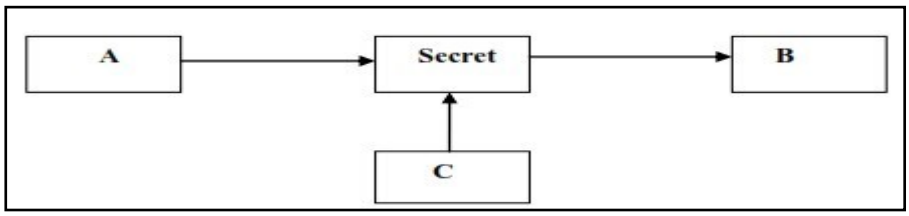
WINTER– 17 EXAMINATION

Subject Name: Computer Security **Model Answer** **Subject Code: 17514**

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 Marks**
	(i)	**State the need 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**	**(1 mark for each point ; Diagram optional)**

Here, the user of a computer A sends 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. 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.**

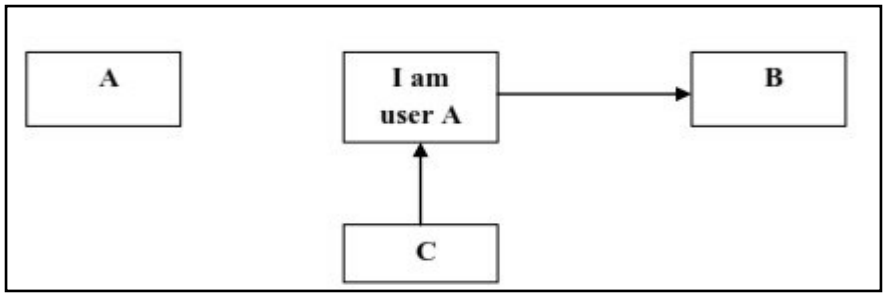


Fig. absence of authentication

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.**

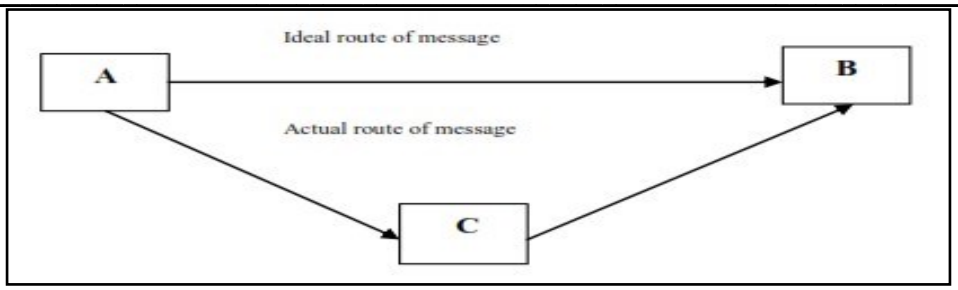


Fig. Loss of Integrity

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.

	(ii)	**List types of attacks. Explain back doors and trap doors attacks**	**4M**
	Ans:	**Types of attacks are:** 1. Passive attacks 2. Active attacks 3. Denial of service attacks 4. Backdoor attacks 5. Trapdoor attacks 6. Sniffing/spoofing attacks 7. 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 a 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.	**(List: 2 Marks, Explanation of Backdoor and Trapdoor attacks: 1 Mark each)**
	(iii)	**Compare symmetric and asymmetric key cryptography.**	**4M**

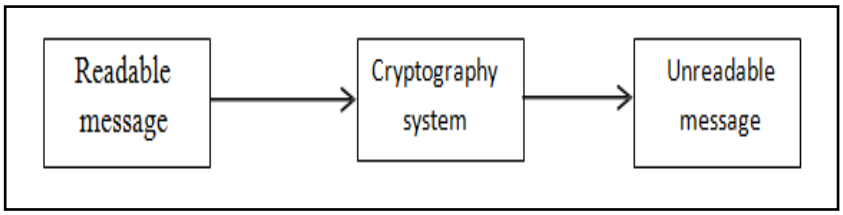
Ans: **(Each comparison point: 1mark , any four points)**

Categories	**Symmetric key**	**Asymmetric key**
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 (Same)	Ke# Kd (not same)
Speed of encryption/ decryption	Very fast	Slower
Size of resulting encrypted	Usually same as or less than	More than the original clear
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.

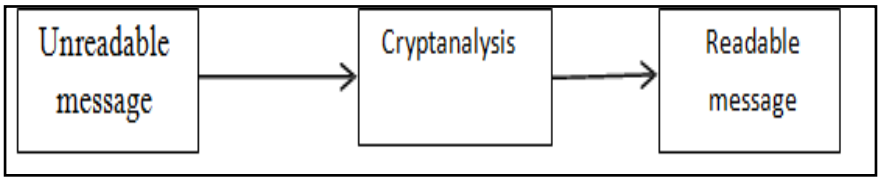
(iv) **Explain the terms: Cryptography, Cryptanalysis and Cryptology.** **4M**

Ans: **(1mark for explanation each term and 1 mark for diagram drawn)**

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 the art and science of transforming the intelligent data into unintelligent data and unintelligent data back to intelligent data.

   Cryptology = Cryptography + Cryptanalysis

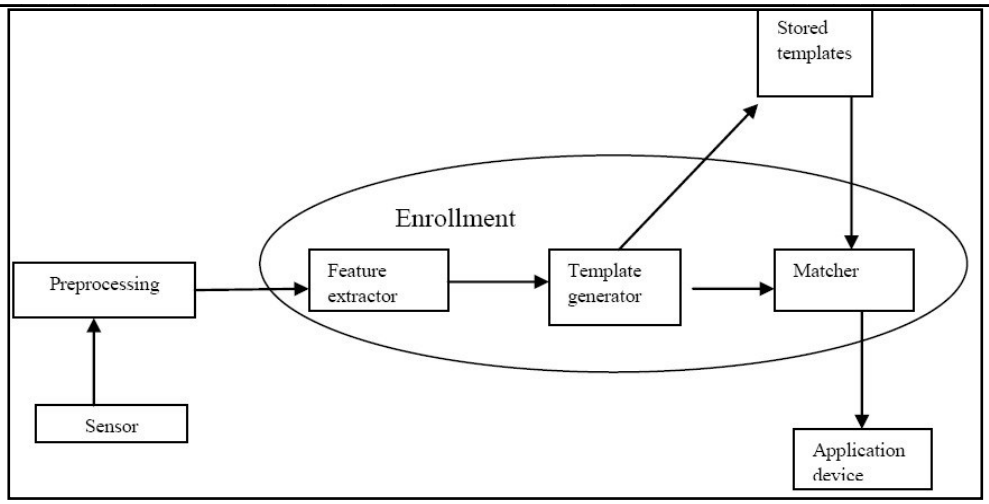
(b) **Attempt any ONE :** **6 Marks**

(i) **Describe the following attacks:** **6M**

		(A) Sniffing **(B) Spoofing**	
	Ans:	**a) Sniffing :** 1. This is software or hardware that is used to observe traffic as it passes through a network on shared broadcast media. 2. It can be used to view all traffic or target specific protocol, service, or string of characters like logins. 3. Some network sniffers are not just designed to observe the all traffic but also modify the traffic. 4. Network administrators use sniffers for monitoring traffic. 5. They can also use for network bandwidth analysis and to troubleshoot certain problems such as duplicate MAC addresses. **b) Spoofing:** 1. Spoofing is nothing more than making data look like it has come from a different source. 2. 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. 3. 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. 4. Example of spoofing: e-mail spoofing, URL spoofing, IP address spoofing.	**(Sniffing : 3 marks, Spoofing: 3 marks)**
	(ii)	**Explain data recovery tools and data recovery procedures.**	**6M**
	Ans:	**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. These are various formatted partition recovery tool available .Although every tool will have different GUI & method of recovery. **Steps of data recovery:** **Step1**: If you cannot boot the computer, please use data recovery bootable disk. **Step 2:** Select the file types you want to recover & volume where the formatted hard drive is. The tool will automatically scan the selected volume. **Step 3:** Then the founded data will be displayed on the screen & you can get a preview of it. Then select the file or directory that you want to recover & save them to a healthy drive. **Data recovery procedures:** A computer data recovery procedure is an important part for any computer literate personality that cannot be neglected. Computer professional or computer forensic expert who uses data recovery should maintain the secrecy and privacy of the client. Any action or activity that leads to disclosure of privacy of the client should be avoided. The values such as integrity, accuracy & authenticity should be exercised in an ethical environment. The evidence that is produced before the court should be fairly examined & analyzed. There should not be any carelessness and ignorance regarding the handling of	**(Explanation of Data recovery : 4 marks, Procedure : 2 marks)**

		evidence. The case evidence should be examined in detail based upon validated principles.	
2.		**Attempt any TWO of the following:**	**16 Marks**
	(a)	**Explain any four attacks on Computer System Security.**	**8M**
	Ans:	**Different types of attacks are as follows:** 1) Denial-of-service attacks 2) Backdoors and Trapdoors 3) Sniffing 4) Spoofing 5) Man In middle attack 6) Replay attack 7) TCP/ IP Hijacking. 8) Malware or malicious code such as viruses **1. 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. **2. Backdoors and Trapdoors:** They are the methods used by software developers to ensure that they could gain access to an application even if something were to happen in the future to prevent normal access methods. For e.g. A hard coded password that could be used to gain access to the program in the event that administrator forgot their own system password. The problem with this sort of password (sometimes referred to as trapdoor) is that since the password is hard coded it cannot be removed. If the attacker learns about the backdoor, all systems running the software would be vulnerable. **3. Sniffing:** A network sniffer is a software or hardware device that is used to observe the traffic as it passes through the network on shared broadcast media. The device can be used to view all traffic, all it can target a specific protocol, service or even string of characters. Normally the network device that connects a computer to a network	**(Explanation of Any four Attacks: 2 marks each)**

		is designed to ignore all traffic that is not destined for that computer. Network sniffers ignore this friendly agreement and observe all traffic on the network whether destined for that computer or others. **4. Spoofing:** It makes the data look like it has come from other source. This is possible in TCP/IP because of the friendly assumptions behind the protocols. When a packet is sent from one system to another, it includes not only the destination IP address but the source IP address. The user is supposed to fill in the source with your own address, but there is nothing that stops you from filling in another system‘s address. **5. 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. **6. Replay Attack:** In replay attack an attacker captures a sequence of events or some data units and resends them. For example suppose user A wants to transfer some amount to user C’s bank account. Both users A and C have account with bank B. User A might send an electronic message to bank B requesting for fund transfer. User C could capture this message and send a copy of the same to bank B. Bank B would have no idea that this is an unauthorized message and would treat this as a second and different fund transfer request from user A. So C would get the benefit of the fund transfer twice once authorized and once through a replay attack.	
	(b)	**What is the importance of biometrics in Computer security? Describe finger prints registration and verification process.**	**8M**
	Ans:	**Importance of Biometrics:** Biometric refers study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral characteristics. 1. Biometric identification is used on the basis of some unique physical attribute of the user that positively identifies the user. Example: finger print recognition, retina and face scan technic, voice synthesis and recognition and so on. 2. Physiological are related to shape of the body. 3. For example finger print, face recognition, DNA, palm print, iris recognition and so on. 4. Behavioural are related to the behaviour of a person. 5. For example typing rhythm, gait, signature and voice. 6. The first time an individual uses a biometric system is called an enrolment. 7. During the enrolment, biometric information from an individual is stored. 8. In the subsequent uses, biometric information is detected and compared with the information stored at the time of enrolment.	**(Diagram: 2 mark, Importance : 4 marks, Fingerprint registration & verification process: 2 mark)**



Different methods of Biometrics
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

Fingerprint registration & verification process: During registration, first time an individual uses a biometric system is called an enrolment. During the enrolment, biometric information from an individual is stored. In the verification process, biometric information is detected and compared with the information stored at the time of enrolment.

	(c)	**Explain transposition technique. Convert plain text to Cipher text using Rail Fence technique "COMPUTER ENGINEERING".**	**8M**
	Ans:	**Transposition Technique:** 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	**(4 mark for Explanation, 2 marks for Step 1, 2 marks for cipher text.)**

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 ENGINEERING**

Step 1: Write down Plain text as sequence of diagonal.

Read Plain text written in Step 1 as sequence of rows. As,

C		**M**		**U**		**E**		**E**		**G**		**N**		**E**		**I**		**G**
	O		**P**		**T**		**R**		**N**		**I**		**E**		**R**		**N**	

Then concatenate these two sequences of text as one to create following

Cipher Text: **CMUEEGNEIGOPTRNIERN**

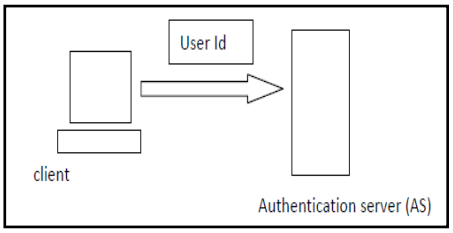
OR

The rail-fence cipher is inscribed by zigzag pattern and extracted by rows.

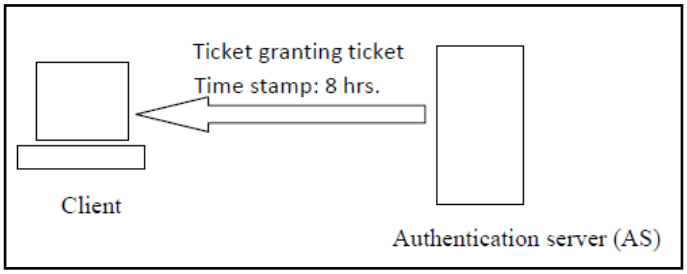
C				**U**				**E**				**N**				**I**		
	O		**P**		**T**		**R**		**N**		**I**		**E**		**R**		**N**	
		M				**E**				**G**				**E**				**G**

Cipher Text: **CUENIOPTRNIERNMEGEG**

3.		**Attempt any FOUR:**	**16 Marks**
	(a)	**Explain the concept of Kerberos.**	**4M**
	Ans:	**Kerberos** is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos was created by MIT as a solution for network security problems and it is freely available from MIT, under copyright permission. **How Kerberos does works?** Kerberos operates by encrypting data with a symmetric key. A symmetric key is a type of authentication where both the client and server agree to use a single encryption/decryption key for sending and receiving data. When working with the encryption key, the details are actually sent to a key distribution center (KDC), instead of sending the details directly between each computer. **The entire process takes a total of eight steps, as shown below.** 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.	**(Explanation with Diagrams of different steps: 4 marks)**

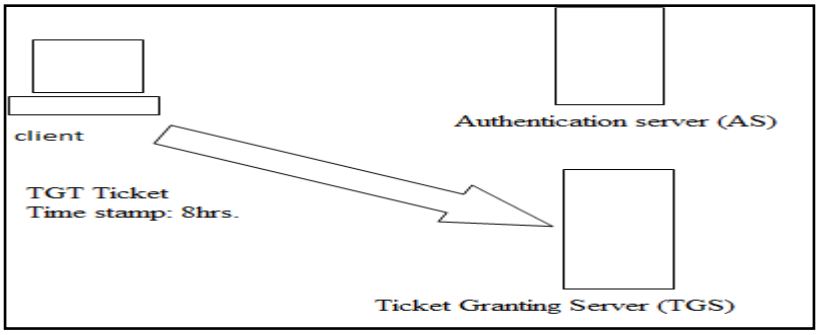


2. Upon verification, a timestamp is crated. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours. The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless. (This is used to make sure a hacker doesn't intercept the data, and try to crack the key. Almost all keys are able to be cracked, but it will take a lot longer than 8 hours to do so)

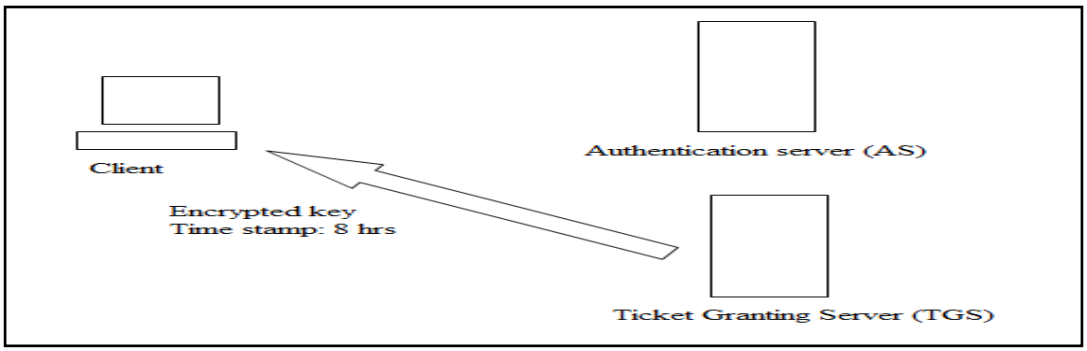


3. The key is sent back to the client in the form of a ticket-granting ticket, or TGT. This is a simple ticket that is issued by the authentication service. It is used for authentication the client for future reference.

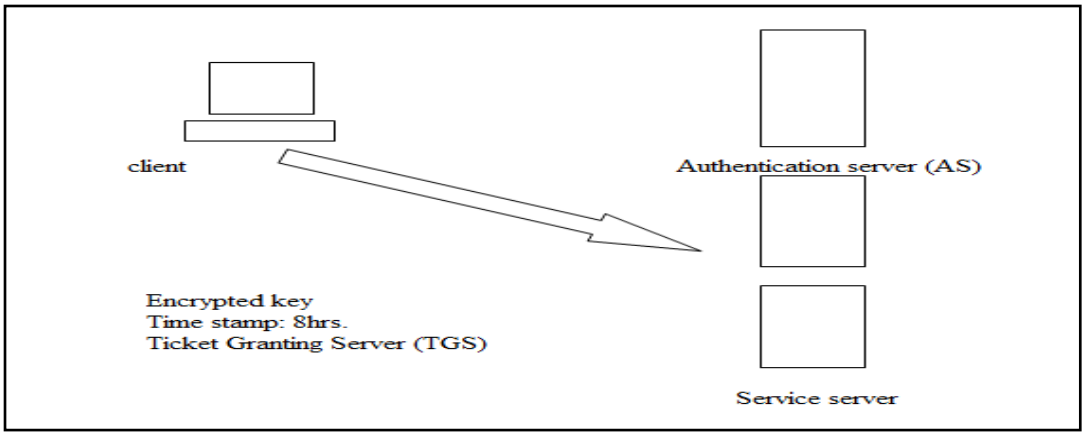
4. The client submits the ticket-granting ticket to the ticket-granting server, or TGS, to get authenticated.



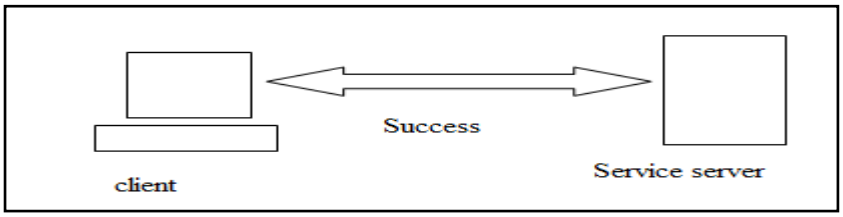
5. The TGS creates an encrypted key with a timestamp, and grants the client a service ticket.



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



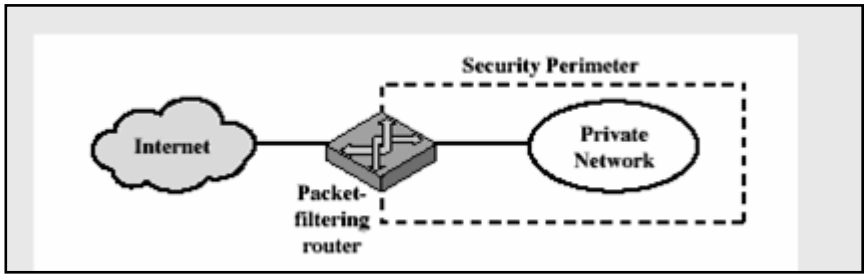
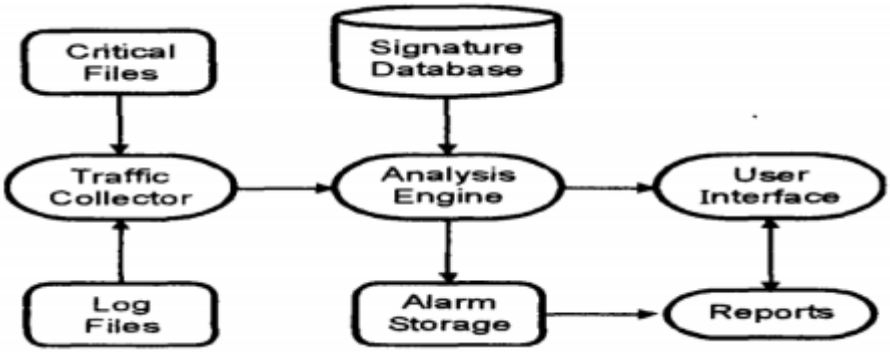
7. The service decrypts the key, and makes sure the timestamp is still valid. If it is, the service contacts the key distribution center to receive a session that is returned to the client.



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

	(b)	**Describe different password selection criteria.**	**4M**
	Ans:	**Password selection criteria :** **1. User education:** Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords. This user education strategy is unlikely to succeed at most installations, particularly where there is a large user	**(Four criteria: 1 mark Each)**

		population or a lot of turn over. Many users will simply ignore the guidelines. Others may not be good judges of what is a strong password. For example, many users believe that reversing a word or capitalizing the last letter makes a password un-guessable. **2. Computer-generated passwords:** Passwords are quite random in nature. Computer-generated passwords also have problems. 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. In general, computer-generated password schemes have a history of poor acceptance by users. 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. 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:** A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user. 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. Furthermore, any existing passwords remain vulnerable until the reactive password checker finds them. **4. Proactive password checking:** The most promising approach to improved password security is a proactive password checker. In this scheme, a user is allowed to select his or her password. However, at the time of selection, the system checks to see if the password is allowable and if not, rejects it. 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. The trick with a proactive password checker is to strike a balance between user acceptability and strength. If the system rejects too many passwords, users will complain that it is too hard to select a password. 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.	
	(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. 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.	**(Listing of types of firewall: 1 mark, Explanation of packet filter as a firewall: 2 marks ,diagram of packet filter as a firewall: 1 mark)**

		Diagram of packet filter as a firewall.  **Packet Filtering**	
	(d)	**Describe host based IDS with its advantages and disadvantages.**	**4M**
	Ans:	**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.	**(Diagram: 1 mark, Explanation: 1 mark , any two advantages: 1 mark , any two disadvantages: 1 mark)**

		• **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. **Advantages:** 1. Operating System specific and detailed signatures. 2. Examine data after it has been decrypted. 3. Application specific. 4. Determine whether or not an alarm may impact that specific. **Disadvantages:** 1. Should have a process on every system to watch. 2. High cost of ownership and maintenance. 3. Uses local system resources. 4. If logged locally, could be compromised or disable.	
	(e)	**Explain the steps for hardening applications.**	**4M**
	Ans:	Application Hardening is a security feature designed to avoid/prevent exploitation of various types of vulnerabilities in software application. It also secures against local and internet attacks. Vulnerabilities are introduced by programmers who fail to check the properly the input data entering into the application. If there are vulnerabilities in application then it can be exploited by an attacker. Hardening application is fairly similar to hardening operating system- you remove the functions or components you do not need, restrict access where you can and make sure that the application is kept up to date with patches & maintain application patches. **Application hardening has following mechanisms:** **a) Process spawning Control:** uses fact that in most cases the application does not need the ability to launch other executable for proper functioning. By taking away the process spawning ability from the application, hackers will not be able to perform the process spawning attack. **b) EXE file protection:** another method to break into system is to trick the vulnerable application into modifying or creating executable file protection defense is based on in most of the cases, the application does not need to create or modify executable files. Hackers will not be able to perform attacks tampering with executable files on the system. **c) System tampering protection:** Another possibility to break into the system is to trick the vulnerable application into modifying special sensitive area of the operating system and taking advantage of those modifications. Those sensitive areas include Windows registry keys used to control launching of application on system startup the system.ini and win.ini files… The system tampering protection defense is based on the fact that in almost all cases normal applications do not need to perform such operations for their proper function, by preventing applications to modify special areas of Operating system. Hackers will not be able to attack by tampering with sensitive special areas of the system. Application Patches will be helpful in this case like Hotfixes, Patches, and upgrades.	**(Any relevant explanation : 4 marks)**

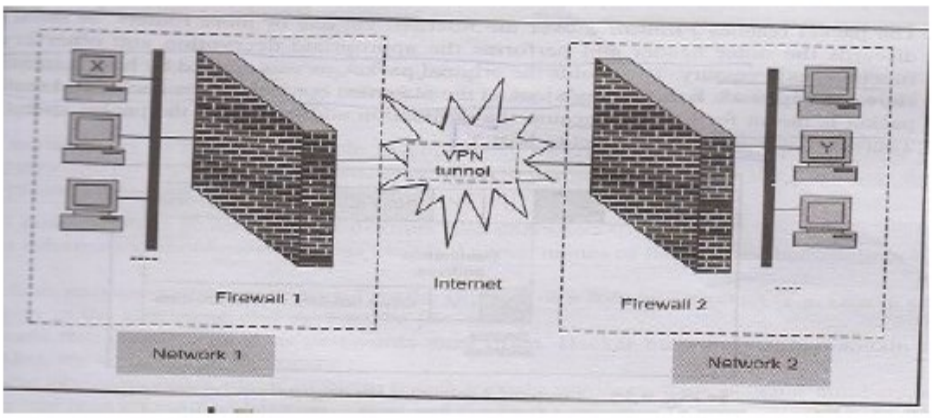
4.	**(a)**	**Attempt any THREE of the following:**	**12 Marks**
	(i)	**Explain simple columnar transposition technique with algorithm and example.**	**4M**
	Ans:	The columnar transposition cipher is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the cipher-text. It can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on its own. The cipher uses a columnar transposition to greatly improve its security. **Algorithm:** 1. The message is written out in rows of a fixed length. 2. Read out again column by column according to given order or in random order. 3. According to order write cipher text. **Example:** The key for the columnar transposition cipher is a keyword e.g. ORANGE. The row length that is used is the same as the length of the keyword. To encrypt a below plaintext COMPUTER PROGRAMMING	**(Explanation: 1 mark, Algorithm: 1 mark, Example: 2 marks)**

O	**R**	**A**	**N**	**G**	**E**
C	O	M	P	U	T
E	R	P	R	O	G
R	A	M	M	I	N
G	L	E	X	X	M

In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.

5	**6**	**1**	**4**	**3**	**2**
O	**R**	**A**	**N**	**G**	**E**
C	O	M	P	U	T
E	R	P	R	O	G
R	A	M	M	I	N
G	L	E	X	X	M

The Encrypted text or Cipher text is: MPMET GNMUO IXPRM XCERG ORAL (Written in blocks of Five)

	(ii)	**Draw and explain virtual private network.**	**4M**
	Ans:	 **Fig: VPN** **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)**
	(iii)	**Explain Cyber Crime.**	**4M**
	Ans:	Crimes against people are a category of crime that consists of offenses that usually involve causing or attempting to cause bodily harm or a threat of bodily harm. These actions are taken without the consent of the individual the crime is committed against, or the victim. These types of crimes do not have to result in actual harm - the fact that bodily harm could have resulted and that the victim is put in fear for their safety is sufficient. i.e. Assault, Domestic Violence, Stalking Cybercrime is a bigger risk now than ever before due to the sheer number of connected people and devices. Cybercrime, as it's a bigger risk now than ever before due to the sheer number of connected people and devices. It is simply a crime that has some kind of computer or cyber aspect to it. To go into more detail is not as straightforward, as it takes shape in a variety of different formats. **Cybercrime:** • Cybercrime has now surpassed illegal drug trafficking as a criminal money maker • Somebody‘s identity is stolen every 3 seconds as a result of cybercrime • Without a sophisticated security package, your unprotected PC can become infected within four minutes of connecting to the Internet.	**(Relevant Explanation of Cyber Crime: 4 marks)**

		Criminals committing cybercrime use a number of methods, depending on their skill-set and their goal. Here are some of the **different ways cybercrime can take shape:** Theft of personal data • Copyright infringement • Fraud • Child pornography • Cyber stalking • Bullying Cybercrime covers a wide range of different attacks, that all deserve their own unique approach when it comes to improving our computer's safety and protecting ourselves. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations. The broad range of cybercrime can be better understood by dividing it into two overall categories.	
	(iv)	**What is software piracy?**	**4M**
	Ans:	Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries. Software piracy causes significant lost revenue for publishers, which in turn results in higher prices for the consumer. Software piracy applies mainly to full-function commercial software. The time-limited or function-restricted versions of commercial software called shareware are less likely to be pirated since they are freely available. Similarly, freeware, a type of software that is copyrighted but freely distributed at no charge. **Types of software piracy include:** • **Soft-lifting:** Borrowing and installing a copy of a software application from a colleague. • **Client-server overuse:** Installing more copies of the software than you have licenses for. • **Hard-disk loading:** Installing and selling unauthorized copies of software on refurbished or new computers. • **Counterfeiting:** Duplicating and selling copyrighted programs. • **Online piracy:** Typically involves downloading illegal software from peer-to-peer network, Internet auction or blog. (In the past, the only place to download software was from a bulletin board system and these were limited to local areas because of long distance charges while online.)	**(Any Relevant Descriptio n: 4 marks)**
	(b)	**Attempt any ONE:**	**6 Marks**
	(i)	**Explain DOS and DDOS with neat diagram.**	**6M**
	Ans:	**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	**(Explanatio n of DOS & DDOS : 2 marks Each, Diagram: 1**

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.

mark Each)

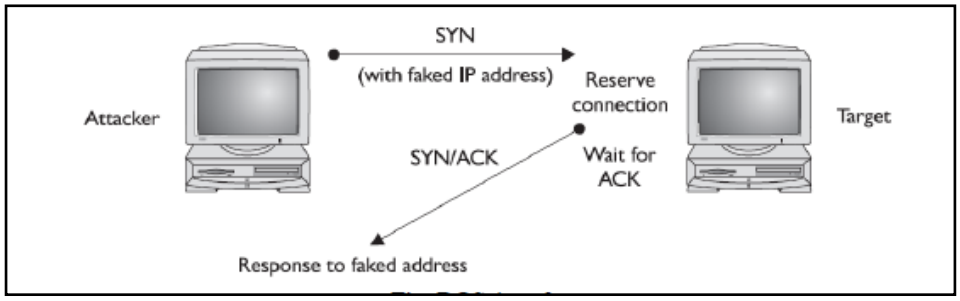


Fig: DOS Attack

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.

Distributed Denial-Of-Service (DDoS): DDoS is the attack where source is more than one, often thousands of, unique IP addresses. It is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations. DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

A Denial of Service (DoS) attack is different from a DDoS attack. The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource. The DDoS attack uses multiple computers and Internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via botnets.

Types of DDoS Attacks:

- **Traffic attacks:** Traffic flooding attacks send a huge volume of TCP, UDP and ICPM packets to the target. Legitimate requests get lost and these attacks may be accompanied by malware exploitation.
- **Bandwidth attacks**: This DDoS attack overloads the target with massive amounts of junk data. This results in a loss of network bandwidth and equipment resources and can lead to a complete denial of service.
- **Application attacks:** Application-layer data messages can deplete resources in the application layer, leaving the target's system services unavailable.

Stacheldraht is a piece of software written by Random for Linux and Solaris systems

which acts as a distributed denial of service (DDoS) agent. This tool detects and automatically enables source address forgery. Stacheldraht uses a number of different DoS attacks, including UDP flood, ICMP flood, TCP SYN flood and Smurf attack.

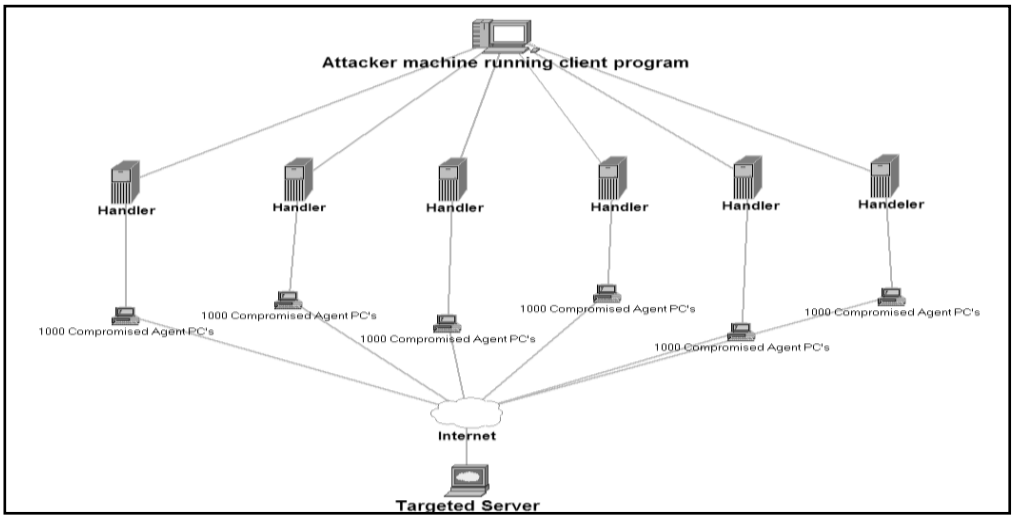


Fig: DDOS Attack

	(ii)	**Define virus. Explain at least 5 types of viruses.**	**6M**
	Ans:	**Viruses:** A program designated to spread from file to file on a single PC, it does not intentionally try to move to another PC and it must replicate and execute itself. Used as delivery tool for hacking. **Types of viruses:** • **Parasitic Viruses:** It attaches itself to executable code and replicates itself. Once it is infected it will find another program to infect. • **Memory resident viruses:** lives in memory after its execution it becomes a part of operating system or application and can manipulate any file that is executed, copied or moved. • **Non- resident viruses:** it executes itself and terminates or destroys after specific time. • **Boot sector Viruses:** It infects boot sector and spread through a system when it is booted from disk containing virus. • **Overwriting viruses:** It overwrites the code with its own code. • **Stealth Virus:** This virus hides the modification it has made in the file or boot record. • **Macro Viruses:** These are not executable. It affects Microsoft word like documents, they can spreads through email. • **Polymorphic viruses:** it produces fully operational copies of itself, in an attempt to avoid signature detection. • **Companion Viruses:** creates a program instead of modifying an existing file. • **Email Viruses:** Virus gets executed when email attachment is open by recipient. Virus sends itself to everyone on the mailing list of sender. • **Metamorphic viruses:** keeps rewriting itself every time, it may change their behavior as well as appearance code.	**(Definition: 1 mark, Five types of virus with explanation : 1 mark each)**

5.		**Attempt any TWO :**	**16 Marks**
	(a)	**Explain individual user responsibilities in Computer Security.**	**8M**
	Ans:	**Individual user responsibilities in computer security are:** 1. Lock the door of office or workspace. 2. Do not leave sensitive information inside your car unprotected. 3. Secure storage media in a secure storage device which contains sensitive information. 4. Shredding paper containing organizational information before discarding it. 5. Do not expose sensitive information to individuals that do not have an authorized need to know it. 6. Do not discuss sensitive information with family members. 7. Be alert to, and do not allow, piggybacking, shoulder surfing or access without the proper identifications. 8. Establish different procedures to implement good password security practice that employees should follow. **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	**(Each point: 1 mark, any 8 points)**
	(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. **<u>Types of security zone:</u>** **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.	**(Security Topology: 1 mark, security zone: 1 mark, Listing types of security zones: 2 Marks, Explanation of four zones: 1 mark each)**

		• 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.	
	(c)	**Explain need for firewall and explain one of the type of firewall with diagram.**	**8M**
	Ans:	Need for Firewall: 1. A firewall works as a barrier, or a shield, between your PC and cyber space. 2. When you are connected to the Internet, you are constantly sending and receiving information in small units called packets. 3. The firewall filters these packets to see if they meet certain criteria set by a series of rules, and thereafter blocks or allows the data. 4. This way, hackers cannot get inside and steal information such as bank account numbers and passwords from you. Capabilities: • All traffic from inside to outside and vice versa must pass through the firewall. • To achieve this all access to local network must first be physically blocked and access only via the firewall should be permitted. • As per local security policy traffic should be permitted.	**(Explanation of need: 4 marks, Any one firewall explanation : 4 marks)**

- The firewall itself must be strong enough so as to render attacks on it useless.

Types of Firewalls

a. Packet Filter Firewall
b. Circuit level Gateway Firewall
c. Application Gateway Firewall
d. Stateful multilayer Inspection Firewall
e. Software
f. Hardware
g. Hybrid

1. Packet Filter Firewall: A packet filtering router firewall applies a set of rules to each packet and based on outcome, decides to either forward or discard the packet. Such a firewall implementation involves a router, which is configured to filter packets going in either direction i.e. from the local network to the outside world and vice versa. Packet filter performs the following functions.

   a. Receive each packet as it arrives.

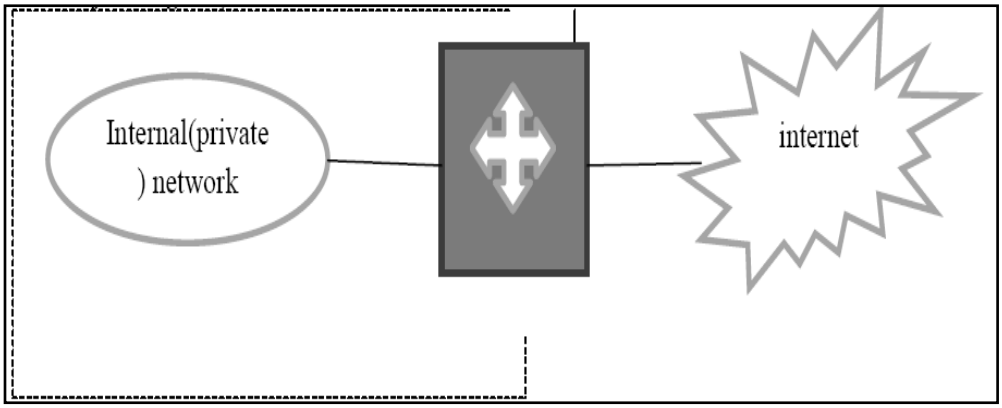
   b. Pass the packet through a set of rules, based on the contents of the IP and transport header fields of the packet. If there is a match with one of the set rule, decides whether to accept or discard the packet based on that rule.

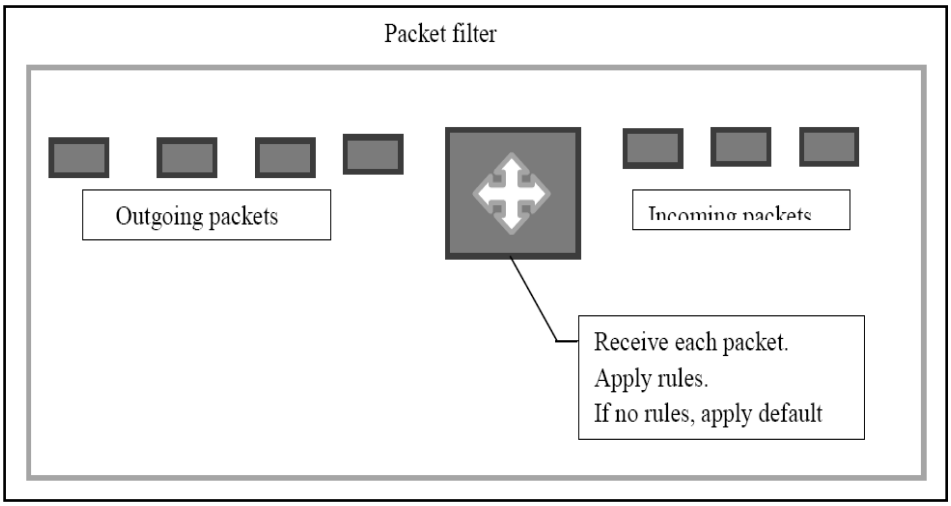
   c. If there is no match with any rule, take the default action. It can be discard all packets or accept all packets.

Advantages: simplicity, transparency to the users, high speed

Disadvantages: difficult to set up packet filtering rules, lack of authentication.

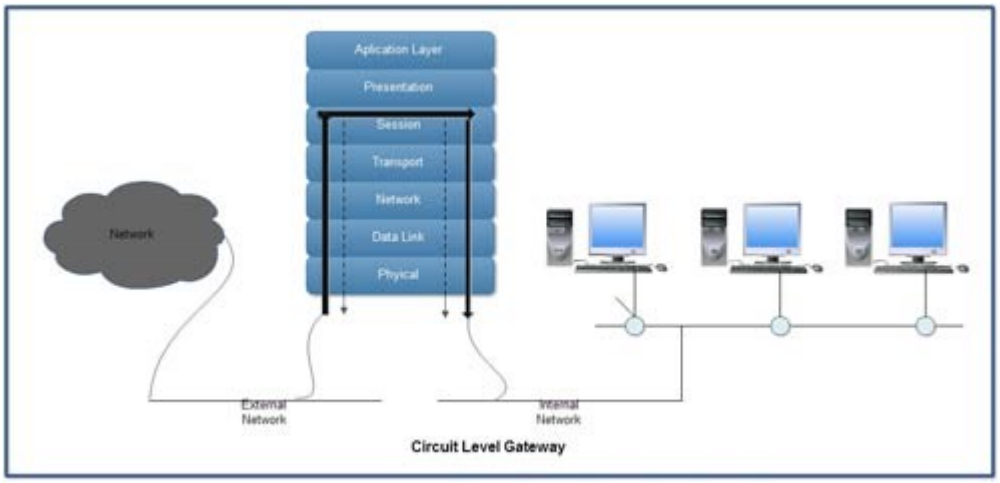
Packet Filtering Firewall





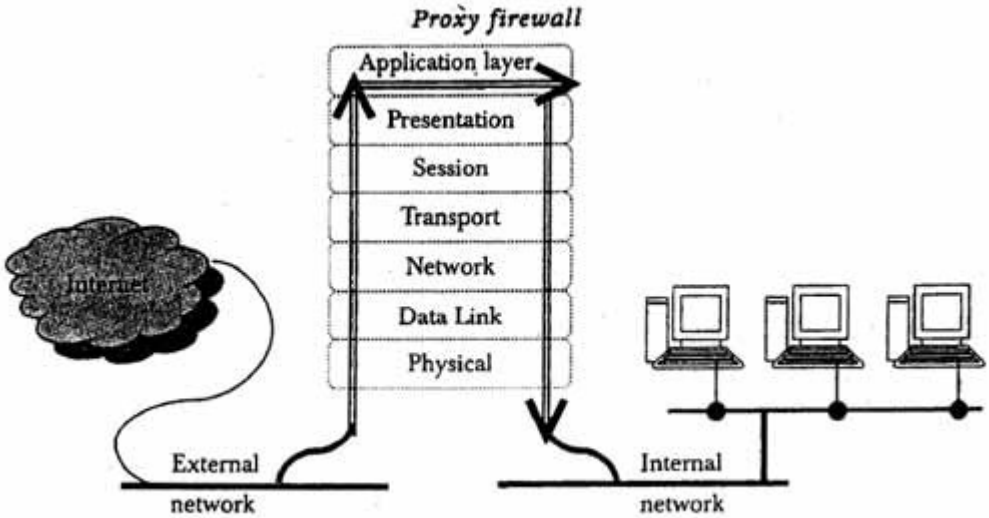
2. Circuit level gateway Firewalls:

The circuit level gateway firewalls work at the session layer of the OSI model. They monitor TCP handshaking between the packets to determine if a requested session is legitimate. And the information passed through a circuit level gateway, to the internet, appears to have come from the circuit level gateway. So, there is no way for a remote computer or a host to determine the internal private ip addresses of an organization, for example. This technique is also called Network Address Translation where the private IP addresses originating from the different clients inside the network are all mapped to the public IP address available through the internet service provider and then sent to the outside world (Internet). This way, the packets are tagged with only the Public IP address (Firewall level) and the internal private IP addresses are not exposed to potential intruders.



3. Application level gateway Firewalls:

Application level firewalls decide whether to drop a packet or send them through based on

		the application information (available in the packet). They do this by setting up various proxies on a single firewall for different applications. Both the client and the server connect to these proxies instead of connecting directly to each other. So, any suspicious data or connections are dropped by these proxies. Application level firewalls ensure protocol conformance. For example, attacks over http that violates the protocol policies like sending Non-ASCII data in the header fields or overly long string along with Non-ASCII characters in the host field would be dropped because they have been tampered with, by the intruders.  *Application level gateway firewall*	
6.		**Attempt any FOUR:**	**16 Marks**
	(a)	**Describe dumpster diving with its prevention mechanism.**	**4M**
	Ans:	**Dumpster diving:** 1. It is the process of going through a target's trash in order to find little bits of information System attackers need certain amount of information before launching their attack. 2. 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. 3. The process of going through target's thrash is known as "dumpster diving". 4. 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. 5. If the attacker is lucky, the target has poor security process they may succeed in finding user ID"s and passwords. 6. If the password is changed and old password is discarded, lucky dumpster driver may get valuable clue. **Prevention Mechanism:** To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company should establish disposal policy.	**(Concept 3 marks, Prevention mechanism 1 mark)**

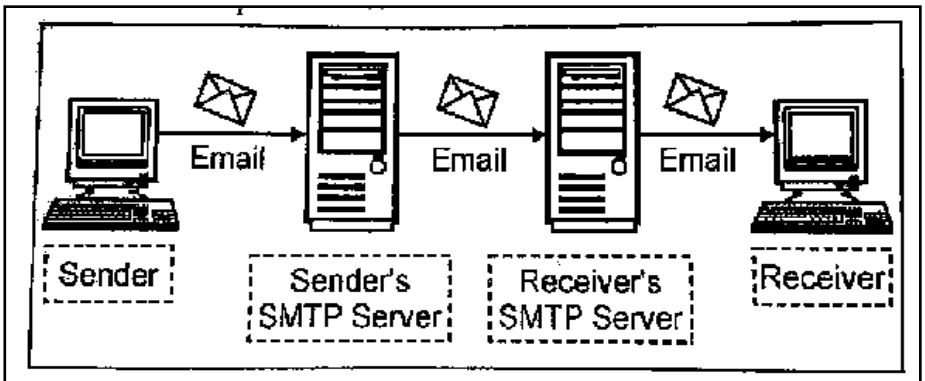
	(b)	**Explain the term stenography with example.**	**4M**
	Ans:	**{{**Note: Considering question as Steganography instead of Stenography**}}** **Steganography:** • Steganography is the art and science of writing hidden message in such a way that no one, apart from the sender and intended recipient, suspects 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. i.e. One can hide text, data, image, sound, and video, behind image.	**(Term:1 mark, Concept: 3 marks)**
	(c)	**Explain e-mail security techniques (protocols).**	**4M**

Ans:

(Listing: 1 mark: any two protocols: 1.5 marks)

A. <u>SMTP- Simple Mail Transfer Protocol.</u>

1. It is a popular network services in Email communication.
2. It is system for sending messages to other computer users based on email.
3. It is request response based activity.
4. It also provides email exchange process.
5. It attempts to provide reliable service but not guarantees to sure recovery from failure.



Working of SMTP protocols

B. <u>PEM- Privacy Enhanced Mail.</u>

1. Privacy-Enhanced Mail (PEM) is an Internet standard that provides for secure exchange of electronic mail.

2. PEM employs a range of cryptographic techniques to allow for

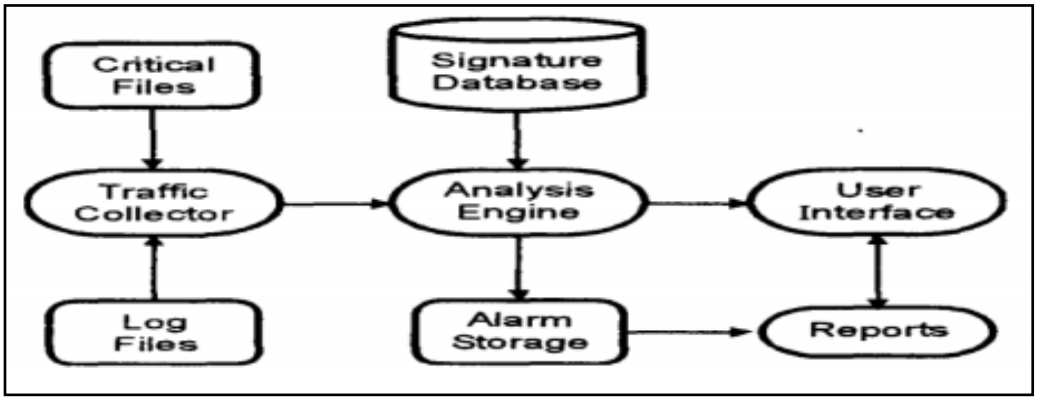
- Confidentiality
- Non - repudiation
- Message integrity
- The confidentiality feature allows a message to be kept secret from people to whom the message was not addressed.
- The Non - repudiation allows a user to verify that the PEM message that they have received is truly from the person who claims to have sent it.
- The message integrity aspects allow the user to ensure that a message hasn't been modified during transport from the sender.

C. <u>PGP- Pretty Good Privacy</u>

- Pretty Good Privacy is a popular program used to encrypt and decrypt email over the internet.
- It becomes a standard for e-mail security.
- 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.

		• PGP can be used to encrypt files being stored so that they are in unreadable form and not readable by users or intruders. • It is available in Low cost and Freeware version. • It is most widely used privacy ensuring program used by individuals as well as many corporations. **D. <u>S/MIME – Secure Multipurpose Internet Mail Extension</u>** • 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. • 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. • And when basic MIME system is enhanced to provide security features, it is called as Secure Multipurpose Internet Mail Extensions. • S/MIME provides security for digital signature and encryption of email message.	
	(d)	**What is intrusion detection system? Explain host based IDS.**	**4M**
	Ans:	**<u>Intrusion detection system (IDS):</u>** 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 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	**(IDS:1mark, Explanation of HIDS: 2 marks, Diagram: 1 mark)**

- 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:

- **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.

	(e)	**What is TLS? What are two layers of TLS?**	**4M**

	Ans:	The Transport Layer security (TLS) protocol provides communications privacy over internet. The protocol allows client-server applications to communicate in a way that is designed to prevent eavesdropping, tampering or message forgery. The primary goal of the TLS protocol is to provide privacy in data integrity between two communicating applications. The protocol is composed of two layers: **1. TLS Record** Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption. The **2. TLS Handshake** Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.	**(Explanation : 2 marks, Layers: 1 mark each)**