**Important Instructions to examiners:**

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more importance (Not applicable for subject English and Communication Skills)
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgment on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

**Q 1. A) Attempt Any Three** **(12 marks)**

a) **What is CIA security? Describe in brief.**
**(1 Mark each Point explanation)Total 4 Marks)**
The need of computer security has been threefold: confidentiality, integrity, and availability—the "CIA" of security. (1 mark for each principle)

**1. Confidentiality:** the principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message.
Example of compromising the Confidentiality of a message is shown in fig.

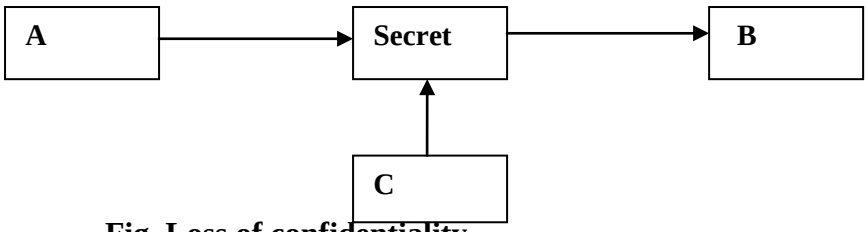



**Fig. Loss of confidentiality**

Here, the user of a computer A send a message to user of computer B. another user C gets access to this message, which is not desired and therefore, defeats the purpose of Confidentiality.
This type of attack is also called as **interception.**

**2. Authentication:** Authentication helps to establish proof of identities. The Authentication process ensures that the origin of a message is correctly identified.
For example, suppose that user C sends a message over the internet to user B. however, the trouble is that user C had posed as user A when he sent a message to user B. how would user B know that the message has come from user C, who posing as user A? This concept is shown in fig. below.
This type of attack is called as **fabrication.**

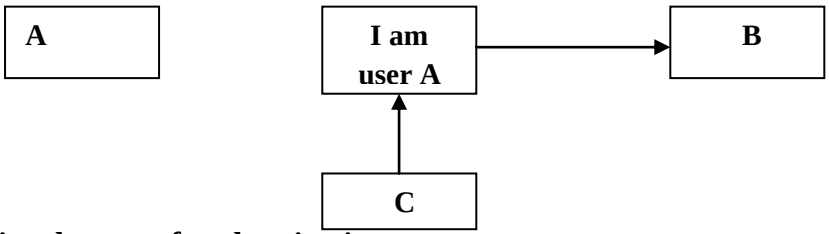



**Fig. absence of authentication**

**3. Integrity**: when the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.
For example, here user C tampers with a message originally sent by user A, which is actually destined for user B. user C somehow manages to access it, change its contents and send the changed message to user B. user B has no way of knowing that the contents of the message were changed after user A had sent it. User A also does not know about this change.
This type of attack is called as **modification**.

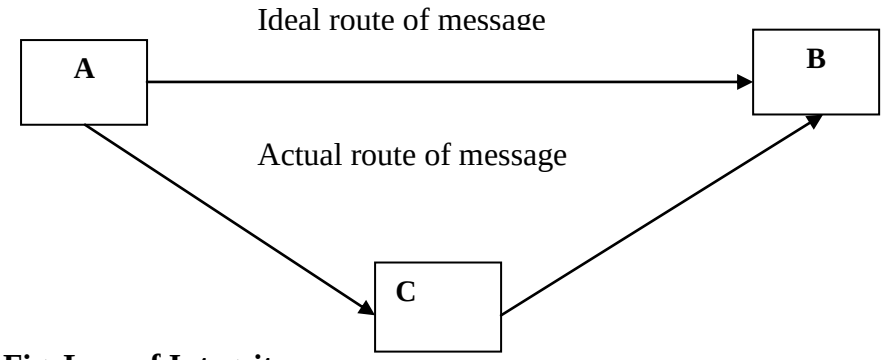



**Fig. Loss of Integrity**

b) **List any four biometrics methods used for identification. List any four advantages of biometrics.**

**Biometric** refers study of methods for uniquely recognizing humans based upon one or more intrinsic **physical** or **behavioral** characteristics.

**Different methods of Biometrics *(any four 2Marks)***

1. Finger print recognition
2. Hand print recognition
3. Retina/iris scan technique
4. Face recognition
5. Voice patterns recognition
6. Signature and writing patterns recognition
7. Keystroke dynamics

**Advantages of biometrics *(any four 2 marks)***

i) Biometrics cannot be lost, stolen or forgotten. Barring disease or serious physical injury, the biometric is consistent and permanent.
ii) It is also secure in that the biometric itself cannot be socially engineered, shared or used by others.
iii) There is no requirement to remember password or pins, thus eliminating an overhead cost.
iv) Coupled with a smart card, biometrics provides strong security for any credentials on the smart card.
v) It provides a high degree of confidence in user identity.

c) **Encryption and Decryption with reference to computer security.**

**Encryption:**

The process of encoding plain text into cipher text message is known as Encryption.


**(1 mark)**

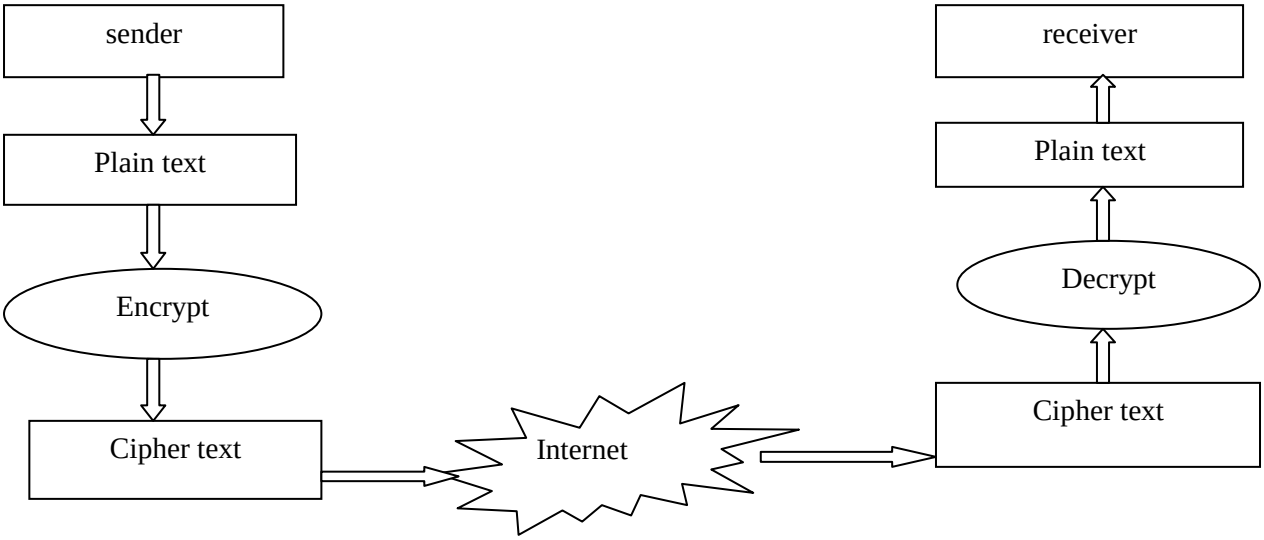
**Decryption:**

The reverse process of transforming cipher text message back to plain text message is called decryption.


**(1 mark)**

**Encryption and Decryption process (2 marks)**

In the communication, the computer at sender's end usually transforms a plain text into cipher text by performing encryption by applying encryption algorithm. The encrypted cipher text is then sent to the receiver over the network. The receiver's computer then takes the encrypted message and then perform the reverse of encryption i.e. decryption by applying decryption algorithm.




d) **Explain following terms with respect to security:**

## i. Intruders *(2 marks)*

**An intruder** is a person that enters territory that does not belong to that person. Intruders try to intrude into the privacy of the network.

**Intruders are said to be of three types, as below:**

a) **Masquerader:** A user who does not have the authority to use a computer, but penetrates into a system to access a legitimate user's account is called a masquerader. It is generally an external user.

b) **Misfeasor:** There are two possible cases for an internal user to be called as a misfeasor:
   i) A legitimate user, who does not have access to some applications, data or resources, accesses them.

ii) A legitimate user, who has access to some applications, data or resources, misuses these privileges.

c) **Clandestine user:** An internal or external user who tries to work using the privileges of a supervisor user to avoid auditing information being captured and recorded is called as a clandestine user.

**ii. Insiders** ***(2marks)***

Insiders are authorized users who try to access system or network for which he is unauthorized. Insiders are legal users. More dangerous than Intruders. They have knowledge about the security system. They have easy access to the system because they are authorized users. There is no such mechanism to protect system from Insiders.

Insiders are more dangerous than intruders because:

The insiders have the access and necessary knowledge to cause immediate damage to an organization. There is no security mechanism to protect system from Insiders. So they can have all the access to carry out criminal activity like fraud. They have knowledge of the security systems and will be better able to avoid detection.

**Q. 1) B) Attempt Any One (6 Marks)**

**a) Describe the following attacks (*3 marks each)***

**i) Sniffing:**

The group of protocols which make up the TCP/ IP suite was designed to work in a friendly environment where everybody who was connected to the network used the protocols as they were designed. The abuse of this friendly assumption is illustrated by network traffic sniffing programs, is referred to as 'sniffers'.

A network "sniffers" is a software or hardware device that is used to observe traffic as it passes through a network on shared broadcast media. The device can be used to views all traffic or it can target a specific protocol, service, or even string of characters.

**ii)spoofing:**

Spoofing is nothing more than making data look like it has come from a different source. This is possible in TCP/ IP because of the friendly assumption behind the protocol. When the protocols were developed, it was assumed that individuals who had access to the network layer would be privileged users who could be trusted. When a packet is sent from one system to another, it includes not only the destination IP address ant port but the source IP address as well which is one of the forms of Spoofing.

Example of spoofing: e-mail spoofing, URL spoofing, IP address spoofing.

**b) Enlist any four cyber-crimes *(2 marks)*. Describe anyone in detail.*(4 marks)***

1) Hacking
2) Cracking
3) Theft
4) Malicious software
5) Child soliciting and abuse

**(Any one explanation is expected)**

(i**) Hacking:**

Hacking is one of the most well-known types of computer crime. A hacker is someone who find out and exploits the weaknesses of s computer systems or networks.

Hacking refers to unauthorized access of another's computer systems. These intrusions are often conducted in order to launch malicious programs known as viruses, worms, and Trojan horses that can shut down hacking an entire computer network.

Hacking is also carried out as a way to talk credit card numbers, intent passwords, and other personal information.

By accessing commercial database, hackers are able to steal these types of items from millions of internet users all at once.

There are different types of hackers:

1. White hat
2. Black hat
3. Grey hat
4. Elite hacker
5. Script hacker

(ii) **Cracking:**

In the cyber world, a cracker is someone who breaks into a computer system or network without authorization and with the intention of doing damage.

Crackers are used to describe a malicious hacker.

Crackers get into all kinds of mischief like he may destroy files, steal personal information like credit card numbers or client data, infect the system with a virus, or undertake many others things that cause harm.

Cracking can be done for profit, maliciously, for some harm to organization or to individuals.

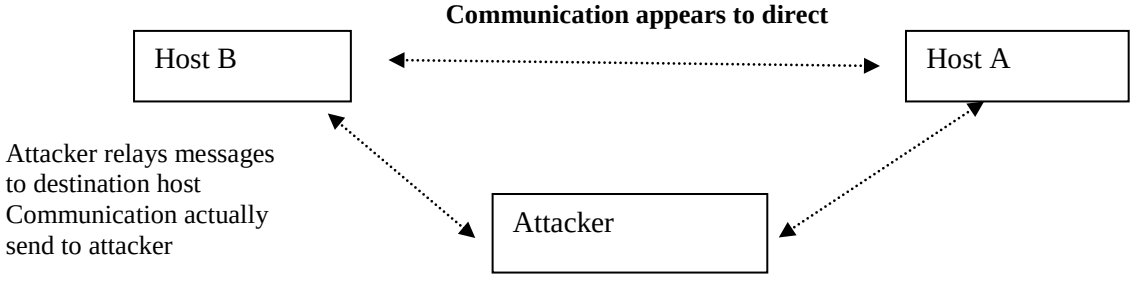
Cracking activity is harmful, costly and unethical.

**Q.2) Attempt Any Two** **16 Marks**

**a) Explain following attacks *(4 marks each)***

**i) Man in the middle attack.**

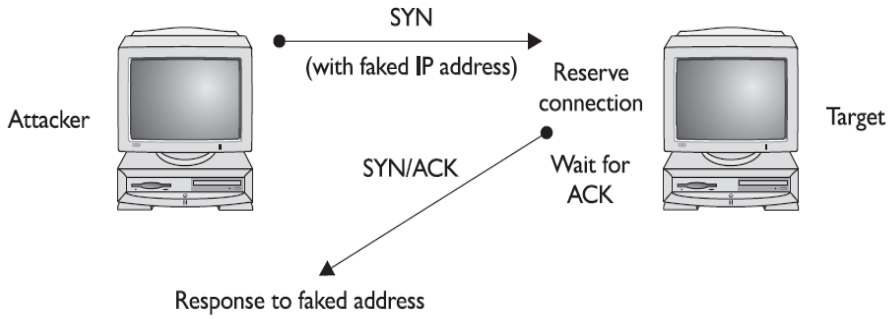
- A man in the middle attack occurs when attackers are able to place themselves in the middle of two other hosts that are communicating in order to view or modify the traffic. This is done by making sure that all communication going to or from the target host is routed through the attacker's host.
- Then the attacker is able to observe all traffic before transmitting it and can actually modify or block traffic. To the target host, communication is occurring normally, since all expected replies are received.



To prevent this attack both sender and receiver must authenticate each other.

**ii) Denial Of Service Attack.**

Denial of service (DOS) attack scan exploits a known vulnerability in a specific application or operating system, or they may attack features (or weaknesses) in specific protocols or services. In this form of attack, the attacker is attempting to deny authorized users access either to specific information or to the computer system or network itself.
The purpose of such an attack can be simply to prevent access to the target system, or the attack can be used in conjunction with other actions in order to gain unauthorized access to a computer or network.
SYN flooding is an example of a DOS attack that takes advantage of the way TCP/IP networks were designed to function, and it can be used to illustrate the basic principles of any DOS attack.SYN flooding utilizes the TCP three-way handshake that is used to establish a connection between two systems.
In a **SYN flooding attack**, the attacker sends fake communication requests to the targeted system. Each of these requests will be answered by the target system, which then waits for the third part of the handshake. Since the requests are fake the target will wait for responses that will never come, as shown in Figure .




The target system will drop these connections after a specific time-out period, but if the attacker sends requests faster than the time-out period eliminates them, the system will quickly be filled with requests. The number of connections a system can support is finite, so when more requests come in than can be processed, the system will soon be reserving all its connections for fake requests. At this point, any further requests are simply dropped (ignored), and legitimate users who want to connect to the target system will not be able to. Use of the system has thus been denied to them.

**Following are types of DOS:**
1. POD (ping-of-death)
2. DDOS (Distributed Denial of Service attack)

These types of attacks are difficult to prevent because the behavior of whole networks needs to be analyzed, not only the behavior of small piece of code.

**b) i) characteristics of good password.*(4 marks)***

1. Password should be at least eight characters in length.
2. Password should have at least three of the following four elements:
   - i. One or more upper case letters (A-Z)
   - ii. One or more lower case letters (a-z)
   - iii. One or more numerical (0to9)
   - iv. One or more special character (!, @,#,$,&,:,.,;,?)
3. Password should not consist of dictionary words.
4. Password should not at all be the same as login name.

5. Password should not consist of user's first or last name, family members name, birth dates, pet names, pin and mobile numbers.

### ii) Dumpster diving *(4 marks)*

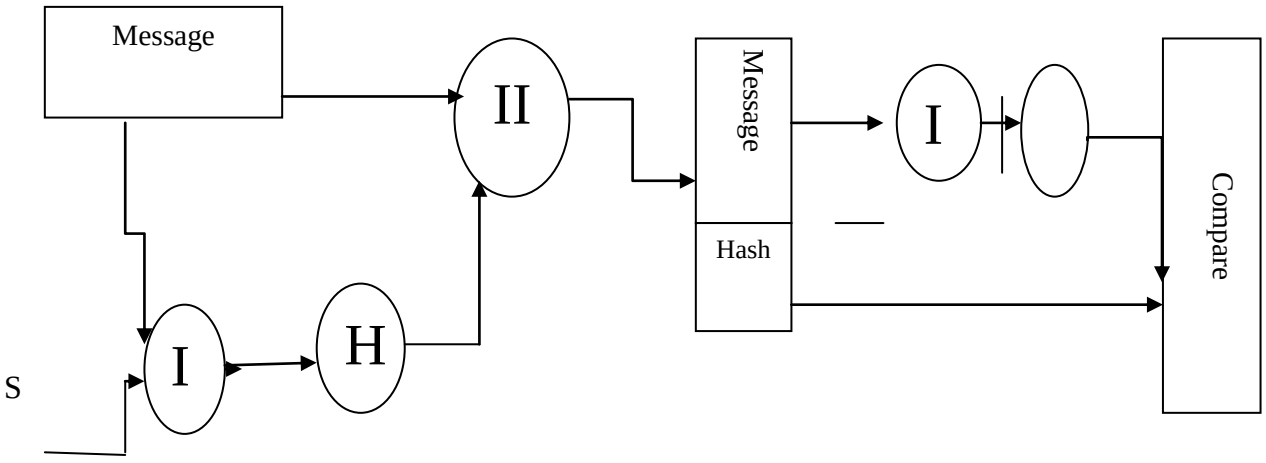
System attackers need certain amount of information before launching their attack. One common place to find this information, if the attacker is in the vicinity of target is to go through the target's thrash in order to find little bits of information that could be useful. The process of going through target's thrash is known as "**dumpster diving**".***(2 marks)***

The search is carried out in waste paper, electronic waste such as old HDD, floppy and CD media recycle and trash bins on the systems etc.

If the attacker is lucky, the target has poor security process they may succeed in finding user ID's and passwords. If the password is changed and old password is discarded, lucky dumpster driver may get valuable clue.(1mark)

**To prevent** dumpster divers from learning anything valuable from your trash, experts recommend that your company should establish disposal policy ***(1 mark)***

***d)*** **Concept of hashing with the help of diagram.** ***(4 marks)*** **.list advantages** ***(4 marks)***




S=single security key

A hash is a special function that performs one way encryption meaning that once the algorithm is processed, there is no feasible way to take the cipher text and retrieve the plain text that was used to generate it.

- The hash code is a function of all bits of the message and provides an error detection capability. A change in any bit or bits result in a change hash value.
- A hash value h is generated by a function H of the form h=H(M)

Where M is variable length message and H(M) is the fix length hash value.

- The hash value is appended to the message at the source at a time when the message is assumed or known to be correct.
- The receiver authenticates that message by recomputing the hash value.
- The message plus concatenated Hash code is encrypted using symmetric encryption. Sender and receiver share the same secret key. The message must have come from authorized sender and has not been altered is checked by recomputing and comparing hash code by receiver.

**Advantages** ***(4 points 1 mark each)***

- *I*t is more efficient to compute a digital signature using a document's message digest.
- A digest can be made public without revealing the contents of the document from which it derives.
- It is used for digital authentication must have certain properties that make it secure enough for cryptographic use.
- Combining the data message with the secret, and running it through a hash function, a signature is generated in the form of the hash value. The data message is transmitted along with the signature. The recipient combines the received message with the secret, generates a hash value, and checks to make sure it's identical to the signature. The message's authenticity is thus verified.

**Q. 3 Attempt any four: (16 Marks)**

**a) What is then application of firewall? How it works? Enlist limitations.**

***(Application – 1 Mark, Working- 2 Marks, Any two Limitation- 1 Mark)***

**Application:**

A firewall is a networking device – hardware, software or a combination of both– whose purpose is to enforce a security policy across its connection.

***Working:*** Firewalls enforce the establishment security policies. Variety of mechanism includes:

- Network Address Translation (NAT)
- Basic Packet Filtering
- Stateful Packet Filtering
- Access Control Lists (ACLs)
- Application Layer Proxies.

One of the most basic security function provided by a firewall is Network Address Translation (NAT). This service allows you to mask significant amounts of information from outside of the network.

This allows an outside entity to communicate with an entity inside the firewall without truly knowing its address. Basic Packet Filtering, the most common firewall technique, looking at packets, their protocols and destinations and checking that information against the security policy. Telnet and FTP connections may be prohibited from being established to a mail or database server, but they may be allowed for the respective service servers. This is a fairly simple method of filtering based on information in each packet header, like IP addresses and TCP/UDP ports. This will not detect and catch all undesired packet but it is fast and efficient.

Limitations:

1. Firewall do not protect against inside threats.
2. Packet filter firewall does not provide any content based filtering.
3. Protocol tunneling, i.e. sending data from one protocol to another protocol which negates the purpose of firewall.

4. Encrypted traffic cannot be examine and filter.

**b) Describe in brief:**

**i. Piggybacking**

**ii. Shoulder surfing**

***(Explanation of Piggybacking- 2 Marks, Explanation of Shoulder surfing- 2 Marks)***

**Piggy-backing** is the simple process of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building. An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card. Piggybacking, in a wireless communications context, is the unauthorized access of a wireless LAN. Piggybacking is sometimes referred to as "Wi-Fi squatting". The usual purpose of piggybacking is simply to gain free network access rather than any malicious intent, but it can slow down data transfer for legitimate users of the network. Furthermore, a network that is vulnerable to piggybacking for network access is equally vulnerable when the purpose is data theft, dissemination of viruses, or some other illicit activity.

**Example:** Access of wireless internet connection by bringing one's own computer within the range of another wireless network & using that without explicit permission

**Shoulder surfing** is a similar procedure in which attackers position themselves in such a way as-to be-able to observe the authorized user entering the correct access code or data. Both of these attack techniques can be easily countered by using simple procedures to ensure nobody follows you too closely or is in a position to observe your actions. Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine. Shoulder surfing can also be done long-distance with the idea of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paper work or your keypad from view by using your body or cupping your hand.

**c) What is meant by steganography? Describe its importance.**

**(*Meaning – 1 Mark, Importance- 3Marks)***

**Steganography:**

Steganography is the art and science of writing hidden message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.

Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, html or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text or even images.

In modern steganography, data is first **encrypted** by the usual means and then inserted, using a special algorithm, into redundant data that is part of a particular file format such as a JPEG image.

Steganography process :

Cover-media + Hidden data + Stego-key = Stego-medium

Cover media is the file in which we will hide the hidden data, which may also be encrypted using stego-key. The resultant file is stego-medium. Cover-media can be image or audio file.

Stenography takes cryptography a step further by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.

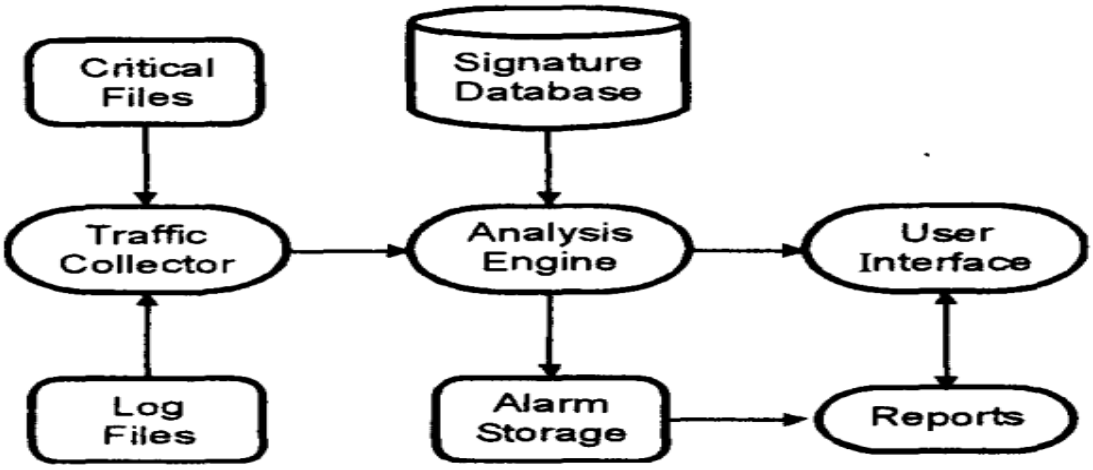
Stenography has a number of drawbacks when compared to encryption. It requires a lot of overhead to hide a relatively few bits of information.

**d) With the help of neat diagram describe host based intrusion detection system (HIDS).**

***(Diagram -2 Marks, Expnation-2 Marks)***

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator when suspicious activity is detected. HIDS is looking for certain activities in the log file are:

Logins at odd hours
Login authentication failure
Adding new user account
Modification or access of critical system files
Modification or removal of binary files
Starting or stopping processes
Privilege escalation
Use of certain programs




**Basic Components HIDS:**

**1. Traffic collector:**

This component collects activity or events from the IDS to examine.

On **Host-based IDS**, this can be log files, audit logs, or traffic coming to or leaving a specific system.

On **Network-based IDS**, this is typically a mechanism for copying traffic of the network link.

**2. Analysis Engine:**

This component examines the collected network traffic & compares it to known patterns of suspicious or malicious activity stored in the signature database.

The analysis engine acts like a brain of the IDS.

**3. Signature database:** It is a collection of patterns & definitions of known suspicious or malicious activity.

**4. User Interface & Reporting:** This is the component that interfaces with the human element, providing alerts when suitable & giving the user a means to interact with & operate the IDS.

**Advantages:**

- O.S specific and detailed signatures.
- Examine data after it has been decrypted.
- Very application specific.
- Determine whether or not an alarm may impact that specific.

**Disadvantages:**

- Should a process on every system to watch.
- High cost of ownership and maintenance.
- Uses local system resources.
- If logged locally, could be compromised or disable.

**e) Describe in brief the process of application hardening.**

**(Explanation – 4 Marks)**

**Application Hardening:** Application hardening- securing an application against local & Internet-based attacks. In this you can remove the functions or components you do not need, restrict the access where you can and make sure the application is kept up to date with patches.

It includes:

1. Application Patches- Application patches are supplied from the vendor who sells the application. They are probably come in three varieties: hot fixes, patches & up-grades.

**Hotfixes:** Normally this term is given to small software update designed to address a particular problem like buffer overflow in an application that exposes the system to attacks.

**Patch:** This term is generally applied to more formal, larger s/w updates that may address several or many s/w problems. Patches often contain improvement or additional capabilities & fixes for known bugs.

**Upgrades:** Upgrades are another popular method of patching application & they are likely to be received with a more positive role than patches.

2. Web servers: Web servers are the most common Internet server-side application in use. These are mainly designed to provide content & functionality to remote users through a standard web browser.

3. Active directory: Active Directory allows single login access to multiple applications, data sources and systems and it includes advanced encryption capabilities like Kerberos and PKI.

**Q. 4**

**A. Attempt any three: 12**

**a) Describe rail fence technique. Convert "I am student" into cipher text using rail fence method.**

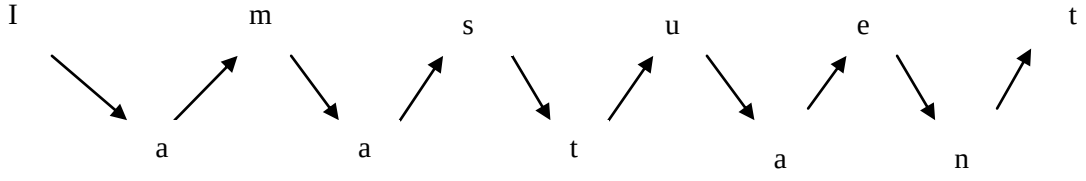
***(Algorithm – 2 Marks, Conversion- 2 Marks)***

**a.** In Rail fence cipher, techniques are essentially Transposition Ciphers and generated by rearrangement of characters in the plaintext. The characters of the plaintext string are arrange in the form of a rail-fence as follows – let the Plaintext be "I AM A STUDENT"

**Rail Fence Technique algorithm:**

1. Write down the plain text message as a sequence of diagonals.
2. Read the plain text written in step1 as a sequence of rows.

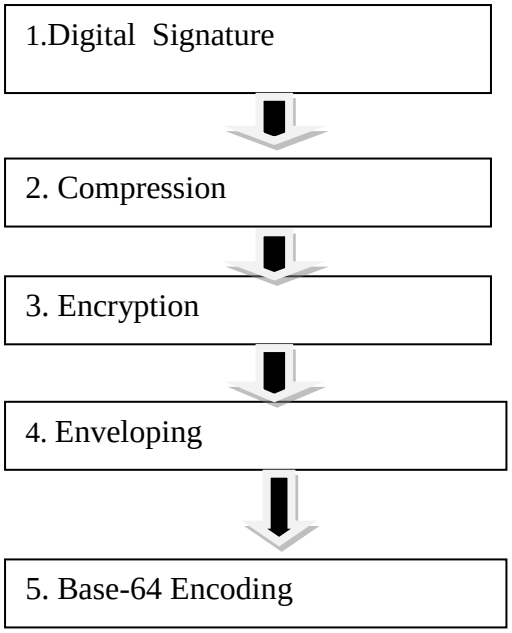
Example: plain **text = "I AM A STUDENT "** is converted to cipher text with this help of Rail Fence Technique with dual slope.



**Cipher text = " IMSUETAATDN"**

**b) Describe PGP with reference to email security.**

**Working of PGP: Five steps in PGP (Diagram- 1 Mark, Explanation- 3 marks)**
**DIG:**




1. Digital Signature
2. Compression
3. Encryption
4. Enveloping
5. Base-64 Encoding

1. **Digital signature**: it consists of the creation a message digest of the email message using SHA-1 algorithm. The resulting MD is then encrypted with the sender's private key. The result is the sender's digital signature.
2. **Compression**: the input message as well as p digital signature are compressed together to reduce the size of final message that will be transmitted. For this the Lempel-Ziv algorithm is used.
3. **Encryption**: The compressed output of step 2 (i.e. the compressed form of the original email and the digital signature together) are encrypted with a symmetric key.
4. **Digital enveloping**: the symmetric key used for encryption in step 3 is now encrypted with the receiver's public key. The output of step 3 and 4 together form a digital envelope.
5. **Base -64 encoding**: this process transforms arbitrary binary input into printable character output. The binary input is processed in blocks of 3 octets (24-bits).these 24 bits are considered to be made up of 4 sets, each of 6 bits. Each such set of 6 bits is mapped into an 8-bit output character in this process.

**c) Explain how deleted file can be recovered.**

***(4 Marks)***

**Deleted file recovery:** When we delete a file on the disk having FAT32 or NTFS (new technology file system) file system, its content is not erased from the disk but only reference to file data in file allocation Table or master table is marked as deleted. It means that we might be able to recover deleted files or make it visible for file system again. **Methods of data recovery from deleted file or File /data recovery process:** There are various data/file recovery tools available these tools find & recover recoverable deleted files from NTFS & FAT.

These tools usually operate as per following process steps:

**Step 1:** scan the hard drive & build the index of existing & deleted files & directories (folder) on any logical drive of your computer with supported file formats.

**Step 2**: Provide control over to the user to select which files to recover and what destination to recover them to. If you find a deleted file if you remember at least one of the following:

- Full or partial name
- File size
- File creation mode
- File last accessed date.

**Step 3**: Allows previewing deleted files of certain types without performing recovery.

**d) Explain with neat sketch then working of secure socket layer (SSL).**

***(Diagram 1 mark, Explanation of blocks 3 marks)***

**SSL:** SSL is a commonly used internet protocol for managing the security of a message transmission between web browser and web server. SSL is succeeded by transport layer security (TLS) and it is based on SSL. SSL uses a program layer which is located between internet's hypertext transfer protocol (http) and transport control protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most web server products. SSL provides two levels of security services, authentication and confidentiality. SSL is logically a pipe between web browser and web server.

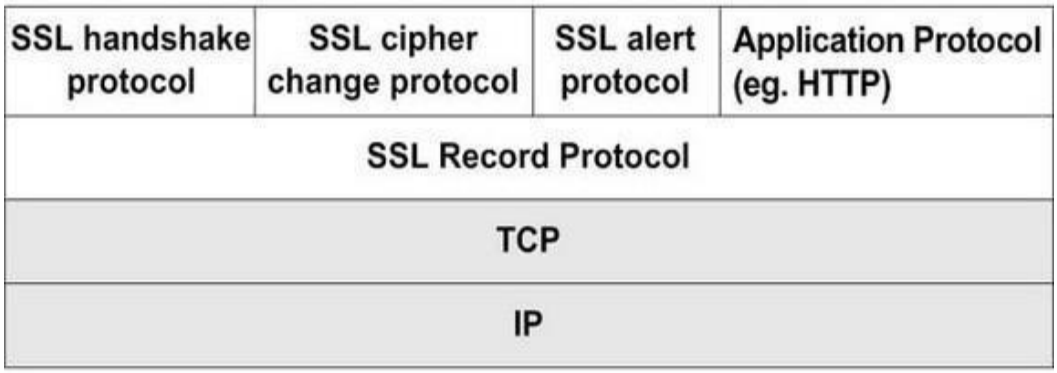



Fig. SSL protocol stack

1. **Handshake protocol:** This protocol allows the server and client to authenticate each other. Also, it will allow negotiating an encryption and MAC algorithm. This protocol is used before transmitting any application data. Basically, this protocol contains a series of messages exchanged by client and server.

The handshake protocol is actually made up of four phases, those are:

I. Establish security capabilities
II. Server authentication and key exchange
III. Client authentication and key exchange
IV. Finish

**2. Record protocol:** Record protocol comes into the picture after a successful completion of handshake between client and server. It provides two services for SSL connection, as follow:

a) **Confidentiality**: this is achieved by using the secret key that is defined by the handshake protocol.

b) **Integrity**: the handshake protocol also defines a shared secret key (MAC) that is used for assuring the message integrity.

**3. Alert protocol:** when either the client or the server detects an error, the detecting party sends an error message to other party. If the error is fatal, both the parties immediately close the SSL connection. Both the parties also destroy the session identifiers, secret and keys associated with this connection before it is terminated.

Other errors, which are not so severe, do not result in the termination of the communication. Instead, the parties handle the error and continue.

**B. Attempt any one : 6**

**a) Enlist different challenges to be faced while considering computer security.** ***(6 Marks)***

Enlist different challenges: It includes different types of threats & attacks.

**Threats to security:**

1. Viruses & worms
2. Intruders & Insiders
3. Criminal organizations
4. Terrorist & Information security

**Different types of attacks:**

1. Denial of service attack
2. Man – In – Middle attack
3. Backdoors & Trapdoors
4. Sniffing & Spoofing
5. Encryption attack
6. Replay attack
7. TCP/IP hacking attack
8. Hacking & Cracking
9. Pornography
10. Software piracy
11. Intellectual property
12. Legal system of information technology
13. Mail Bombs
14. Bug Exploits
15. Cyber-crime investigation

**[Any Related answer shall be considered]**

**b) With suitable example explain:**

**i. Logic Bomb attack and**

**ii. Time Bomb attack**

***(Each attack- 3 Marks)***

**i. Logic Bomb attack:**

Logic bombs are a type of malicious software that is deliberately installed, generally by an authorized user. A logic bomb is a piece of code that sits dormant for a period of time until some event invokes its malicious payload.

An example of a logic bomb might be a program that is set to load & run automatically and that periodically checks an organization's payroll or personal database for a specific employee. If the employee is not found, the malicious payload executes, deleting vital corporate files.

Logic bombs are difficult to detect because they are often installed by authorized users & by administrators.

**ii. Time bomb attack:**

A time **bomb** refers to a computer program that has been written so that it will stop functioning after a predetermined date or time is reached. Time bombs are commonly used in beta (pre-release) software when the manufacturer of the software does not want the beta version being used after the final release date.

Example of time bomb software would be Microsoft's Windows Vista Beta 2, which was programmed to expire on May 31, 2007. The time limits on time bomb software are not usually as heavily enforced as they are on trial software, since time bomb software does not usually implement secure clock functions.

**Q. 5 Attempt any two:** **16**

**a) Describe the role of individual user while maintaining security. What are then limitations of following biometric identification method?**

**i. Hand print**

**ii. Retina**

**iii. Voice**

**iv. Signature**

Ans: **Role of in individual user in security** ***(each point ½ Mark)***

**Individual user responsibilities:**

i) Lock the door of office or workspace.

ii) Do not leave sensitive information inside your car unprotected.

iii) Secure storage media which contains sensitive information.

iv) Shredding paper containing organizational information before discarding it.

**Give proper guidelines for:**

a) Password selection:

b) Piggybacking:

c) Shoulder surfing:

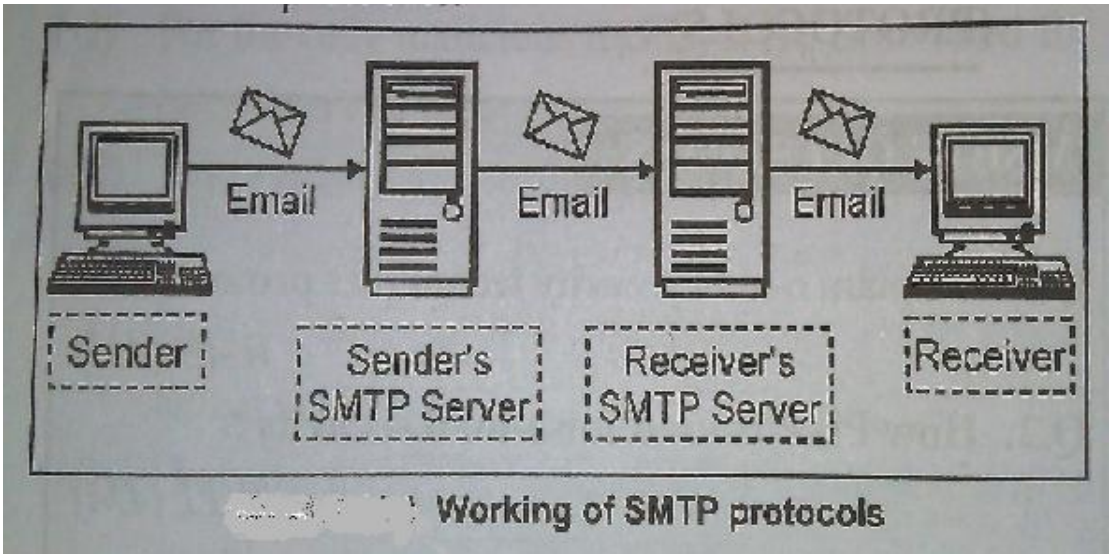
d) Dumpster diving:
e) Installing Unauthorized Software /Hardware:
f) Access by non-employees:
g) Security awareness:

i. **Hand print:** Because of cuts in hands and rough work handled by user it may create error while reading occasionally
ii. **Retina:** As per change in age and physical conditions and accidents there may be problem in accessing (Even changing numbers of spectacles, Lenses etc.)
iii. **Voice:** because health problem illness there is variation in voice even because of weather change it may cause errors.
iv. **Signature:** As per mood and temper there is change in signature of user which also creates problem to access the data.

**b)**

**i. Describe working principle of SMTP.**

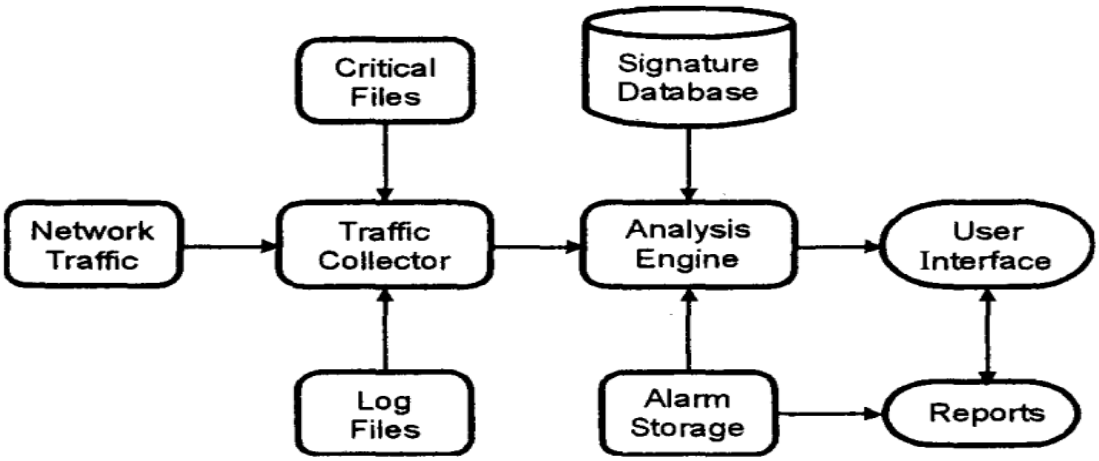
***(2marks diagram, 2 marks explanation of working principle.)***




**Simple mail Transfer Protocol:**

- Popular network services in Email.
- It is system for sending messages to other computer users based on email.
- It is request response based activity.
- Also provides email exchange process.
- It attempts to provide reliable service but not guarantees to sure recovery from failure.

**ii. With neat sketch explain then working of Network Based IDS.**




**Network Based IDS**

1. Network-based IDS focuses on network traffic —the bits & bytes traveling along the cables & wires that interconnect the system.
2. A network IDS should check the network traffic when it passes & it is able to analyze traffic accordingto protocol type, amount, source, destination, content, traffic already seen etc.
3. Such an analysis must occur quickly, &the IDS must be able to handle traffic at any speed the network operates on to be effective.
4. Network-based IDSs are generally deployed so that they can monitor traffic in &out of an organization's major links like connection to the Internet, remote offices, partner etc.

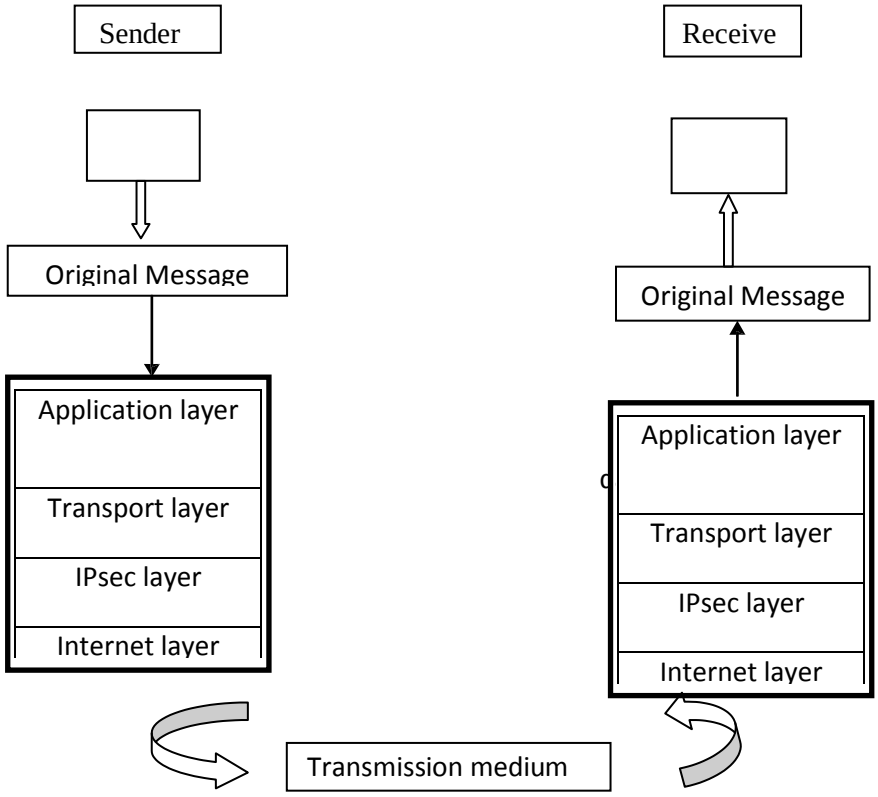
**Network-based IDSs looks for certain activities like:**

- Denial of service attacks
- Port scans or sweeps
- Malicious content in the data payload of a packet or packets
- Vulnerability scanning
- Trojans, viruses, or worms
- Tunneling
- Brute-force attacks

**c) Give IP Sec configuration. Describe AH and ESP mode of IPSEC.**

(***Diagram 1 Mark, 1 Mark Explanation, 1 Mark for AH and ESP***

***Advantages and Disadvantages -Optional)***




**IP sec overview:**

- It encrypts and seal the transport and application layer data during transmission. It also offers integrity protection for internet layer.
- It sits between transport and internet layer of conventional TCP/IP protocol.

**1. Secure remote internet access:**

Using IPsec make a local call to our internet services provider (ISP) so as to connect to our organization network in a secure fashion from our house or hotel from there; To access the corporate network facilities or access remote desktop/servers.

**2. Secure branch office connectivity:**

Rather than subscribing to an expensive leased line for connecting its branches across cities, an Organization can setup an IPsec enabled network to securely can't al lits branches over internet.

**3. Setup communication with other organization:**

Just as IPsec allow connectivity between various branches of an organization, it can also be used to connect the network of different organization together in a secure & inexpensive fashion.

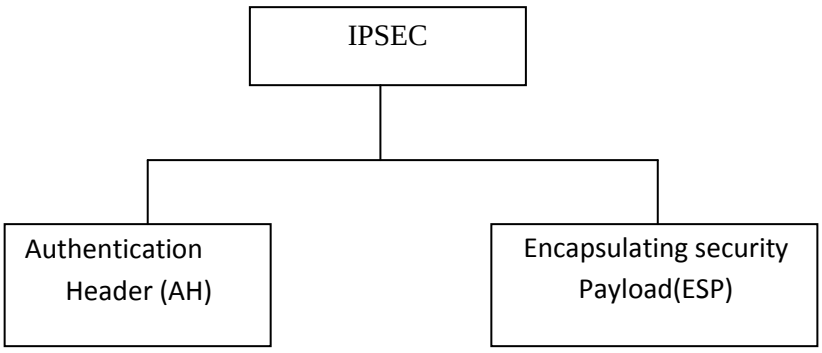
**Main advantages of IPsec:**

- IPsec is transparent to end users.
- There is no need for an user training key, key issuance or revocation.
- When IPsec is configured to work with firewall it becomes the only entry-exit point for all traffic, making it extra secure.
- IPsec works at network layer. Hence no changes are needed to upper layers or router, all outgoing & incoming traffic gets protected.
- IPsec allow travelling staff to have secure access to the corporate network
- IPsec allows interconnectivity between branches/offices in a very in expensive manner.

**Basic Concept of IPsec Protocol:**

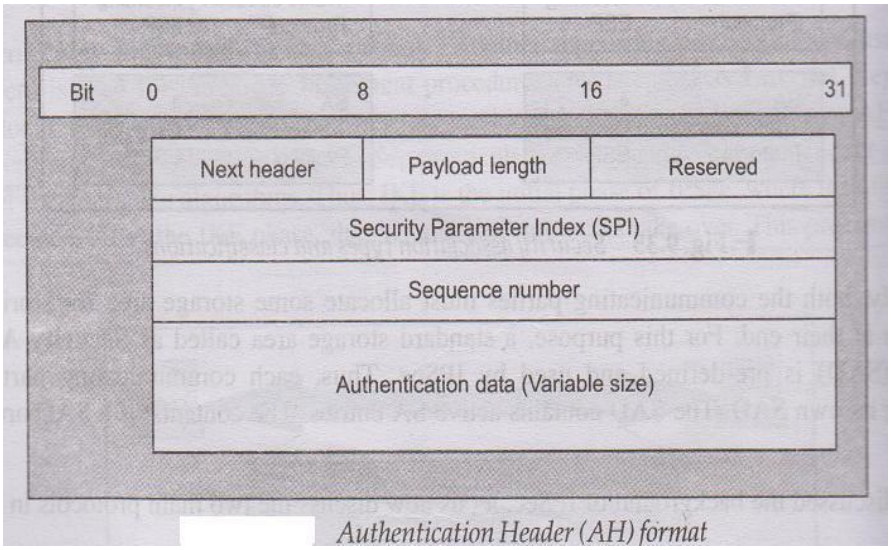
IP packet consist two position IP header & actual data IPsec feature are implemented in the form of additional headers called as extension header to the standard, default IP header. IPsec offers two main services authentication & confidentially. Each of these requires its own extension header. Therefore, to support these two main services, IPsec defines two IP extension header one for authentication & another for confidentiality.

It consists of two main protocols.



**Authentication header (AH):**

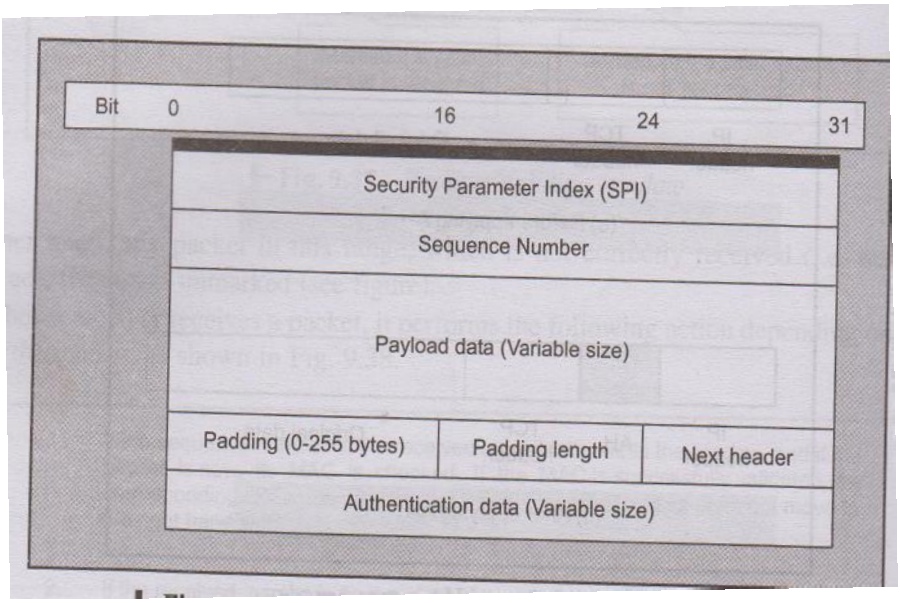
Authentication header is an IP Packet (AH) protocol provides authentication, integrity &an optional anti-reply service. The IPsec AH is a header in an IP packet. The AH is simply inserted between IP header & any subsequent packet contents no changes are required to data contents of packet. Security resides completing in content of AH. (2Marks)




*Authentication Header (AH) format*

**Encapsulation Header (ESP):**

- Used to provide confidentiality, data origin authentication, data integrity,
- It is based on symmetric key cryptography technique.
- ESP can be used in isolation or it can be combined with AH.




Q. 6 **Attempt any four:** **(16 Marks)**

**a) Describe role of people in security.**

Ans: Role of people in security ***(each point ½ Mark)***

**a) Password selection:**

1) User should be able to create their own easy to remember passwords, but should not be easy for someone else to guess or obtain using password cracking utilities.

2) Password should meet some essential guidelines for eg.pw should contain some special characters etc

3) It should not consist of dictionary words. etc

**b) Piggybacking:** It is a simple approach of following closely behind a person who has just used their own access card or PIN to gain physical access. In this way an attacker can gain access to the facility without knowing the access code.

**c) Shoulder surfing**: An attacker positions themselves in such a way that he is able to observe the authorized user entering the correct access code.

**d) Dumpster diving**: It is the process of going through a target's trash in order to find little bits of information.

**e) Installing Unauthorized Software/Hardware**: because of possible risks, many organizations do not allow their users to load software or install new hardware without the information and help of administrators. Organizations also restrict what an individual do by received e-mails.

f) **Access by non-employees**: If attacker can get physical access to a facility then there are many chances of obtaining enough information to enter into computer systems and networks. Many organizations restrict their employees to wear identification symbols at work.

**g) Security awareness**: security awareness program is most effective method to oppose potential social engineering attacks when organization's security goals and policies are established. An important element that should concentrate in training is which information is sensitive for organization and which may be the target of a social engineering attack.

**h) Individual user responsibilities:**

i) Lock the door of office or workspace.

ii) Do not leave sensitive information inside

your car unprotected. iii) Secure storage media

which contains sensitive information.

iv) Shredding paper containing organizational information before discarding it.(more points can be added).

**b) What is meant by access control Describe in brief:**

**i. DAC**

**ii. MAC**

**iii. RBAC**

**Ans:**

***(1 Mark for Access control , 1 Mark each for Type of Access Control)***

Access is the ability of a subject to interest with an object. Authentication deals with verifying the identity of a subject. It is ability to specify, control and limit the access to the host system or application, which prevents unauthorized use to access or modify data or resources.

It can be represented using **Access Control matrix or List**:

| | **Process 1** | **Process 2** | **File 1** | **File 2** | **Printer** |
|---|---|---|---|---|---|
| **Process 1** | Read, Write, Execute | --- | Read | Read | Write |
| **Process 2** | Execute | Read, Write, Execute | Read | Read, Write | Write |

**Various access controls are**:

- **Discretionary Access control (DAC):** Restricting access to objects based on the identity of subjects and or groups to which they belongs to , It is conditional, basically used by military to control access on system. **UNIX based System** is common method to permit user for read/write and execute
- **Mandatory Access control (MAC):** It is used in environments where different levels of security are classified. It is much more restrictive. It is sensitivity based restriction, formal authorization subject to sensitivity. In MAC the owner or User can not determine whether access is granted to or not. i.e. **Operating system rights.** Security mechanism controls access to all objects and individual cannot change that access.
- **Role Based Access Control (RBAC):** Each user can be assigned specific access permission for objects associated with computer or network. Set of roles are defined. Role in-turn assigns access permissions which are necessary to perform role.

Different User will be granted different permissions to do specific duties as per their classification.

**c) Explain Virtual Private Network in brief. Define DMZ.**

Ans.: ***VPN architecture and working (2 marks)***

**A VPN** is a mechanism of employing encryption, authentication, and integrity protection so that we can use a public network as if it is a private network Suppose an organization has two networks, Network 1 and Network 2, which are physically apart from each other and we want to connect them using VPN approach. In such case we set up two firewalls, Firewall

1 and Firewall 2.The encryption and decryption are performed by firewalls. Network 1 connects to the Internet via a firewall named Firewall 1 and Network 2 connects to the Internet with its own firewall , Firewall 2.

**Working**

Let us assume that host X on Network 1 wants to send a data packet to host Y on Network 2.

1) Host X creates the packet, inserts its own IP address as the source address and the IP address of host Y as the destination address.

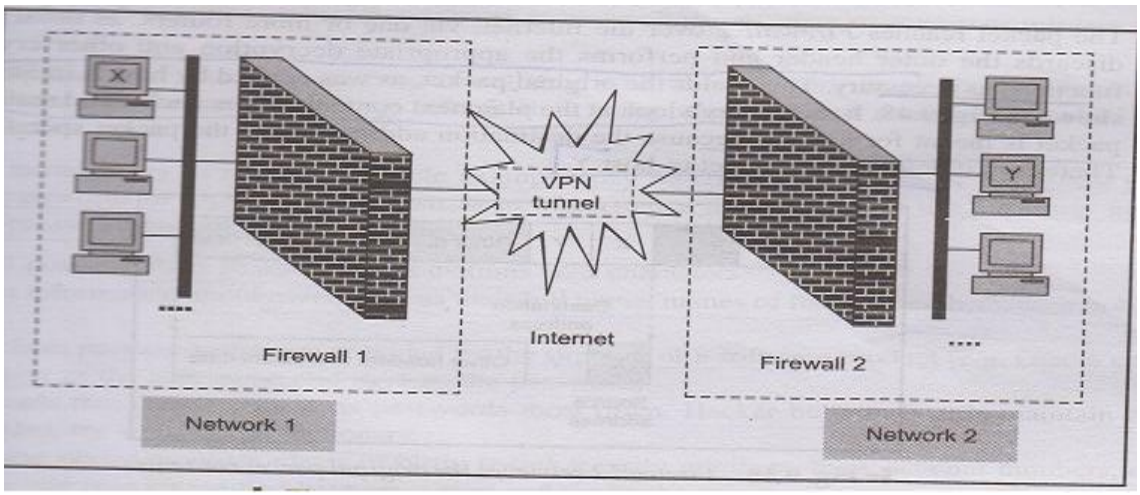
2) The packet reaches Firewall 1.Firewall 1 now adds new headers to the packet. It changes the source

IP address of the packet from that of host X to its own address(i.e. IP address of Firewall 1, F1).

3) It also changes the destination IP address of the packet from that of host Y to the IP address of Firewall 2,F2.It also performs the packet encryption and authentication, depending on the settings and sends the modified packet over the Internet

4) The packet reaches to firewall 2 over the Internet, via routers. Firewall 2 discards the outer header and performs the appropriate decryption. It then takes a look at the plain text contents of the packet and realizes that the packet is meant for host Y.It delivers the packet to host Y

**Diagram (1 marks)**




**Definition of Demilitarized Zone (DMZ):** It is a computer host or a small network inserted as a neutral zone between company's private network and outside public network. It prevents direct Access to a server that has company data.

**d) Describe data recovery principle and ethnics.**

**Ans.*:( 2 marks Data Recovery 2 marks Ethics)***

**Data recovery**: All computer users need to be aware of backup and recovery procedures to protect their data. Data Protection can be taken seriously as its important for financial, legal or personal reasons.

**Explanation of following points in short**.

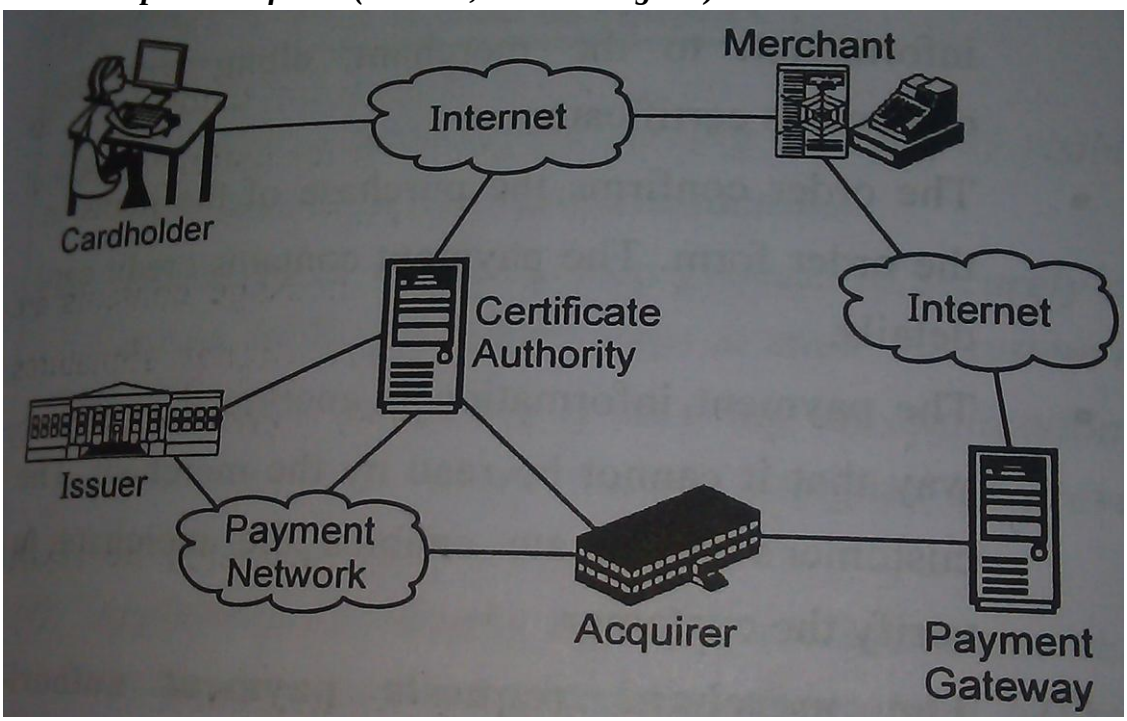
- Evaluation of Hard drive
- Recovering data
- Securing the data
- Returning of data.

**Data Recovery Ethics:** It is concerned with security of your data. These are used to think through different situations.

- ✓ It is a major part of the society and should be followed in letter and spirit
- ✓ There are policies in many organizations that provide guidelines for ethics.
- ✓ It is a behavior of the person in relation with the subject.
- ✓ There are four primary issues:
  **Privacy, Accuracy, Property and Access**
- ✓ Some standards are :
  - **Standard of right and wrong behavior**
  - **A gauge of personal integrity**
  - **The basis of trust and cooperation in relationships with others.**

**e) Describe any four components of secure electronic transaction. Give sketch also.**

**Ans.:** ***Components of SET (3 marks, 1 mark Diagram)***




Transactions supported by SET are:

a) Purchase request
b) Payment authorization
c) Payment capture

**a) Purchase request:**

Before the purchase request exchange begins, the cardholder has completed browsing, selecting, and ordering. The end of this preliminary phase occurs when the merchant sends a completed order from to the customer. All of the preceding occurs without the use of SET. The purchase request exchange consists of four messages: initiate Request, Initiate Response, and Purchase Response.

In order sent SET messages to the merchant, the cardholder must have a copy of the certificates of the merchant and the payment gateway. The customer requests the

certificates in the **Initiate Request** message, sent to the merchant. This message includes the brand of the credit card that the customer is using. The message also includes an ID assigned to this request/ response pair by the customer and a nonce used to ensure timeliness.

The cardholder verifies the merchant and gateway certificates by means of their respective CA signatures and then creates the OI and PI. The transaction ID assigned by the merchant is placed in both the OI and PI. The OI does not contain explicit order data such as the number and price of items Rather, it contains an order reference generated in the exchange between merchant and customer during the shopping phase before the first SET message. Next, the cardholder prepares the **Purchase Request** message. For this purpose, the cardholder generates a one-time symmetric encryption key; K. the message includes the following:

1. **Purchase- related information**.

2. **Order-Related information.**

3. **Cardholder certificate**

The **Purchase Response** message includes a response block that acknowledges the order and references the corresponding transaction number. This block is signed by the merchant using its private signature key. The block and its signature are sent to the customer, along with the merchant's signature certificate.

**b) Payment Authorization**

During the processing of an order from a cardholder, the merchant authorizes the transaction with the payment gateway. The payment authorization ensures that the transaction was approved by the issuer. This authorization guarantees that the merchant will receive payment; the merchant can therefore provide the services or goods to the customer. The payment authorization exchange consists of two messages: **Authorization Request** and Authorization **response**.

The merchant sends an **Authorization Request** message to the payment gateway consisting of

1. **Purchase-Related information**
2. **Authorization-related information**.
3. **Certificates.**

Having obtained authorization from the issuer, the payment gateway returns an **Authorization Response** message to the merchant. It includes the following elements:

1. **Authorization- related information.**
2. **Capture token information.**
3. **Certificate.**

With the authorization from the gateway, the merchant can provide the goods or service to the customer.

**c) Payment Capture**

To obtain payment, the merchant engages the payment gateway in a payment capture transaction, consisting of a capture request and a capture response message.

For the **Capture Request** message, the merchant generates, signs, and encrypts a capture request block, which includes the payment amount and the transaction ID. The message also includes the encrypted capture token received earlier for this transaction, as well as the merchant's signature key and key-exchange key certificates.

When the payment gateway receives the capture request message, it decrypts and verifies the capture request block and decrypts and verifies the capture token block. It then checks for consistency between the capture request and capture token. It then creates a clearing request that is sent to the issuer over the private payment network. This request causes funds to be transferred to the merchant's account.

The gateway then notifies the merchant of payment in a **Capture Response message**.

The message includes a capture response block that the gateway signs and encrypts. The message also includes the gateway's signature key certificate. The merchant software stores the capture response to be used for reconciliation with payment received from the acquirer.