted pre-master secret message.

Step 4 : Connection establishment and data transfer

Once all the connection parameters are negotiated and exchanged, a connection between the server and the client is established. Once the connection is established, the data transfer begins between the server and the client. The data is encrypted based on the negotiated terms.

Q. 6(c) Explain ISAKMP protocol of IPSec with header format. **(7 Marks)**

Ans. :

ISAKMP protocol

Definition : ISAKMP provides a framework for authentication and key exchange.

- ISAKMP does not define the exact algorithms to be used. It is just a framework within which various exchange protocols can work.

ISAKMP defines the procedures for

- Authenticating communication devices
- Creation and management of Security Associations (SA)
- Key generation techniques
- Threat mitigation

- ISAKMP is distinct from key exchange protocols in order to cleanly separate the details of security association management (and key management) from the details of key exchange. There may be many different key exchange protocols, each with different security properties. However, a common framework is required for agreeing to the format of SA attributes, and for negotiating, modifying, and deleting SAs. ISAKMP serves as this common framework.
- Fig. 1-Q. 6(c) shows a simplistic diagram of ISAKMP header.

Fig. 1-Q. 6(c) : ISAKMP header

1. **Initiator cookie (8 bytes) :** The cookie of entity that initiated Security Association (SA) establishment, SA notification, or SA deletion.
2. **Responder cookie (8 bytes) :** The cookie of entity that is responding to a SA establishment request, SA notification, or SA deletion.
3. **Next Payload (1 byte) :** Indicates the type of first payload in the message. ISAKMP supports the following payload types :
   - None
   - Security Association
   - Proposal
   - Transform
   - Key Exchange
   - Identification
   - Certificate
   - Certificate Request
   - Hash
   - Signature
   - Nonce
   - Notification
   - Delete
   - VendorID

- NAT Discovery Payload
- NAT Original Address Payload
- Reserved
- Private Use

4. **Major version (4-bits) :** Major version of the ISAKMP protocol in use.
5. **Minor version (4-bits) :** Minor version of the ISAKMP protocol in use.
6. **Exchange Type (1 byte) :** The type of exchange in a given ISAKMP session. The primary difference between exchange types is the ordering of the messages and the payload ordering within each message.
7. **Message ID (4 bytes) :** The unique message identifier.
8. **Length (4 bytes) :** The length, in bytes, of the total message (header + payloads).

- **ISAKMP offers two phases of negotiation**
  - **Phase 1 :** In the first phase, two entities agree on how to protect further negotiation traffic between themselves, establishing an ISAKMP SA.
  - **Phase 2 :** The second phase of negotiation is used to establish security associations for other security protocols. This second phase can be used to establish many security associations. The security associations established by ISAKMP during this phase can be used by a security protocol to protect many message/data exchanges.

Chapter 5 : Firewall and Intrusion [Total Marks - 32]

Q. 7(a) What are the various types of firewall? Discuss limitations of firewall. **(8 Marks)**

Ans. :

Types of Firewalls

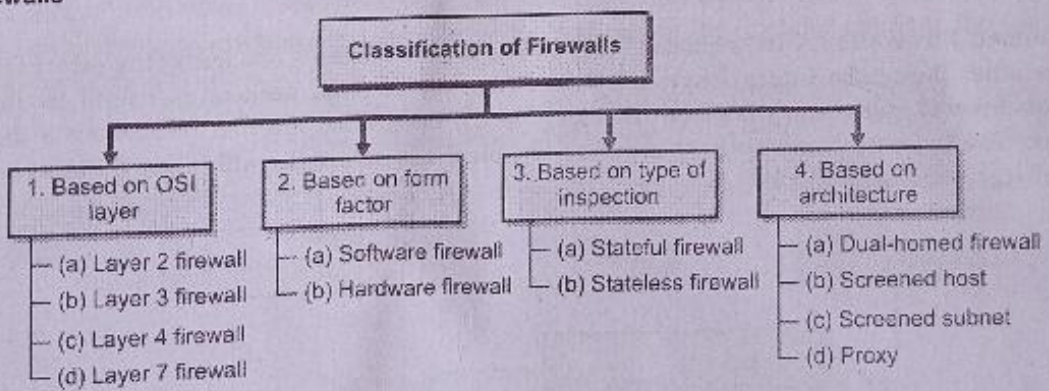


Fig. 1- Q. 7(a)

1. **Based on the OSI Layer**
   - **a. Layer 2 Firewall :** These firewalls work at the "Data Link" layer of the OSI model. These firewalls require MAC, VLAN or device hardware level information to operate. One of the greatest advantage of these types of firewalls is that they are not IP dependent.
   - **b. Layer 3 Firewall :** These firewalls work at the "Network" layer of the OSI model. These filter traffic based on source/destination IP, port, and protocol. These are one of the most prevalent types of firewalls in use today. These are also called as Stateless firewalls. These are also called *first-generation* firewalls.
   - **c. Layer 4 Firewall :** These firewalls work at the "Transport" layer of the OSI model. These firewalls do everything that a Layer 3 firewall does and additionally track the active network connections and allow/deny traffic based on the state of those connections.

These can effectively stop DoS attacks such as the ones based on TCP SYN/ACK as these are aware of the state of connection. These are also called as Stateful firewalls. These are also called second-generation firewalls.

d. **Layer 7 Firewall :** These firewalls are called Layer 7 but can work at three layers – Session, Presentation and Application. For simplicity, these are just called Layer 7 firewalls. Layer 7 firewalls do everything that a Layer 4 firewall does and additionally include the ability to intelligently inspect the contents of the network packets passing through them. For example, a Layer 7 firewall could deny all the HTTP requests from Korean IP addresses.

2. **Based on the form factor**

a. **Software Firewalls :** These firewalls work as a software program and require an operating system to run them. All the implementation logic is coded in software and they are installed, patched, upgraded and maintained like a regular computer software. These firewalls could work at any of the OSI layers as discussed before.

b. **Hardware Firewalls :** Firewalls can also be deployed as a hardware device. Hardware firewall may have better performance and they come packaged in a ready to use hardware device. Like any other firewall, you need to configure it as per your security requirements.

3. **Based on the type of inspection**

a. **Stateful Firewalls :** These firewalls keep track of the state of connections apart from the defined firewall rules. These precisely understand various handshake protocols and can effectively stop attacks that try to manipulate connection establishment or maintenance process.

b. **Stateless Firewalls :** Stateless firewalls typically work at the Layer 3 and take decisions based on the defined rule parameters such as IP, Port and Protocol. These do no track connection states and cannot effectively protect against attacks that manipulate connection processes.

4. **Based on architecture**

a. **Dual-homed Firewalls :** A Dual-Homed Firewall has two interfaces – one facing the external network and the other facing the internal network. It receives the external packets on one of its interfaces, evaluates firewall rules, and passes on the traffic to the designated internal resources via the second interface. The two interfaces are kept separate to isolate the external traffic with the internal traffic physically.

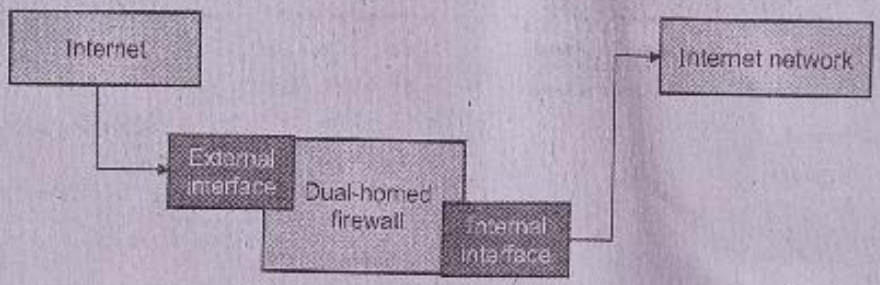


Fig. 2-Q. 7(a)

b. **Screened Host :** In a screened host firewall, all internet (and other regulated) traffic goes through the firewall, no matter what. The internet router device first screens (filters) all the packets that are relevant to the network and then passes it to the Screened Host firewall for further inspection and applying rules.

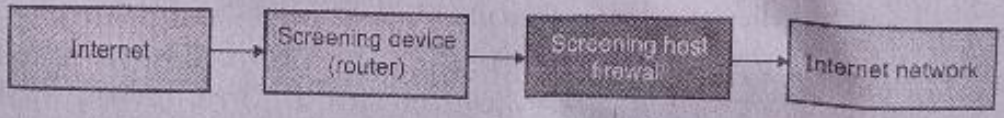


Fig. 3-Q. 7(a)

c. **Screened Subnet :** In screened subnet architecture, two firewalls are used. One just after the external network and the one just before the internal network. Any network that lies between the two firewalls is called a Demilitarized Zone (DMZ). You place your public facing servers such as web servers, email servers etc. in DMZ. An attacker would have to bypass both the firewalls before she can hit the internal network. This kind of architecture is commonly used in the industry today.

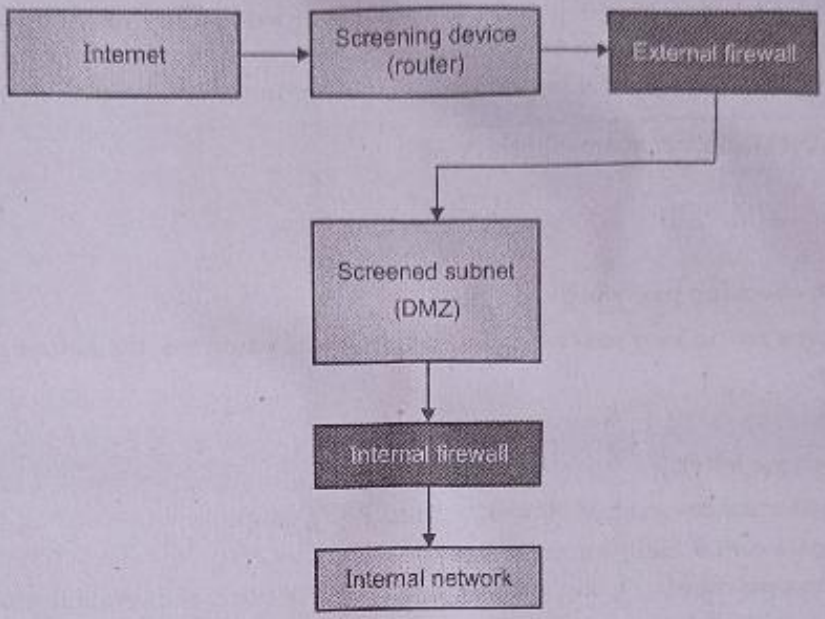


Fig. 4-Q. 7(a)

d. **Proxy :** A proxy firewall stands between the trusted and the untrusted network and takes allow or deny decisions after careful inspection of what is being passed along. Like a regular proxy, the proxy firewall breaks the connection between the source and the destination. After examining the traffic, it self-establishes a connection with the destination and passes the intended traffic to the destination as if the packets were originating from it.

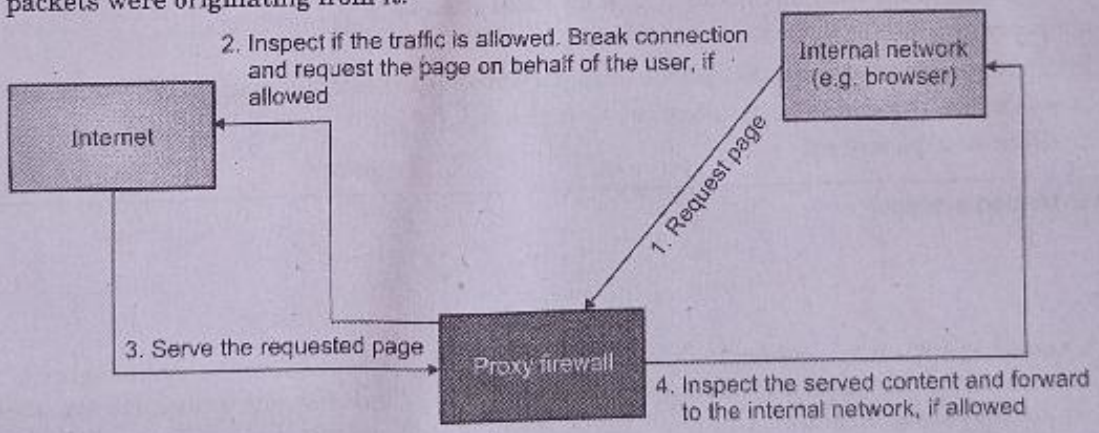


Fig. 5-Q. 7(a)

Limitations :

1. **Performance :** Since the traffic (as well as the content) needs to pass through the firewalls, there is a little performance degradation of the network. The adequate traffic examination may add up to a few milliseconds of latency on each packet.
2. **Business agility :** Firewall rules are usually manually added, edited or deleted. The pace of business might be too high to require several changes to the firewall rules frequently. Keeping up with these changes without making errors is difficult.
3. **Costs :** Modern (or advanced) firewalls that provide content and protocol level inspection may be cost-prohibitive for small or medium sized organizations.

4. **Insider attacks :** Firewalls are usually designed and deployed to protect a trusted network from an untrusted network. But, if there were other vulnerabilities (such as a missing OS security patch) that were exploited such that an attacker is already on the trusted network, firewalls might not be able to protect or limit damages to the other resources on the trusted network.
5. **Managing firewalls themselves :** Like your OS, printers or other software or hardware devices, firewalls need to be installed, patched, updated, etc. to remain operational. This adds a management overhead. Additionally, firewalls could have known vulnerabilities that need to be patched else a firewall that itself is lacking protection may not be very useful in providing you the required level of protection.

Q. 7(b) Explain any two password management practices. **(4 Marks)**

Ans. :

Password Management

General guidelines when choosing passwords

1. Choose at least 12 characters in your password. The lengthier the password, the harder it is to crack it.
2. Use mix of characters.
   a. At least one digit.
   b. At least one uppercase letter.
   c. At least one special character such as (@,#, $, %, ^, &, *, (,), etc.).
3. Do not use the same password for all your accounts.
4. Do not use easy to guess passwords. Do not use your name, date of birth, school name etc. as your password.
5. Check your password quality before using it.
6. Do not use words found in the dictionaries. For example, avoid creating a password such as "Apple".

General Password Usage Guidelines

Here are some general guidelines to follow when working with passwords.

1. Do not send your password in cleartext. Avoid entering them on sites that do not use https.
2. Do not share your password with anyone in your family and friends.
3. Change your passwords periodically to avoid overuse.
4. Do not tell your password to anyone over phone or email howsoever the conversation may sound legitimate.
5. Wherever possible, use two-factor authentication with password.
6. Do not write down your password!

Q. 7(c) What is trusted system? **(4 Marks)**

Ans. :

Trusted System

- Designing a secure system is a complex task. You need to follow several basic elements of security and need to model the security of the system around approved principles. These security principles are often derived and stated in mathematical formulae. One such model is the State Machine Model.
- **Definition :** The State Machine Model ensures that a system is in a secure state all the time. Any events that alter the state of the machine are not allowed.
- It means that the system boots up in a secure state, carries out operations that are secure and then shutdown securely.
- A system is continuously in the secure state.

Q. 8(a) Explain need and challenges of intrusion detection system. Define signature based IDS. **(8 Marks)**

Ans. : Intrusion detection system

- In digital terms, intrusion refers to the similar situation where the malicious code or attackers try to encroach (forcibly enter and capture) information systems without requiring permission of the system owner. An Intrusion Detection System (IDS) is defined as,
- **Definition :** A software that helps to find out if a system is breached.

Need of IDS

IDS is one of the software-based security mechanisms that help to protect information system. At a high level, it is needed for the following reasons :

1. **Defense in Depth :** As in the security architecture section, security is about minimizing the damage that can be possibly done. Defense in depth (or the layered approach) of security designing ensures that even if one of the controls is to fail, the overall security of the system would still be possibly healthy. IDS fulfill this need to bring an added layer of protection where any breaches or their possibilities can be identified quickly.
2. **Automate intrusion detection :** Imagine that you have a large set of machines, say 1,000 and more. How would you inspect each and every machine and find out if there were attacks or attempts to attack it? IDS helps you to automate this need and alert you when it detects any threat or likely a breach.
3. **Corrective actions :** Learning from threats or breaches that the IDS identifies, you can take corrective actions on your infrastructure design and could possibly strengthen its security. In some unprotected areas in our infrastructure that can be highlighted with the use of IDS.

Challenges of IDS

1. **Does not prevent attacks :** IDS can only detect and raise alerts when it finds a likelihood of a breach. It cannot prevent or block the breach from happening.
2. **High rate of false alerts (noise) :** IDS might generate a lot of false alerts. It could happen so for example, when there is a new traffic from a source that IDS has not seen before. You need to spend your resources to take a note of each alert and appropriately deal with it – either fix it or ignore it.
3. **Complex systems :** IDS systems are typically complex in nature and require regular administrative actions and tuning for adequate operations.
4. **Bypassing IDS :** Advanced attackers know what actions and activities a version and brand of IDS can detect and what not. They tune their activities to bypass such detection mechanisms and go undetected.

Signature Based IDS

– IDS can be classified based on **what** it monitors and **how** it monitors.

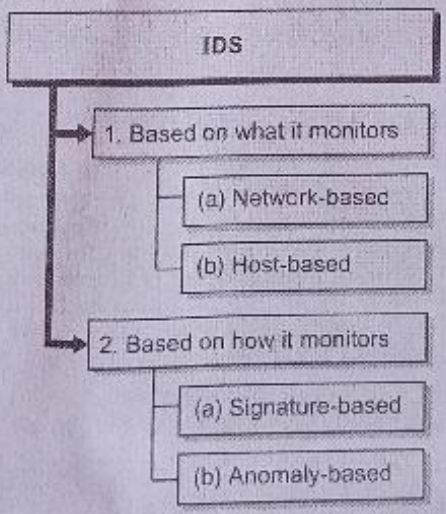


Fig. 1- Q. 8(a)

1. Based on what it monitors

– IDS can be classified into Network-based IDS (NIDS) and Host-based IDS (HIDS).

a. **Network-based IDS (NIDS) :** Network-based IDS evaluate intrusions from the networking side. They watch all network traffic as it reaches the various information systems. If there are any alerting situations based on the network traffic analysis, it notifies the administrator to take the corrective actions. NIDS do not have visibility into what's actually going on within the information system. It can only watch and detect threats and breaches from the networking viewpoint.

b. **Host-based IDS (HIDS) :** Host-based IDS are typically installed on the individual information systems and then they watch for suspicious activities occurring on the system. A system entity such as system services and processes, system files, privileged user actions, downloads etc. are closely monitored to detect any undesired activities. HIDS do not have visibility into what's going on at the networking side of the system. It can only watch and detect activities with respect to individual machines only.

2. **Based on how it monitors**

IDS can be classified into Signature-based and Anomaly-based.

a. **Signature-based :** Like banks and other organizations use human signature to validate requests and transactions, similarly Signature-based IDS has a pre-loaded database of various attack signatures (patterns of a possible attack). When it watches the activities, it constantly compares the activities' patterns with that in the database. If a match is found, it raises an alert. there are 3 things.

- Signature based IDS can only detect attacks if it already and historically knows about an attack pattern.
- For new types of attack, signature-based IDS would not raise alerts.
- It is important for you to update the signature definitions time to time (like how you do in anti-virus system).

b. **Anomaly-based :** Anomaly typically means "deviation from routine". For example, if you wake up at 7 AM every day and one day you wake up at 4 AM that is an anomaly situation.

If I were to plot your wake-up time graph, 4 AM would show up away from your regular wake-up time. That 4 AM point on the graph is called outlier (or away from other samples). Similarly, the Anomaly-based IDS first establishes the baseline (common routine) of activities. It might take up to 2-3 weeks to "learn" what's right for a system. Once the learning phase is over, it would watch out for any activities that are not part of that baseline and raise alerts. there are 3 things to understand here as well :

- It does not require signature and hence can possibly detect new attacks.
- It requires a learning period during which the system should have undergone all possible activities.
- If you plan to use the system for other purposes, you need to retrain the IDS.

Q. 8(b) What is access control security services? **(4 Marks)**

Ans. :

Access Control Security Services

- **Definition :** Access Control Policies and Models dictate how and under what constraints (or conditions) principals (entities or subjects) access resources (objects).

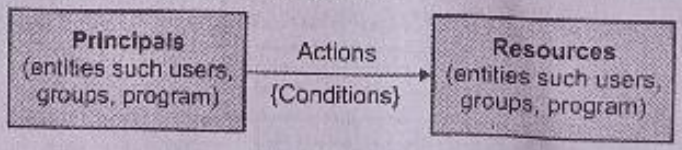


Fig. 1- Q. 8(b)

- It follows the PARC model :
  - P = Principals (users, groups, programs)
  - A = Actions (Create, Read, Update, Delete)
  - R = Resources (OS, Network, Files, etc.)
  - C = Conditions (time of the day, type of OS, etc.)
- Access control is the primary way to restrict entities from
  - Interacting with unauthorised resources
  - Carrying out unauthorised actions on authorised resources
- There are 4 types of access control models.

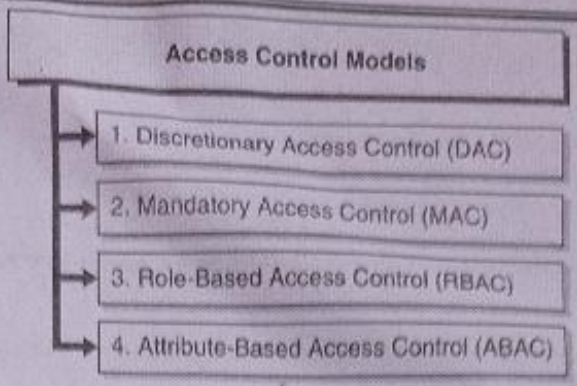


Fig. 2- Q. 8(b)

Q. 8(c) Explain packet filtering firewall. **(4 Marks)**

Ans. : Please refer Q. 7(a) of May 2019.

Chapter 6 : Confidentiality and Cyber Forensic [Total Marks - 32]

Q. 9(a) Explain personally identifiable information PII. Describe PII impact levels with examples. **(8 Marks)**

Ans. :

Personally Identifiable Information (PII)

Definition : Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- PII is the information (or combination of information) that is sufficient to trace you as an individual. It could be several elements such as
  1. Name
  2. IDs such as Aadhar, Passport, Email ID, PAN, Bank Account, Phone Number, etc.
  3. Address – Physical or Digital (IP Address)
  4. Demography details such as location, caste, gender, age, income group, etc.
- Here the personal information itself may not always be unique enough to identity someone. For example, Narendra itself could just be the name of any individual and may not be unique enough to identify someone without further details about him. But, if you say, "Prime minister of India in 2018", it could certainly be referring to Shri. Narendra Modi. The single attribute is strong enough to identify the person uniquely.
- So, when we talk about privacy, we are talking about protecting the information that could be used to uniquely identify someone and possibly track him or her. Just a scary fact, if someone just knows your name, your date of birth and your postal code, there is more than 75% chance to pinpoint you!

Q. 9(b) What is cyber stalking? How to identify and detect cyber stalking. **(8 Marks)**

Ans. :

Cyber Stalking : cyber staling is nothing but harrasing some user / people over internet. like false accusation, threats, data destruction, monitoring, data manipulation etc.

- Cyber stalker usually uses Emails, instant message, phone calls to mentally harass someone.
- Cyber stalking even uses public news group posting an inappropriate content for harassment.

Types of Stalkers

They are of two types :

1. **Online stalker :** In this type stalker uses internet to interact with the victim. The communication media can be any social media, Email, phone call, instant messages etc.

2. **Offline stalker :** In this type stalker mostly stalk victim by analyzing victims daily routine, research every past activity through different medium and gathering information of the victim using internet.

Identify

- Review privacy settings
- accounts are set to private where user can control who has access to the information on your profile through friend requests.
- set differing privacy preferences for different kinds of posts, and the privacy settings are differently managed on different platforms.
- Parents can review children's accounts and ensure they understand what information they should not share with others online, such as their address or phone number.
- Review friend requests/phone numbers before adding
- Be sure about people which are known and unknown. Based on this add people on social media.
- Avoid interaction between unknown people.
- Track Trends : Always pay attention to trends of someone liking and commenting on posts or communicating repeatedly in a suspicious or threatening manner through text, phone call, email, or other forms of electronic communication.
- Pay attention to people who do not take

Detect

- Block the person
- Report to the platform involved
- Call the police

Q. 10(a) What are different phases of cyber forensics? Explain with suitable diagram. **(8 Marks)**

Ans. :

- At a high level, there are four phases of cyber forensics. They are as shown in Fig. 1- Q. 10(a).

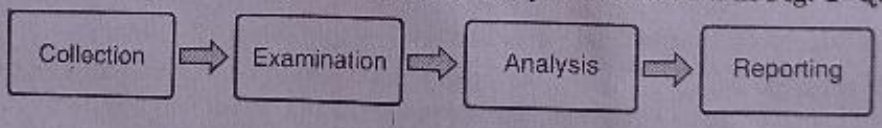


Fig. 1- Q. 10(a)

1. **Phase 1 : Evidence Collection :** During collection, data related to a specific event is identified, labelled, recorded, and collected, and its integrity is preserved. The sources of data could be logs, memory dumps, process tables, users logged in, hard disk state, system photograph, etc.
2. **Phase 2 : Examination :** In the examination phase, various forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity. Examination may use a combination of automated tools and manual processes.
3. **Phase 3 : Analysis :** The analysis phase involves analyzing the results of the examination to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
4. **Phase 4 : Reporting :** The final phase involves reporting the results of the analysis, which may include describing the actions performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.

Q. 10(b) Discuss PII confidentiality safeguards. **(8 Marks)**

Ans. : PII confidentiality safeguards

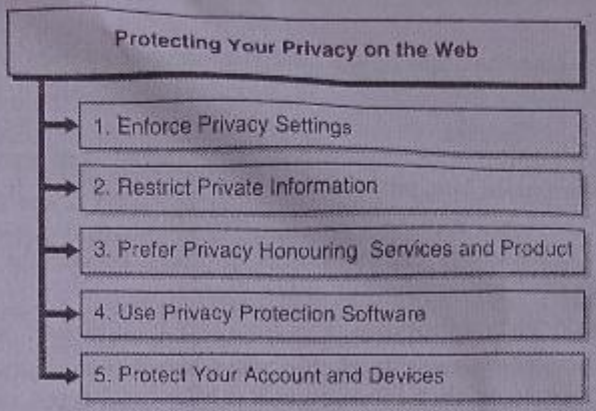


Fig. 1-Q. 10(b)

1. Enforce Privacy Settings

Mostly any device, software or service that you use today come with a host of privacy enhancement settings. The default privacy settings might not be optimum, and you must carefully review the privacy settings of each device, software or service that you use to ensure that your private data is potentially protected. It might be a little time consuming to periodically check them all, but it can go a long way to ensure that your online privacy is adequately protected.

A. Privacy Settings on Device

- The CIS Security Benchmark for Android devices has listed several privacy enhancement settings that you could set on your Android device for improved privacy. Following are some of the privacy settings -
  - Ensure 'Notifications on the lock screen' is set to 'Disabled'
  - Ensure 'Location Services' is set to 'Disabled'
  - Ensure 'Back up to Google Drive' is 'Disabled'
  - Ensure 'Web and App Activity' is set to 'Disabled'
  - Ensure 'Device Information' is set to 'Disabled'
  - Ensure 'Voice & Audio Activity' is set to 'Disabled'
  - Ensure 'YouTube Search History' is set to 'Disabled'
  - Ensure 'YouTube Watch History' is set to 'Disabled'
  - Ensure 'Google Location History' is set to 'Disabled'
  - Ensure 'Opt out of Ads Personalization' is set to 'Enabled'

B. Privacy Settings on Software

Software such as browsers offer quite a few privacy settings. You should configure them to provide maximum privacy even if that means a little bit of discomfort or little distorted user experience. Some browsers are more privacy centric than others.

- **Definition :** Do Not Track (DNT) refers to a mechanism for communicating a user's preference regarding tracking on the internet.
- Tracking collects the user's activities. DNT is a mechanism to let the webserver know that you do not wish to be tracked. Note here that even if you have configured DNT, honouring it or not is up to the webserver. Some webservers do honour it whereas plenty others continue to track you ignoring your tracking preference.
- So, look at all the software that you use for your online activities on all your devices and ensure to configure the privacy settings on them to maximise your privacy protection.

C. Privacy Settings on Service

- Once you have protected your device and software, you should look at what specific privacy enhancing settings does the online service provide you specifically and configure them suitably.

- Is it similar to what you have configured for your account? Can anyone who has your number see your online presence, your photos and your status? Is this desirable?

2. Restrict Private Information

- In sports, there is a usual saying that "the points saved are equal to points scored". Similarly, restricting your private information to yourself is way easier than trying to safeguard it later on once the information is already given out.
- Do not give your personal information to any random sites, forms, competition, surveys, piracy websites, or social media. The more information you put out there the more difficult it is to protect it later on. Refrain from updating about your status and whereabouts very frequently.
- Do not disclose much in advance about your activities in plans. Be careful about what you post online and what effect it might have for your privacy now or in the future.

3. Prefer Privacy Honouring Services and Products

- You have a variety of options these days to choose what services and products you use. When making a choice, prefer services and products that honour your privacy and have controllable privacy configuration options.

Examples -

- Table 1-Q. 10(b) shows a list of browsers and their probable privacy ranking based on the features they provide.

Table 1-Q. 10(b) : Browsers and their privacy ranking

Sr. No.	Browser Name	Privacy Ranking
1.	Opera	Low
2.	Google Chrome	Low
3.	Microsoft Internet Explorer	Medium
4.	Microsoft Edge	Medium
5.	Brave	High
6.	Mozilla Firefox	Very High
7.	Apple Safari	Very High
8.	Tor Browser	Very High

- You should choose the browser that provide you more privacy protection. Similarly, you could choose search engines that provide more privacy protection than Google Search. Some of the options are as following.
  - Search Encrypt
  - StartPage
  - DuckDuckGo
  - Gibiru
  - Swisscows
  - Yippy
  - BitClave
  - Qwant
  - Discrete Search
  - Oscobo

4. Use Privacy Protection Software

- You can add multiple extensions to your existing software (browsers, OS, network connections, etc.) that could provide enhanced privacy protection.
- These additions top-up the privacy protection capabilities that are lacking in the base software.

Examples -

A. Privacy Protecting Browser Extensions

- There are several browser extensions that you can install to provide privacy protection. These extensions come with various capabilities. The most used capabilities are blocking trackers and removing advertisements whenever you visit any website.

- You can search for various add-ons for your respective browsers. These add-ons are available for most of the widely used browsers and provide similar capabilities. Here is an example on Mozilla Firefox.

B. Virtual Private Network (VPN)

- You could use a VPN software to connect to the internet. That way your location and other demographic details are protected automatically. The IP address assigned to your device is not the actual IP assigned by your internet service provider but the one assigned by the VPN server.
- You could also alter your location. For example, being in India, you can connect via a server in Singapore. The websites that you visit would then consider that you are coming from Singapore and would not be able to track your demographics solely based on your device characteristics or IP address.

C. Private Mode of Browsing

- You could also choose to use the private mode of browsing. Most of the widely used browsers allow you to use private mode. Note here that the private mode does not make you anonymous on the internet and neither it hides the information from your internet service provider or the websites that your transact with.
- Private Browsing works by removing cookies, browsing history, and stored passwords while you are browsing once you close your Private Window. This makes it harder for the websites to track your browsing habits if you are not logged in. Also, if anyone else shares your device, it would be difficult to trace what websites you have visited previously using that device.

5. Protect Your Account and Devices

- Privacy protection also requires that you secure your devices and accounts. Follow regular security practices such as
  - Strong passwords for your accounts and devices
  - Multi-factor authentication
  - Security hardening
  - Installing anti-malware protection
  - Locking your devices when you are not using them
  - Not sharing your account details
  - Watching out if someone is overlooking as you type
  - Cautious when clicking links
  - Cautious when opening email attachments
  - Cautious when providing your personal details anywhere
  - Cautious of which websites you go to
  - Cautious of which services you subscribe to
  - Cautious of which accounts you have linked for identity management

Such security hygiene practices go a long way to ensure that your private information is kept secured and is not disclosed..

□□□