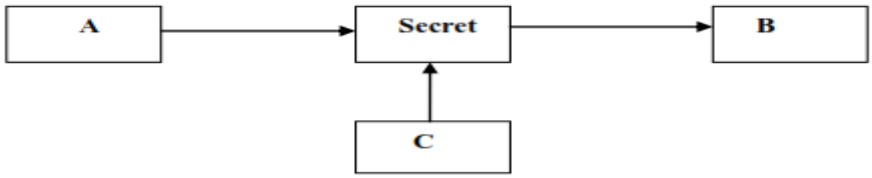
Important Instructions to examiners:

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 judgement 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. No.	Sub Q. N.	Answer	Marking Scheme
1.	**a)**	**Attempt any three.**	**12**
	a)	**Describe the basic principles of computer security.**	**4M**
	Ans:	The need of computer security has been threefold: confidentiality, integrity, and availability the "CIA" of security. Confidentiality, Integrity, Availability, Availability, Authentication, Other elements are Authorization, Non-repudiation, Access control and accountability. **1. Confidentiality:** The goal of confidentiality is to ensure that only those individuals who have the authority can view a piece of information, 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	***(1 mark for each element)***

Authentication process ensures that the origin of a message is correctly identified. Authentication deals with the desire to ensure that an individual is who they claim to be.

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.**

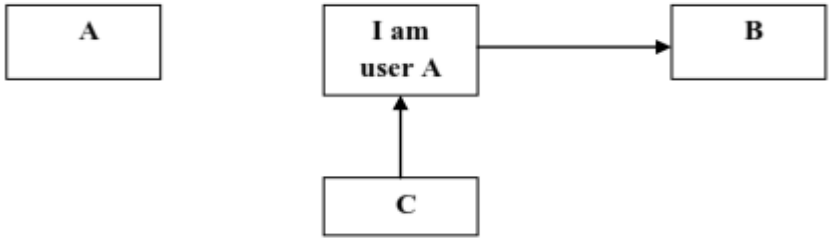


Fig. absence of authentication

3. Integrity: Integrity is a related concept but deals with the generation and modification of data. Only authorized individuals should ever be able to create or change (or delete) information. 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**.

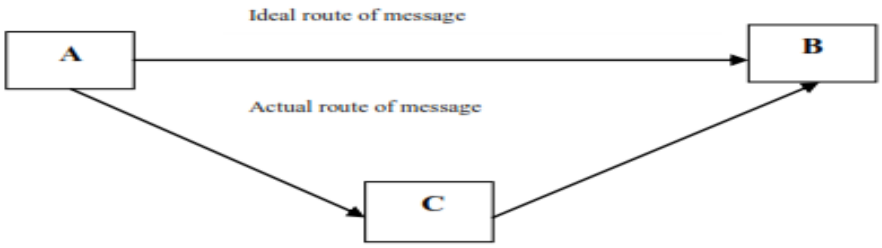
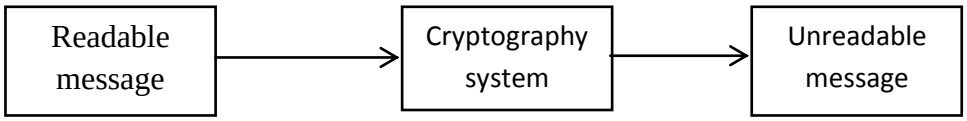
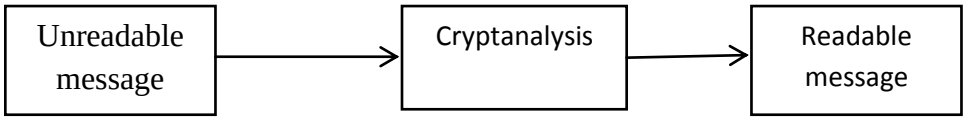


Fig. Loss of Integrity

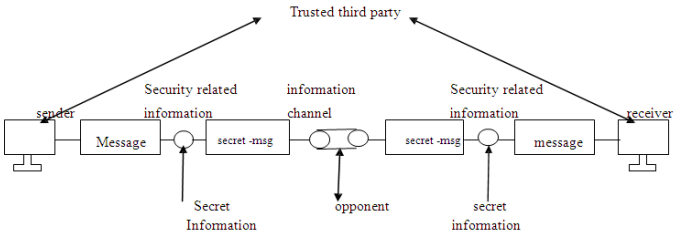
4. Availability: The goal of availability s to ensure that the data, or the system itself, is available for use when the authorized user wants it.

	b)	**List types of attacks. Explain backdoors and trapdoors attack.**	**4M**
	Ans:	Attack is any attempt to expose, destroy alter, modify sizable, steal or gain unauthorized access or use of an asset. It is kind of malicious activity that attempts to collect disrupt, deny degrade, or destroy information system resources or information. **Types of attacks are:** • Passive attacks	***(List: 2 mark and 1 mark each for explanation of backdoor and trap***

		• Active attacks • Denial of service attacks • Backdoor attacks • Trapdoor attacks • Sniffing/spoofing attacks • Man-in-the middle attacks **Backdoor Attacks:** ➢ It is secret entry point into program that allows user to gain access without going through the usual security access procedures. ➢ It is used legitimately in debugging and testing ➢ It also refers to the entry and placement of a program or utility into a network that creates a backdoor entry for attackers. ➢ This may allow a certain user ID to log on without password a program or gain of administrative services. ➢ It becomes threat when programmers use them to gain unauthorized access. ➢ There are several backdoor programs and tools used by hackers in terms of automated tools **Trapdoor Attacks:** ➢ A trap door is an entrance in an system which circumvents the normal safety measures. ➢ It is secret entry point into a program that allows someone who is aware of gaining access using procedure other that security procedure. ➢ It might be hidden program which makes the protection system ineffective. ➢ This entry can be deliberately in traduced by the developer to maintain system in case of disaster management. ➢ Trapdoor programs can be installed through malware using internet.	***door attacks)***
	c)	**Describe piggy backing and shoulder surfing.**	**4M**
	Ans:	**Piggybacking:** It 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. i.e.: Access of wireless internet connection by bringing one's own computer within range of another wireless connection & using that without explicit permission , it means when an authorized person allows (intentionally or unintentionally) others to pass through a secure door. Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge. It is a legally and ethically controversial practice, with laws that vary by jurisdiction around the world. While completely outlawed or regulated in some places, it is permitted in others. The process of sending data along with the acknowledgment is called piggybacking. Piggybacking is distinct from war driving, which involves only the logging or mapping of the existence of access points. It is the simple tactic 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	***(2 marks each for piggybacks & shoulder surfing)***

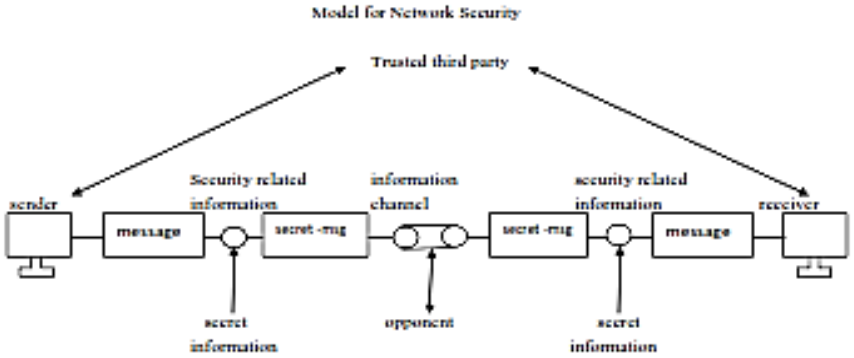
		to know the access code or having to acquire an access card .Piggybacking, in a wireless communications context, is the unauthorized access of a wireless LAN. Piggybacking is sometimes referred to as "Wi-Fi squatting." The usual purpose of piggybacking is simply to gain free network access rather than any malicious intent, but it can slow down data transfer for legitimate users of the network. **Shoulder surfing** is a similar procedure in which attackers position themselves in such away as -to be-able to observe the authorized user entering the correct access code. 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, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. 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.	
	d)	**Explain the terms: Cryptography, cryptanalysis and Cryptology.**	**4M**
	Ans:	**1. Cryptography**: Cryptography is art & science of achieving security by encoding messages to make them non-readable.  **2. Cryptanalysis**: Cryptanalysis is the technique of decoding messages from a non-readable format without knowing how they were initially converted from readable format to non-readable format.  **3. Cryptology:** It is originated from the Greek logos, means hidden words. This technique is used in cryptography for generating secured information.	***(1 mark for explanation each term and 1 mark for diagram drawn)***
	b)	**Attempt any one.**	**6**
	a)	**Describe Model for security with the help of diagram.**	**6M**
	Ans:	 	***(Diagram 2 marks and explanation 4 marks)***

OR



A message is to be transferred from one use to another user in secret form using this security system it can be two or more parties accessing information via Internet.

OR



Sender & receiver are principals of transaction and must cooperate for exchange to take place.

Model shows four basic tasks:

1. Design algorithm in such a way that an opponent cannot defeat its purpose. This algorithm is used for security related information.
2. Generate secret information that can be used with algorithm.
3. Develop method for distributing and sharing of secret information.
4. Specify a protocol which can be used by two principals that make use of security algorithm and secret information to achieve a security service. An information channel is established by defining a route through Internet from source to destination with the help of communication protocol like TCP/IP or using normal PC to PC communication through any media. Techniques for providing security have following components:-

- A security related transformation on information to be sent.
- This information shared by two principals should be secret.
- A trusted party is required to achieve secure transmission.
- This is responsible for distributing secret information between two principals.

	b)	**Explain IT Act, 2000 and IT Act, 2008.**	**6M**

	Ans:	**1) IT Act 2000*:*** According to Indian cyber laws, Information technology is the important law and it had passed in Indian parliament in year 2000.This act is helpful to encourage business by use of internet. Due to misuse of internet and increase of cybercrime, the Govt. of India made an act for safeguarding the internet users. The main objectives of this act are as follows. 1. To provide legal recognition to the transaction that can be done by electronic way or by using internet. 2. To provide legal recognition to digital signature used in transaction. 3. To provide facilities like filling of document online relating to admission or registration. 4. To provide facility to any company that they can store their data in electronic storage. 5. To provide legal recognition for bankers and other companies to keep accounts in electronic form. **It is introduced with many additional features of IT Act 2000:** They have amplified the existing provisions or introduced new provisions***. (OPTIONAL)*** • Electronics signature introduced • Important definitions added • Legally validated electronic documents reemphasized. • Critique on power of controller under the IT Act 2008 • The role of adjudicating officer under the IT Act 2008. • Composition of CAT (Cyber Appellate Tribunal) • New cybercrimes as offences under amended Act • Power of Block unlawful websites should be exercised with caution. • Section 69B added to confer power to collect, monitor traffic data • Significance of the term Critical Information Infrastructure • Important Clarifications on the Act's application and effect • The combination effect of section 88 and 77B • Combined effect of section 78 and 80. This helps to effective enforce cyber law in India. **IT acts 2008*:*** It is the Information Technology Amendment Act, 2008.the act was developed for IT industries, control e-commerce, to provide e-governance facility and to stop cybercrime attacks. **Following are the characteristics of IT ACT 2008:** This act provides legal recognition for the transaction i.e. Electronic Data Interchange (EDI) and other electronic communications. This Act also gives facilities for electronic filling of information with the Government agencies. It is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records. **State characteristics of IT Act 2008.** **Different Fraudulent situations: *(OPTIONAL)*** ➢ Tampering with any computer source code use for a computer, computer programmer computer system or computer network. ➢ Hacking with computer system ➢ Sending offensive or false information through computer or a communicative device.	***(3 marks each for IT Act 2000 ,and IT Act 2008)***

		➢ Receiving or retaining stolen computer resource or communication device. ➢ Capturing transmitting or publishing the image of a private area of any person without consent. ➢ Punishment for Cyber terrorism. ➢ Publishing transmitting information which is obscene in electronic form. ➢ Publishing and transmission of containing sexually explicit act or conduct. ➢ Penalty for mis-representation.: imprisonment for a term which may extend to two years or with fine up to Rs. 1 lakh or with both. ➢ Penalty for breach of confidentiality and privacy ➢ Punishment for disclosure of information in breach of contract. ➢ Punishment for publishing digital signature certificate false in certain particulars. ➢ Publication for fraudulent purpose. **Features of I.T. Amendment Act 2008:** ***(Optional)*** • Focusing on data privacy • Focusing on information security. • Defining cyber café. • Making digital signature technology neutral. • Defining reasonable security practices to be followed by corporate. • Redefining the role of intermediaries. • Recognizing the role of Indian computer Emergency Response Team. • Inclusion of some additional cybercrimes like child pornography and cyber terrorism. • Authorizing an Inspector to investigate cyber offences.	
2.		**Attempt any two.**	**16**
	a)	**Explain threat to security in detail w.r.t virus, worms, intruders, insiders.**	**8M**
	Ans:	Threats create vulnerabilities in computer system or network. Following are threats to security. 1. Virus & worms 2. Intruders 3. Insiders 4. Criminal organization 5. Terrorists 6. Information warfare 7. Avenues of attack 8. Steps in attack **Virus:** Computer Virus attach itself to a program or file enabling it to spread from one computer to another , leaving infection as it travels from PC to PC or over network. It copies itself into previously uninfected programs or files, and executes over other source of attack. It can cause the loss or alteration of program or data and can compromise confidentiality. It is almost attached with executable files, Steps are:	***(2 marks for each threat)***

- Virus program is launched.
- Virus code is loaded into destination.
- Virus delivers itself destructive payload.
- Virus copies itself to another program.

Characteristics are: hard to detect, not easily destroyable, spreads infection widely, easy to create, machine and operating system independent.

Worms:

- Worms are malicious programs that spread them automatically.
- Spread from computer to computer, without any human action intervention.
- It propagate autonomously, they are spread by exploiting vulnerabilities in computer system.
- Worm is designed to copy itself from PC to PC via networks or internet.
- They spread much faster than viruses.
- Its effects are localized its damage to the computer network by causing increased bandwidth.
- Worms consists of attack mechanism, payload and target selection

Intruders :

- Extremely patient as time consuming More dangerous than outsiders
- Outsiders Insiders
- Keep trying attacks till success As they have the access and knowledge to cause immediate damage to organization
- Individual or a small group of attackers They can be more in numbers who are
- Next level of this group is script writers, i.e. Elite hackers are of three types: Masquerader, Misfeasor, Clandestine user is misuse of access given by insiders directly or indirectly access the organization.
- They may give remote access to the Organization
- Intruders are authorized or unauthorized users who are trying access the system or network.
- They are hackers or crackers
- Intruders are illegal users.
- Less dangerous than insiders They have to study or to gain knowledge about the security system
- They do not have access to system.
- Many security mechanisms are used to protect system from Intruders.

Insiders:

- More dangerous than outsiders As they have the access and knowledge to cause immediate damage to organization
- They can be more in numbers who are directly or indirectly access the organization.
- They may give remote access to the organization.
- Insiders are authorized users who try to access system or network for which he is unauthorized.
- Insiders are not hackers.
- 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:
i) The insiders have the access and necessary knowledge to cause immediate damage to an organization.
ii) 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.

b) What is access control? Explain DAC, MAC and RBAC access control model. **8M**

Ans: 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. ***(2 marks for description and 2 mark each for three types of control including table)***

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 cannot 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 transposition technique. Convert plain text to cipher text using rail Fence technique "COMPUTER SECURITY". — 8M

Ans:

C		M		**U**		E		S		C		R		T	
	O		P		T		R		E		U		I		Y

(2 marks for definition, 2 marks for Step 1, 2 marks for conversion and 2 marks for cipher text.)

TYPES OF TRANSPOSITION SYSTEMS:

Nature of Transposition: Transposition systems are fundamentally different from substitution systems. In **substitution systems**, plaintext values are replaced with other values. In **transposition systems**, plaintext values are rearranged without otherwise changing them. All the plaintext characters that were present before encipherment are still present after encipherment. Only the order of the text changes. Most transposition systems rearrange text by single letters. It is possible to rearrange complete words or groups of letters rather than single letters, but these approaches are not very secure and have little practical value. Larger groups than single letters preserve too much recognizable plaintext.

a) Some transposition systems go through a single transposition process. These are called single transposition. Others go through two distinctly separate transposition processes. These are called double transposition.

b) Most transposition systems use a geometric process. Plaintext is written into a geometric figure, most commonly a rectangle or square, and extracted from the geometric figure by a different path than the way it was entered. When the geometric figure is a rectangle or square, and the plaintext is entered by rows and extracted by columns, it is called columnar transposition. When some route other than rows and columns is used, it is called route transposition.

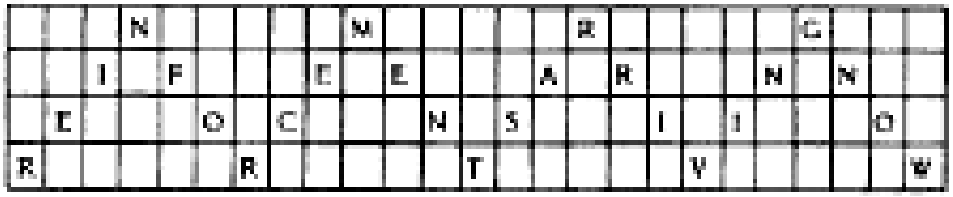
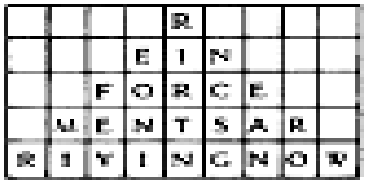
Rail Fence Technique: It is one of the easiest transposition techniques to create cipher text. When plain text message is codified using any suitable scheme, the resulting message is called Cipher text or Cipher.

Steps are:

Plain text = **COMPUTER SECURITY**

1. Write down Plain text as sequence of diagonal.

   Read Plain text written in Step 1 as sequence of rows.
   As ,
   CMUESCRT,
   Followed with
   OPTREUIY

		Then concatenate these two sequences of text as one to create following	
		Cipher text: CMUESCRTOPTREUIY	
		Following details will be OPTIONAL. **Some other examples of rail fence techniques** (1) The rail-fence cipher is inscribed by zigzag pattern and extracted by rows.  Ciphertext: NMRGI FEEAR NNEOC NSIDO RRTVW (2)The triangular pattern is inscribed by rows and extracted by columns.  Ciphertext: RMIFE YEONI RIRTN NCSGE ANROV	
3.		**Attempt any four.**	**16**
	a)	**Explain use of Biometrics in computer Security. List various Biometrics used for computer security.**	**4M**
	Ans:	**Use of biometric system in computer Security**: Biometric is a science & technology of measuring & statically analyzing biological data. The purpose of biometrics is to uniquely identify or verify an individual through the characteristics of the human body. Biometric technology must first gather information into a computer database, for example, a database of fingerprints. The computer will compare the fingerprints in the database to any new sample and recognize when there is a match. The matches can be used for both identification and verification purposes. **Enrollment:** A biometrics system searches the database for a match to the newly captured sample, and grants access if it is found. Using a fingerprint as part of the login process to a computer is an example of this mode. **Verification:** A biometrics system searches the database for a match to the newly captured sample, and authenticates an individual's claimed identity from his or her previously enrolled pattern. Biometrics uses characteristics that can be physical such hand shape, a fingerprint, facial characteristics, voice, or DNA. Biometrics can also use characteristics	***(Use of biometric system in computer Security: 2 marks, listing of any four biometric security system:2 marks)***

that are learned or acquired, behavioral traits such our signature, they way we speak or use a computer.
Strongest & highly reliable authentication method which involves the creation of users sample of authentication & store it on high end server.

During actual authentication user is required to provide same sample of authentication
Both are matched up to certain degree
Biometric helps to prove WHO ARE YOU.
At very important places like BARC, ISRO you are supposed to prove your identity biometric system is the answer.
List of various biometrics used for computer security:

1. Finger print
2. Hand print
3. Iris scan
4. Face recognition
5. DNA recognition
6. Voice pattern
7. Signature recognition
8. Keystrokes

b) Distinguish between substitution cipher and transportation cipher. **4M**

Ans:

Substitution cipher	Transposition cipher
Simple letter substitution	Letter substitution along with permutation
Guessing key is easy	Bit difficult to find a key
Less security	more security
Example Caesar Cipher	Rail fence technique / columnar technique

(Each point carries 1 mark)

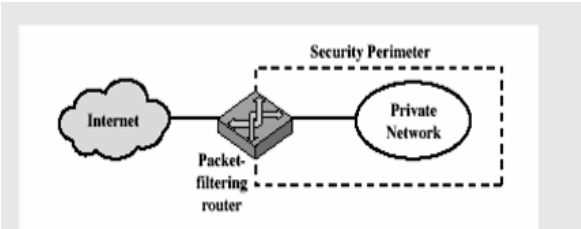
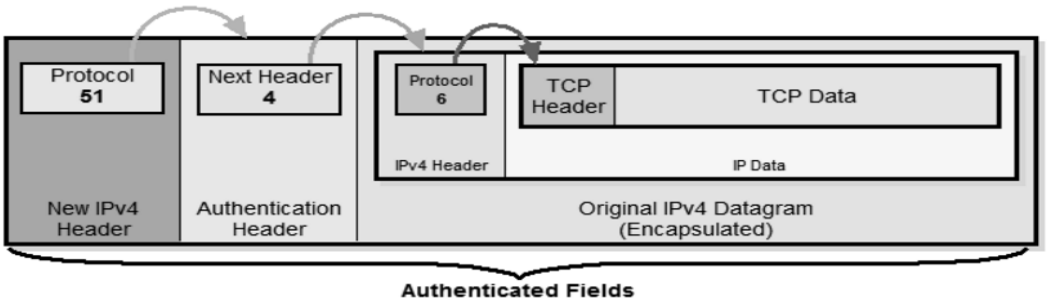
c) List types of firewall. Explain packet filter with diagrams. **4M**

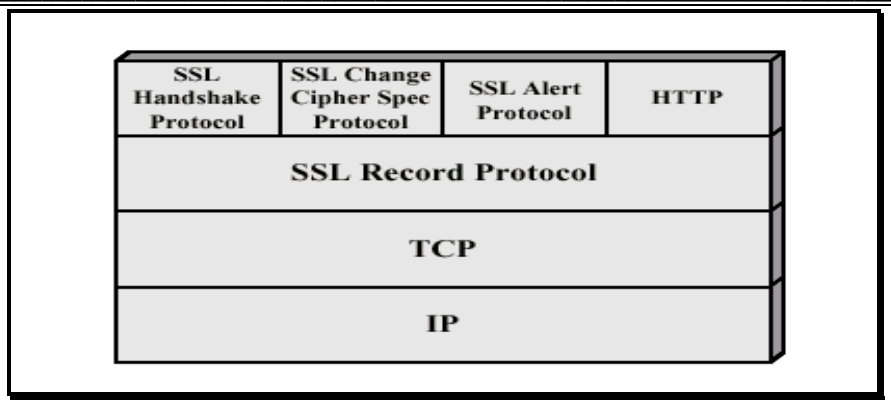
Ans: **List of types of firewall:**

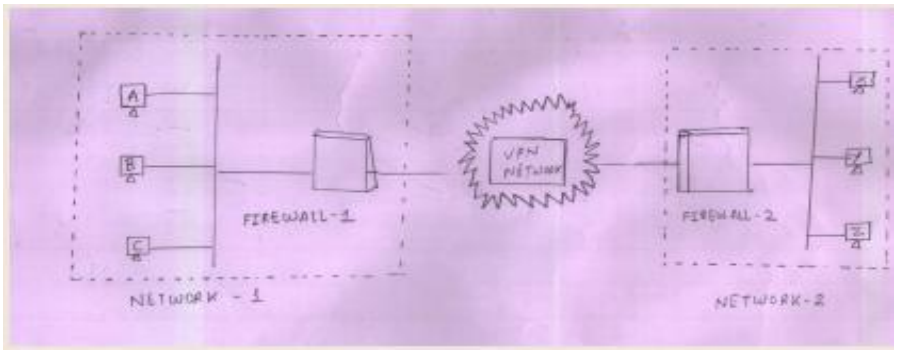
- Packet filter as a firewall
- Circuit level gateway firewall
- Application level gateway firewall
- Proxy server as a firewall

Explanation : As per the diagram given below Firewall will act according to the table given for example source IP 150.150.0.0 is the IP address of a network , all the packets which are coming from this network will be blocked by the firewall in this way it is acting as a firewall.

(Listing of types of firewall: 1 mark, Explanation of packet filter as a firewall: 2 marks ,diagram of

		Table also having port 80, IP Address 200.75.10.8 & port 23 firewall will act in the similar fashion. Port 23 is for Telnet remote login in this case firewall won't allow to login onto this server IP Address 200.75.10.8 is the IP address of individual Host, all the packet having this IP address as a destination Address will be denied. Port 80 no HTTP request allowed by firewall. Diagram of packet filter as a firewall:  **Packet Filtering**	***packet filter as a firewall: 1 mark)***
	d)	**What is IP security? Describe authentication header mode of IP security.**	**4M**
	Ans:	The IPSec Authentication Header (AH) protocol allows the recipient of a datagram to verify its authenticity. It is implemented as a header added to an IP datagram that contains an integrity check value computed based on the values of the fields in the datagram. This value can be used by the recipient to ensure that the data has not been changed in transit. The Authentication Header does not encrypt data and thus does not ensure the privacy of transmissions. Authentication Header (AH) is a member of the IPSec protocol suite. AH guarantees connectionless integrity and data origin authentication of IP packets. Further, it can optionally protect against replay attacks by using the sliding window technique and discarding old packets.  **IPv4 AH Datagram Format - IPSec Tunnel Mode**	***(IP security: 1 mark , Diagram: 1mark , Explanation: 2 marks)***
	e)	**Explain the architecture of secure socket layer.**	**4M**
	Ans:	**Architecture of SSL: Diagram:**	**(*Explanation: 2 marks, Diagram:2***

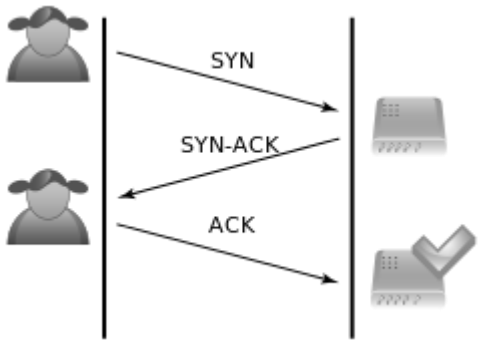
		 • SSL developed for NETSCAPE NAVIGATOR • Provides secure & authenticated communication between BROWSER & SERVER • SSL provide transport layer security (TLS) • SSL provide either server only authentication or client server authentication In server only authentication client receives the server certificate, verify it & generate KEY & encrypt it with server's public key • Client sends this encrypted secret Key to the server • Server decrypt it with his private key & use the client generated key to encrypt the message to be sent to the client In SERVER / CLIENT authentication client sends it's certificate along with secret Key so client can be authenticated • SSL consists of following protocols: • SSL Handshake Protocol • SSL Change Cipher Spec Protocol • SSL Alert Protocol • SSL Record Protocol • SSL Handshake Protocol: • Used to initiate session between client & server • Authenticate both parties to each other Algorithm & key used for encryption are negotiated • SSL Change Cipher Spec Protocol: • Used to choose cryptographic key between client & server • Key exchange method • Encryption algorithm used Functions used to obtain MAC value	***marks)***
4.	**a)**	**Attempt any three.**	**12**
	a)	**Define Caesar cipher. Write its algorithm and convert "COMPUTER SECURITY" using Caesar cipher.**	**4M**

	Ans:	**Caesar Cipher:** In cryptography, a **Caesar cipher**, also known as **Caesar's cipher**, the **shift cipher**, **Caesar's code** or **Caesar shift**, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence. **Plain Text : Computer Security** **CIPHER TEXT: FRPSXWHU VHFXULWB** **Algorithm:** **1.** Write all the Alpha bit from A TO Z **2.** Give The Numbering As 1 To 26 **3.** Replace 1st With Fourth Alpha Bit That Is A With D **4.** Write the cipher text	***(definition: 1 mark., Algorithm 2 marks, Conversion 1 mark*)**
	b)	**Draw and explain virtual private network.**	**4M**
	Ans:	**VPN Diagram:**  **Explanation:** private network created virtually between two branch networks of same company across the world. Instead of using dedicated leased line to the internetwork of company public lines can be used called as VPN. In the diagram two firewalls are acting as an intermediate between user X & user Y. If the user x is sending the message to user .If the user X is sending the message to user Y message first comes to firewall 1 which uses its own address to send this message to user Y thus over the network the packet send from user X is protected & it's IP address is protected like private network .In VPN the Tunnel technology is used to have communication between two branches of same company by wrapping the packet on another packet thus protecting network like private network.	**(*Diagram of VPN :2 marks , Explanation: 2 marks*)**
	c)	**Describe pornography and software piracy related to cybercrime.**	**4M**

	Ans:	**PORNOGRAPHY:** Is the depiction of erotic behavior (as in pictures or writing) intended to cause sexual excitement material (as books or a photograph) that depicts erotic behavior and is intended to cause sexual excitement the depiction of acts in a sensational manner so as to arouse a quick intense emotional reaction. Pictures. movies and writing about sex is called pornography (or porn). Pornography is a picture. movies and writing that is created to make people get sexually excited. **SOFTWARE PIRACY:** The unauthorized copying of software. Most retail programs are licensed for use at just one computer site or for use by only one user at any time. By buying the software, you become a *licensed* user rather than an owner (see *EULA*). You are allowed to make copies of the program for backup purposes, but it is against the law to give copies to friends and colleagues. Software piracy is all but impossible to stop, although software companies are launching more and more lawsuits against major infectors. Originally, software companies tried to stop software piracy by protecting their software. This strategy failed, however, because it was inconvenient for users and was not 100 percent foolproof. Most software now requires some sort of registration, which may discourage would-be pirates, but doesn't really stop software piracy.	***(Pornograph: 2 marks, software piracy:2 marks)***
	d)	**Explain what application hardening is.**	**4M**
	Ans:	**Application Hardening :** In computing, **hardening** is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary services. Application hardening specifically involves updating the application up to date. Don’t keep open your application always Use hot fix & patches whenever required Take license copy of application always Don’t down load an application from internet site which is not registered Don’t share admin key to anybody	***(Application Hardening (Each point carries 1 mark)***
	b)	**Attempt any one.**	**6**
	a)	**With neat sketches explain the following:** **(i). SYN Flood Attack** **(ii). Main-in-the middle attack**	**6M**

Ans:

Diagram:



(SYN flood Attack: diagram 1 mark, explanation 2 marks)

A **SYN flood** is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic

Normally when a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:

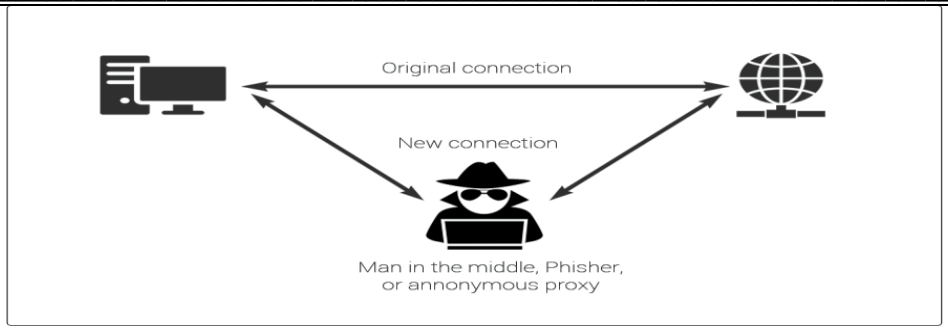
1. The client requests a connection by sending a SYN (*synchronize*) message to the server.
2. The server *acknowledges* this request by sending SYN-ACK back to the client.
3. The client responds with an ACK, and the connection is established.

This is called the TCP three-way handshake, and is the foundation for every connection established using the TCP protocol.

A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, causing the server to send the SYN-ACK to a falsified IP address - which will not send an ACK because it "knows" that it never sent a SYN.

The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK. However, in an attack, the *half-open connections* created by the malicious client bind resources on the server and may eventually exceed the resources available on the server. At that point, the server cannot connect to any clients, whether legitimate or otherwise. This effectively denies service to legitimate clients. Some systems may also malfunction or crash when other operating system functions are starved of resources in this way.

ii) **Man in the middle attack** :



In cryptography and computer security, a **man-in-the-middle attack** (often abbreviated **MitM**, **MiM attack**, **MitMA** or the same using all capital letters) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. A man-in-the-middle attack can be used against many cryptographic protocols.[1] One example of man-in-the-middle attacks is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones

	b)	**Describe packet sniffing and packet spoofing attacks.**	**6M**
	Ans:	**packet sniffing:** A **packet analyzer** also known as a network analyzer, protocol analyzer or packet sniffer, for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet. Packet sniffer specifically viewing the contents of the packet & can intimated to third required party. Like tender of a company can obtain just by viewing the info of other companies tender info & can adjusted the value as per requirement. **Packet Spoofing:** In the context of network security, a **spoofing attack** is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage spoofing involves packet can be captured , data can be modified as per the requirement of third party and may sent to recipients. Following are the types of spoofing IP Address spoofing GPS spoofing Caller id spoofing Mail spoofing Third party may use any spoofing technique as per requirement & may get	***(Packet sniffing: 3 marks packet spoofing: 3 marks)***
5.		**Attempt any two.**	**16**

	a)	Explain the role of people with respect to password selection in detail.	8M
	Ans:	**Four Password selection strategies are:** **1. User education:** (i). Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords. (ii). This user education strategy is unlikely to succeed at most installations, particularly where there is a large user population or a lot of turnover. Many users will simply ignore the guidelines. iii). Others may not be good judges of what is a strong password. iv). For example, many users believe that reversing a word or capitalizing the last letter makes a password un-guessable. **2. Computer-generated passwords:** (i). Passwords are quite random in nature. Computer generated passwords also have problems. (ii). If the passwords are quite random in nature, users will not be able to remember them. Even if the password is pronounceable, the user may have difficulty remembering it and so be tempted to write it down. (iii). In general, computer-generated password schemes have a history of poor acceptance by users. (iv). FIPS PUB 181 defines one of the best-designed automated password generators. The standard includes not only a description of the approach but also a complete listing of the C source code of the algorithm. (v). The algorithm generates words by forming pronounceable syllables and concatenating them to form a word. A random number generator produces a random stream of characters used to construct the syllables and words. **3. Reactive password checking:** (i). A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords. (ii). The system cancels any passwords that are guessed and notifies the user. iii). This tactic has a number of drawbacks. First it is resource intensive, if the job is done right. Because a determined opponent who is able to steal a password file can devote full CPU time to the task for hours or even days an effective reactive password checker is at a distinct disadvantage. iv). Furthermore, any existing passwords remain vulnerable until the reactive password checker finds them. **4. Proactive password checking:** (i). The most promising approach to improved password security is a proactive password checker. (ii). In this scheme, a user is allowed to select his/her own password. However, at the time of selection, the system checks to see if the password is allowable and if not, rejects it. (iii). Such checkers are based on the philosophy that with sufficient guidance from the system, users can select memorable passwords from a fairly large password space that are not likely to be guessed in a dictionary attack. (iv). The trick with a proactive password checker is to strike a balance between user acceptability and strength. (v). If the system rejects too many passwords, users will complain that it is too hard to select a password.	***(2 marks list: 1.5 marks: explanation of each strategy)***

		(vi). If the system uses some simple algorithm to define what is acceptable, this provides guidance to password crackers to refine their guessing technique. In the remainder of this subsection, we look at possible approaches to proactive password checking.	
	b)	**What is security topology? Describe security zone in detail.**	**8M**
	Ans:	**Security topology:** A security topology is the arrangement of hardware devices on a network with respect to internal security requirements and needs for public access. **OR** Security topology is a local map that depicts the interconnectivity between security devices and security domains that host these networks. **Security Zone:** Security zones are the building blocks for policies; they are logical entities to which one or more interfaces are bound. Security zones provide a means of distinguishing groups of hosts (user systems and other hosts, such as servers) and their resources from one another in order to apply different security measures to them. **Types of security zone:** **i. Internet Zone:** ➢ This zone contains websites. ➢ These sites are not on your computer or on your local intranet. ➢ It is not a single network but it is a series of interconnected networks. ➢ It is used to transfer email, files, financial records etc from one network to another. ➢ Since everyone has access to this network, so it is difficult to impose security policies, so it is considered to be un-trusted system. ➢ www (World Wide Web) is frequently used with internet. **ii. Intranet Zone:** ➢ It is a private network and is restricted within an organization (LAN). ➢ It consists of connections through one or more gateway computers to the outside world i.e. Internet. ➢ Purpose of Intranet is to share information and computing resources between the employees of a company. ➢ It provides facility to work in groups and for telecommunication. ➢ It uses Internet protocol like TCP/IP, HTTP etc. **iii. Trusted Sites:** ➢ This zone contains websites that you trust are safe. ➢ When you add websites to trusted site zone you believe that files you download or that you run from the websites will not damage the computer or data. **iv. Restricted Sites:** ➢ This zone contains websites which are not trusted. ➢ When anyone adds a website to this zone, he believes that the files that are downloaded or that run from this website may damage the computer or data.	***(2 marks Definition: 1 mark Listing zones: 1.5 marks explanation of each zone)***
	c)	**What is Kerberos? Explain with diagram different servers involved in Kerberos.**	**8M**
	Ans:	1. Kerberos is a network authentication protocol. It is designed to provide strong	***(2 marks***

authentication for client/server applications by using secret-key cryptography.

2. It uses secret key cryptography.

3. It is a solution to network security problems.

4. It provides tools for authentication and strong cryptography over the network to help you secure your information system

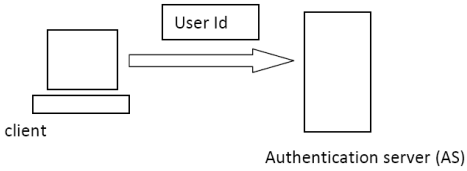
5. There are 4 parties involved in Kerberos protocol

- User
- Authentication service (AS)
- Ticket granting server (TGS)
- Service server

Kerberos Explanation: 6 marks working with diagram)

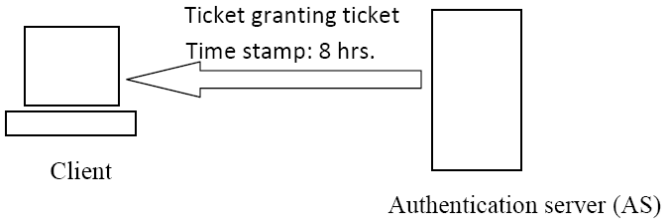
Working of Kerberos:

1. The authentication service, or AS, receivers the request by the client and verifies that the client is indeed the computer it claims to be. This is usually just a simple database lookup of the user's ID.

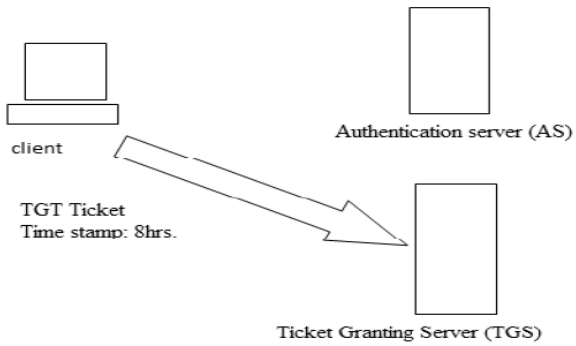


2. Upon verification, a timestamp is created. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours. The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless.

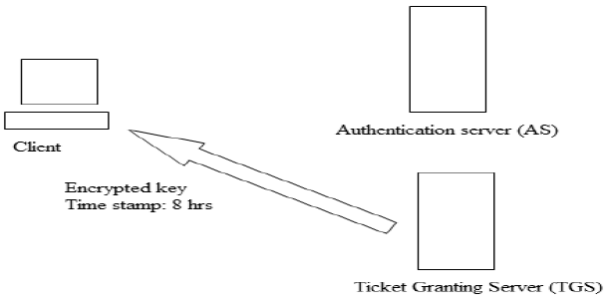
3. The key is sent back to the client in the form of a ticket-granting ticket, or TGT. This is a simple ticket that is issued by the authentication service. It is used for authentication the client for future reference.



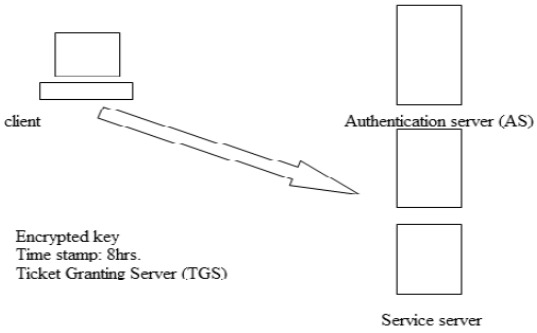
4. The client submits the ticket-granting ticket to the ticket-granting server, or TGS, to get authenticated.



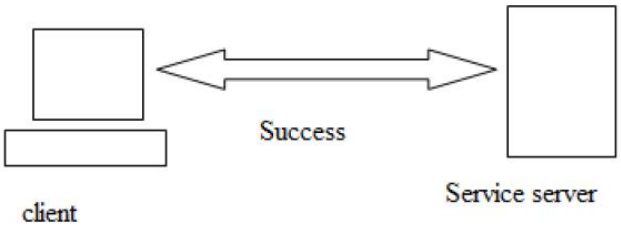
5. The TGS creates an encrypted key with a timestamp, and grants the client a service ticket.



6. The client decrypts the ticket, tells the TGS it has done so, and then sends its own encrypted key to the service.



7. The service decrypts the key, and makes sure the timestamp is still valid. If it is, the service contacts the key distribution center to receive a session that is returned to the client.



8. The client decrypts the ticket. If the keys are still valid, communication is initiated between client and server.

6.		**Attempt any four.**	**16**
	a)	**Describe security awareness in security.**	**4M**
	Ans:	**1.** Security awareness program is most effective method to oppose potential social engineering attacks when organization's security goals and policies are established. **2.** 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. **3.** Companies implement tools and procedures to protect against these threats and to comply with law and regulations. **4.** Establishing and maintaining information-security awareness through a security awareness program is vital to an organization's progress and success. A robust and properly implemented security awareness program assists the organization with the education, monitoring, and ongoing maintenance of security awareness within the organization.	***(1 mark for each relevant point)***

5. Security awareness should be conducted as an on-going program to ensure that training and knowledge is not just delivered as an annual activity, rather it is used to maintain a high level of security awareness on a daily basis.

b) Distinguish between symmetric and asymmetric cryptography (any 4 points). 4M

Ans:

Categories	**Symmetric key Cryptography**	**Asymmetric key Cryptography**
Key used for encryption /decryption	Same key is used for encryption & decryption.	One key is used for encryption & another different key is used for decryption.
Key process	Ke=Kd	Ke# Kd
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original clear text size.	More than the original clear text size.
Key agreement/exchange	A big problem	No problem at all.
Usage	Mainly used for encryption and decryption, cannot be used for digital signatures.	Can be used for encryption and decryption as well as for digital signatures.
Efficiency in usage	Symmetric key cryptography is often used for long messages.	Asymmetric key cryptography is more efficient for short messages.

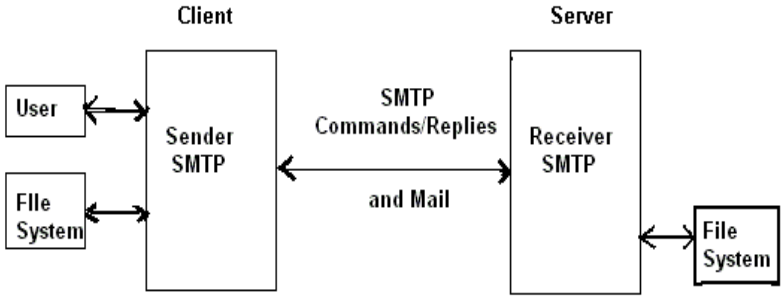
(Each comparison point: 1mark , any four points)

c) Explain e-mail security techniques (protocols). 4M

Ans: **(i). <u>SMTP- Simple Mail Transfer Protocol.</u>**

(2 marks for any two protocol and its explanation)

(i). It is a popular network services in Email communication.
(ii). It is system for sending messages to other computer users based on email.
(iii). It is request response based activity.
(iv). It also provides email exchange process.
(v). It attempts to provide reliable service but not guarantees to sure recovery from failure.



(ii). PEM- Privacy Enhanced Mail.

(i). Privacy-Enhanced Mail (PEM) is an Internet standard that provides for secure exchange of electronic mail.
(ii). PEM employs a range of cryptographic techniques to allow for
(iii). Confidentiality
(iv). Non - repudiation
(v). Message integrity
(vi). The confidentiality feature allows a message to be kept secret from people to whom the message was not addressed.
(vii). The Non - repudiation allows a user to verify that the PEM message that they have received is truly from the person who claims to have sent it.
(viii). The message integrity aspects allow the user to ensure that a message hasn't been modified during transport from the sender.

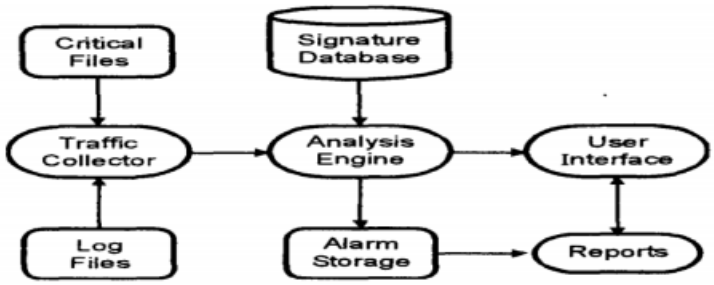
(iii). PGP- Pretty Good Privacy: Pretty Good Privacy is a popular program used to encrypt and decrypt email over the internet.

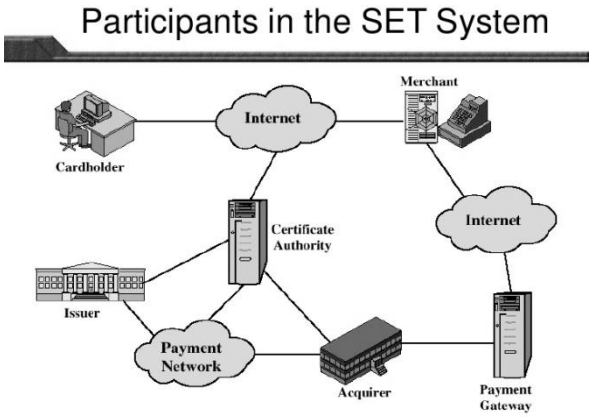
(i). It becomes a standard for e-mail security.
(ii). It is used to send encrypted code (digital signature) that lets the receiver verify the sender‘s identity and takes care that the route of message should not change.
(iii). PGP can be used to encrypt files being stored so that they are in unreadable form and not readable by users or intruders.
(iv). It is available in Low cost and Freeware version.
(v). It is most widely used privacy ensuring program used by individuals as well as many corporations.

(iv). S/MIME – Secure Multipurpose Internet Mail Extension:

(i). The traditional email system using SMTP protocol are text based which means that a person can compose text message using an editor and them sends it over Internet to the recipient, but multimedia files or documents in various arbitrary format cannot be sent using this protocol.
(ii). To cater these needs the Multipurpose Internet Mail Extensions (MIME) system extends the basic email system by permitting users to send the binary files using basic email system.
(iii). And when basic MIME system is enhanced to provide security features, it is called as Secure Multipurpose Internet Mail Extensions.
(iv). S/MIME provides security for digital signature and encryption of email message.

	d)	**What is intrusion detection system? Explain host based IDS.**	**4M**
	Ans:	**Intrusion detection system (IDS):** An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action	***(1 mark IDS: 2 marks,***

		such as blocking the user or source IP address from accessing the network. **HIDS Host Intrusion Detection Systems:** (i). They are run on individual hosts or devices on the network. (ii). A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator when suspicious activity is detected. (iii). 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  **(i). Basic Components HIDS:** • **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 • **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. • **Signature database:** It is a collection of patterns & definitions of known suspicious or malicious activity. • **User Interface & Reporting:** This is the component that interfaces with the human element, providing alerts & giving the user a means to interact with & operate the IDS.	***HIDS explanation: 1 mark diagram)***
	e)	**List and explain the key participants in secure electronic transaction.**	**4M**
	Ans:	**Secure electronic Transaction** is an open encryption and security specification that is designed for protecting credit card transactions on the Internet. It is a set of security protocols and formats that enable the users to employ the existing credit card payment infrastructure on the internet in a secure manner.	***(1 mark: list, 3 marks for any Three***



Components)

Components of SET:

1. Cardholder
2. Merchant
3. Issuer
4. Acquirer
5. Payment gateway
6. Certification Authority(CA)

1. Cardholder: A cardholder is an authorized holder of a payment card such as MasterCard or Visa that has been issued by an Issuer.

2. Merchant: Merchant is a person or an organization that wants to sell goods or services to cardholders.

3. Issuer: The issuer is a financial institution that provides a payment card to a cardholder.

4. Acquirer: this is a financial institution that has a relationship with merchants for processing payment card authorizations and payments. Also provides an assurance that a particular cardholder account is active and that the purchase amount does not exceed the credit limits. It provides electronic fund transfer to the merchant account.

5. Payment Gateway: It processes the payment messages on behalf of the merchant. It connects to the acquirer's system using a dedicated network line.

6. Certification Authority (CA): This is an authority that is trusted to provide public key certificates to cardholders, merchant, and Payment Gateway.