Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in themodel answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may tryto 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 thefigure. 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 constantvalues may vary and there may be some difference in the candidate's answers and modelanswer.
6) In case of some questions credit may be given by judgment on part of examiner of relevantanswer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

Q.1) A) Attempt any three: **12M**

i) State the need for computer security.
(1M for each point, any four points)

Ans.

1. For prevention of data theft such as bank account numbers, credit card information, passwords, work related documents or sheets, etc.
2. To make data remain safe and confidential.
3. To provide confidentiality which ensures that only those individuals should ever be able to view data they are not entitled to.
4. To provide integrity which ensures that only authorized individuals should ever be able change or modify information.
5. To provide availability which ensure that the data or system itself is available for use when authorized user wants it.
6. To provide authentication which deals with the desire to ensure that an authorized individual.
7. To provide non-repudiation which deals with the ability to verify that message has been sent and received by an authorized user.

ii) Describe role based access control.
(Relevant explanation - 4M)

Ans.

Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. 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.

RBAC enables users to carry out a wide range of authorized tasks by dynamically regulating their actions according to flexible functions, relationships & constraints. In RBAC roles can be easily changed as per need of the enterprise, without having to individually update the privileges for every user.

In RBAC there are three rules:

1. A person must be assigned a certain role in order to conduct a certain action, called a transaction.
2. A user needs a role authorization to be allowed to hold that role.
3. Transaction authorization allows the user to perform certain transactions. The transaction has to be allowed to occur through the role membership. Users won't be able to perform transaction other than the ones they are authorized for.

iii) Define the following term:

A) Cryptograph **B) Cryptology**

C) Cryptanalysis **D) Cipher text**

(Each term 1M)

Ans.

A. Cryptography: Cryptography is art & science of achieving security by encoding messages to make them non-readable.

B. Cryptology: Cryptology is a combination of cryptography and cryptanalysis.

C. 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.

D. Cipher Text: When plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

iv) Define virus and logic bomb.

(Each definition- 2M)

Ans.

Virus: Virus is a program which attaches itself to another program and causes damage to the computer system or the network. It is loaded onto your computer without your knowledge and runs against your wishes.

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

Q.1) B) Attempt any one: **6M**

i) Describe the following attacks:
A) Sniffing **B) Spooting**
(Sniffing-3M, Spoofing- 3M)

Ans.

A) Sniffing: This is software or hardware that is used to observe traffic as it passes through a network on shared broadcast media. It can be used to view all traffic or target specific protocol, service, or string of characters like logins. Some network sniffers are not just designed to observe the all traffic but also modify the traffic. Network administrators use sniffers for monitoring traffic. They can also use for network bandwidth analysis and to troubleshoot certain problems such as duplicate MAC addresses.

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

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

ii) Describe data recovery procedure.
(Relevant explanation- 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 tools available.Every tool will have different GUI & method of recovery.

There are standard ethical procedures that need be followed as described in following steps:

1. Incident identification: - Identifying the incident and the analysis of the case.
2. Preparation of tools, monitoring, techniques, management support and authorization etc.
3. Decide a clear and well defined approach, strategy to proceed with the case.
4. Collection of the evidence & even duplicating the digital evidence is also an important part of ethical conduct.
5. The evidence that is collected should be incorporated with the date, time & the place where it was found. The importance of preservation of the evidence need be prevented.
6. The analysis of the evidence should be carried out in such a way so as to eliminate the evidence that cannot be produced in the court law.

7. This step in an ethical behaviour includes the presentation of the evidence in the court of law.
8. The return of evidence to the owner also forms a part in ethical behaviour.

Q.2) Attempt any two: **16M**

a) Describe CIA model for computer security with example.
(CIA- 2M, Explanation of each concept with example- 2M (Three Points))

Ans.CIA Model for security: Confidentiality, Integrity and Authentication i.e. these three concepts are considered as backbone of security. These concepts represent the fundamental principles of security.

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

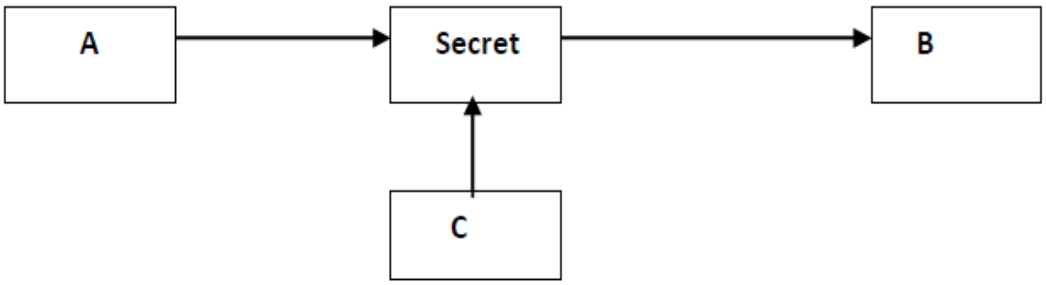


Fig. Loss of confidentiality

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

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

This type of attack is called as **Fabrication.**

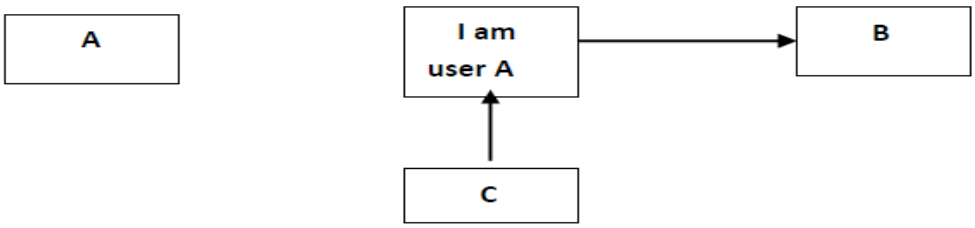


Fig. Absence of authentication

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

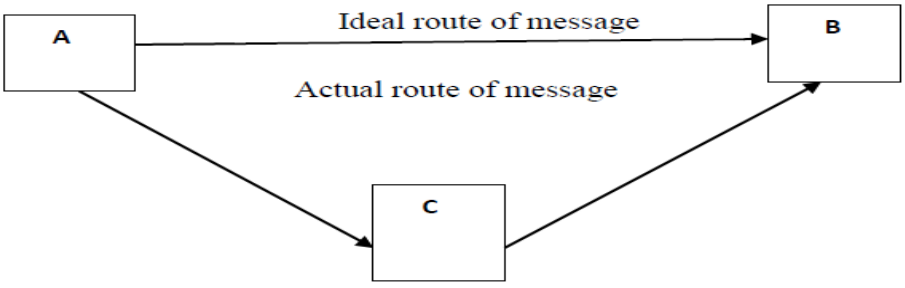


Fig. Loss of Integrity

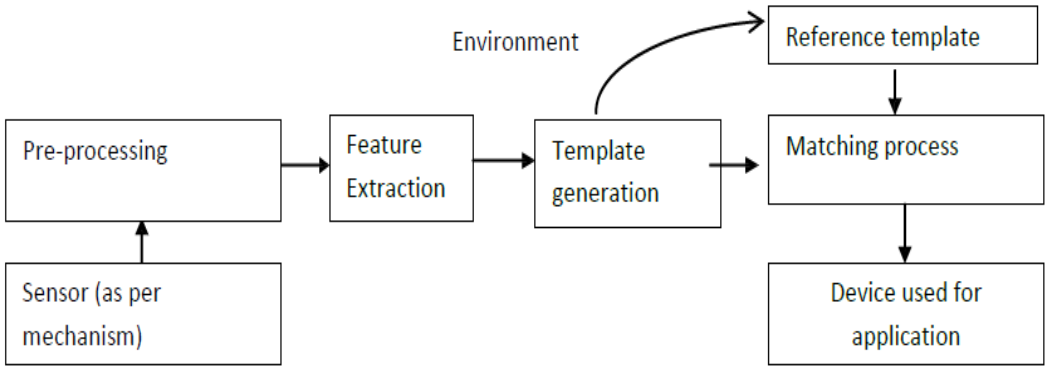
b) What is the importance of biometrics in computer security? Describe finger prints registration and verification process.
(Importance- 4M, Registration &Verification process- 4M)

Ans.

Importance:

1. Biometric refers study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral characteristics.
2. 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 technique, voice synthesis and recognition and so on.
3. Biometrics cannot be lost, stolen or forgotten. Barring disease or serious physical injury, the biometric is consistent and permanent.
4. It is also secure in that the biometric itself cannot be socially engineered, shared or used by others.

5. There is no requirement to remember password or pins, thus eliminating an overhead cost.
6. Coupled with a smart card, biometrics provides strong security for any credentials on the smart card.
7. It provides a high degree of confidence in user identity.



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.

1) The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data.
2) The 2nd block performs all the necessary pre-processing.
3) The third block extracts necessary features. This step is an important step as the correct features need to be extracted in the optimal way.
4) If enrolment is being performed the template is simply stored somewhere (on a card or within a database or both).if a matching phase is being performed the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm. The matching program will analyze the template with the input. This will then be output for any specified use or purpose.

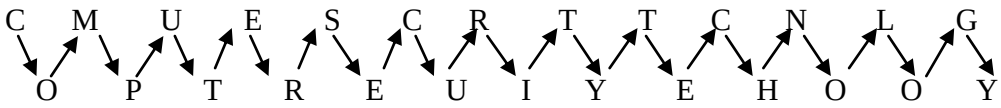
c) Explain rail fence technique with algorithm. Encrypt "Computer Security Technology" using rail fence technique.
(Algorithm- 4M, encryption - 4M)

Ans.

In Rail fence cipher, techniques are essentially Transposition Ciphers and generated by rearrangement of characters in the plaintext. The characters of the plain text string are arranged in the form of a rail-fence as follows.
Given Plaintextis — COMPUTER SECURITY TECHNOLOGY
Rail Fence Technique algorithm:

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

Example: plain text = ―COMPUTER SECURITY TECHNOLOGY―is converted to cipher text with this help of Rail Fence Technique with dual slope.



Ciphertext: CMUESCRTTCNLGOPTREUIYEHOOY

Q.3) Attempt any four: **16M**

a) Explain VPN with Neat diagram. Enlist different VPN protocols.
(Diagram: 1M, Explanation: 2M, Listing Protocols: 1M (any 2))

Ans:

A VPN or Virtual Private Network is a network connection that enables you to create a secure connection over the public Internet to private networks at a remote location. With a VPN, all network traffic (data, voice, and video) goes through a secure virtual tunnel between the host device (client) and the VPN provider's servers, and is encrypted. VPN technology uses a combination of features such as encryption, tunneling protocols, data encapsulation, and certified connections to provide you with a secure connection to private networks and to protect your identity.

VPN connections technically give you all the benefits of a Local Area Network (LAN), which is similar to that found in many offices but without requiring a hard-wired connection.These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

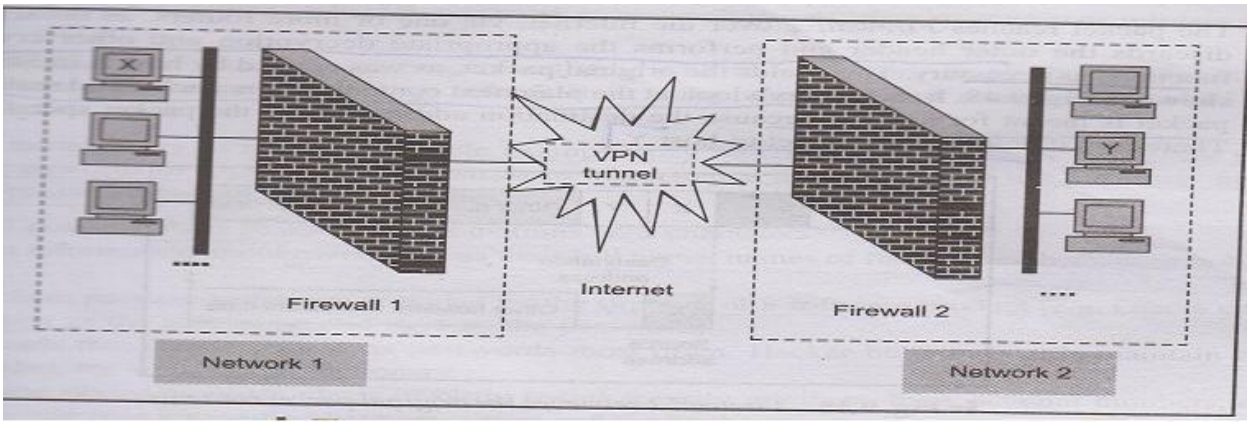


Figure: VPN

Different VPN protocols are:

1. **PPTP** (Point-to-Point Tunneling Protocol)
2. **L2TP** (Layer 2 Tunneling Protocol)
3. **IPsec (**Internet Protocol Security)
4. **SSL** (Secure Socket Layer)

b) Describe different Password Selection criteria
(Any 4 Criteria: 1M each)

Ans. There are four basic techniques passwords selection strategies:

a) User education: Tell the importance of hard-to-guess passwords to the users and provide guidelines for selecting strong password.

b) Computer generated password: Computer generated passwords are random in nature so difficult for user to remember it and may note down somewhere.

c) Reactive password checking: the system periodically runs its own password cracker program to find out guessable passwords. If the system finds any such password, the system cancels it and notifies the user.

d) Proactive password checking: It is a most promising approach to improve password security. In this scheme, a user is allowed to select his own password, if password is allowable then allow or reject it.

c) Distinguish between Symmetric and asymmetric key cryptography (four points).
(Any 4 differences: 1M each)

Ans.

Symmetric-key Cryptography	Asymmetric-key Cryptography
It only needs one key to encrypt the message. And both users only need the same key to decode the message	It needs two different keys- public key and private key. Everyone can see the public key and only the person who has private key can decode the message.
The symmetric-key system only needs one key, in order to crack the message.	Asymmetric-key is like double encryption. First, the user use his private key to encrypt the message, them he/she public the message with public key; although everyone can see the message, only the person with his own private key can decode the message. So, in order to crack the system, you need the person's private key, or need to know how they created the private key
Symmetric-key confirms sender's identity by knowing who can encrypt the message or decode the message; in other words, by	Asymmetric-key confirms the sender's identity by double the encryption. One person encrypts the message with his private key, and sends that with

knowing who has the key	public key. And only the person with another private key can decode the message.
Advantages: Safer (lots of probability), and faster.	Advantages: Allow letting other people read the encrypted message without any risk. No problem for distributing the key.
Disadvantages: One time transactions, how to give the key to the other person. And once other people know the key, you have to change the key at both sides.	Disadvantages: Big and slow
Example: DES	Example: Diffie-Hellman Algorithm

d) Describe Host based IDS with its advantages and disadvantages.

(Diagram: 1M, Explanation: 1M, any twoadvantages: 1M, any two disadvantages: 1M)

Ans.

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

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

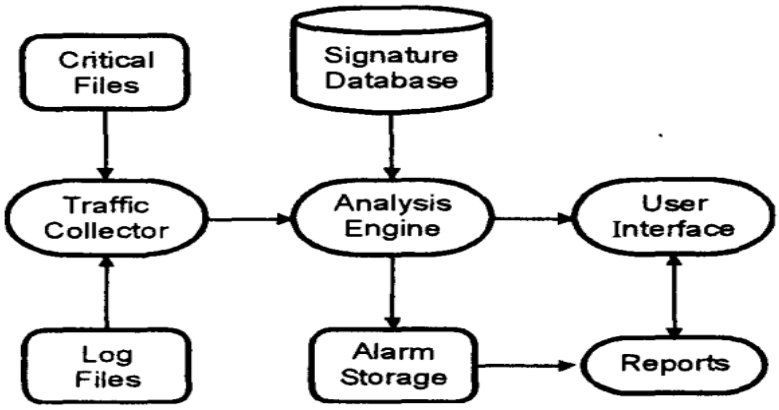


Figure: HIDS

Basic Components HIDS:

1. Traffic collector: This component collects activity or events from the IDS to examine. In Host-based IDS, this can be log files, audit logs, or traffic coming to or leaving a specific system.

2. Analysis Engine: This component examines the collected network traffic & compares it to known patterns of suspicious or malicious activity stored in the signature database. The analysis engine acts like a brain of IDS.

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

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

Advantages:

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) Describe SET with its requirements and participants.
(SET description: 1M, Requirements: 1M, Participants: 2M(any 4))

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.

There are four essential security requirements for **Secure electronic Transaction**

1. Authentication
2. Encryption
3. Integrity
4. Non-repudiation

Participants/Components of SET

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.

Q.4) a) Attempt any three: 12M

i) Explain simple columnar transposition technique with algorithm and example. ***(Algorithm-2M, Example: 2M)***

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 cipheruses 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

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

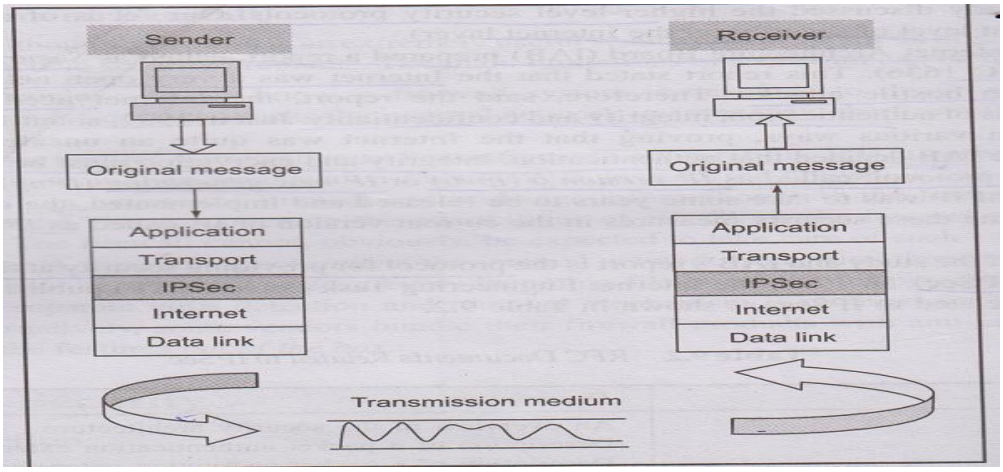
The Encrypted text or Cipher text is:

MPMET GNMUO IXPRM XCERG ORAL (Written in blocks of Five)

ii) Describe IP security architecture.
(Diagram: 2M, Explanation: 2M)

Ans:

IPsec architecture: IPsec is to encrypt and seal the transport and application layer data during transmission. Also offers integrity protection for the Internet layer. IPSec layer sits in between the transport and the Internet layers of conventional TCP/IP protocol stack.



IPSec actually consists of two main protocols
a) Authentication Header (AH):
b) Encapsulating Security Payload (ESP):

a) Authentication Header (AH): The AH provides support for data integrity and authentication of IP packets. The data integrity service ensures that data inside IP packet is not altered during the transit. The authentication service enables an end user or computer system to authenticate the user or the application at the other end and decides to accept or reject packets accordingly. This also prevents IP spoofing attacks. AH is based on MAC protocol, which means that the two communicating parties must share a secret key in order to use AH.

b) Encapsulating Security Payload (ESP): ESP is a member of the IPsec protocol suite. In IPsec it provides origin authenticity, integrity and confidentiality protection of packets. ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure.

Modes of operation: Both AH and ESP works in two modes:

1. Tunnel mode: In tunnel mode, IPsec protects the entire IP datagram. It takes an IP datagram, adds the IPSec header and trailer and encrypts the whole thing. It then adds new IP header to this encrypted datagram.

2. Transport mode: Transport mode does not hide the actual source and destination addresses. They are visible in plain text, while in transit. In the transport mode, IPSec takes the transport layer payload, adds IPSec header and trailer, encrypts the whole thing and then adds the IP header. Thus IP header is not encrypted.

iii) Define cyber crime. List different types of cyber crimes.
(Define: 2M, Types: 2M (any 4))

Ans.

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Cybercrime may also be referred to as computer crime.
Types of Cybercrimes are

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

iv) What is Software piracy?
(Any Relevant Description: 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.)

Q.4) b) Attempt any one: **6M**

i) Explain DOS and DDOS with neat diagram.
(Explanation: 2M Each, Diagram: 1M Each)

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 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.

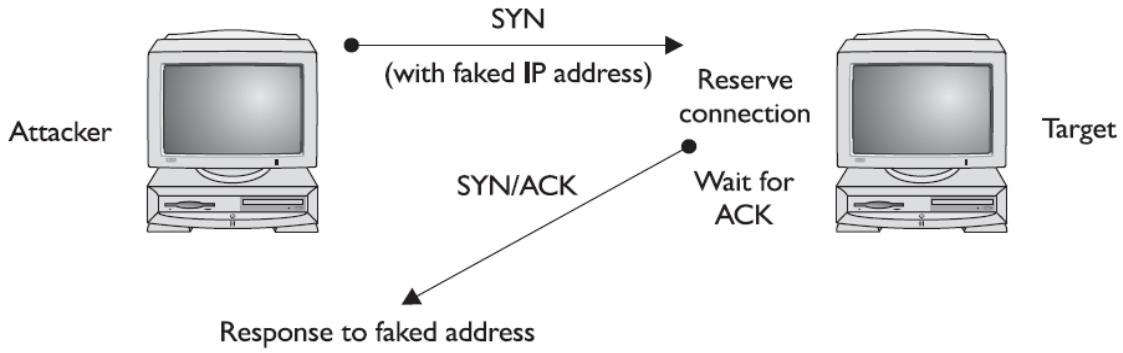


Fig: DOS Attack

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 Solarissystems 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 andSmurf attack.

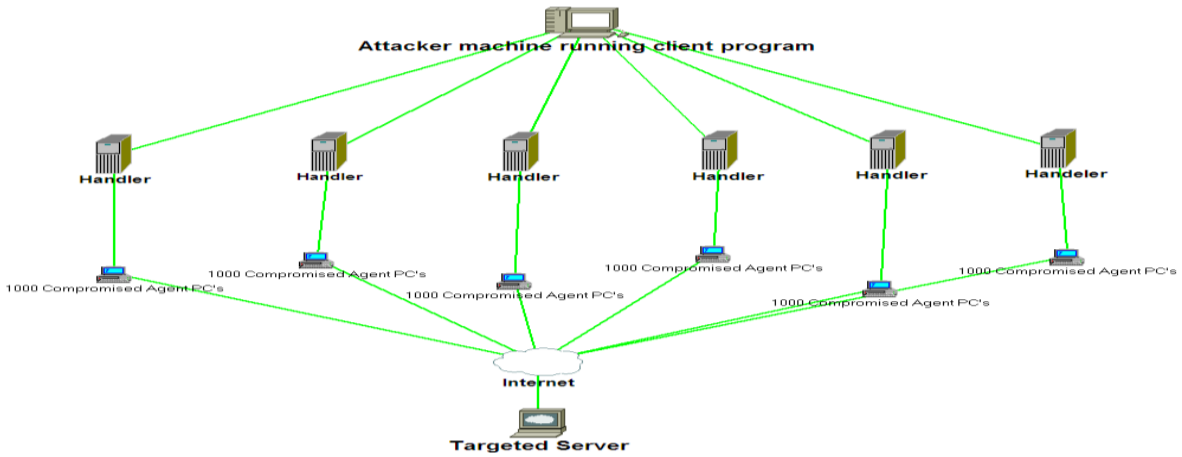


Fig: DDOS Attack

ii) Explain worm and virus. Differentiate between worm and virus.
(Explanation of Worm & Virus: 2M Each, Any 2 Differences: 2M)

Ans.

Worm: A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm

replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line.

Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. In recent worm attacks such as the much-talked-about Blaster Worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

Virus:A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to anexecutable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program.
It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. Because a virus is spread by human action people will unknowingly continue the spread of a computer virus by sharing infecting files or sending emails with viruses as attachments in the email.

Virus	Worm
The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.
It inserts itself into a file or executable program.	It exploits a weakness in an application or operating system by replicating itself.
It has to rely on users transferring infected files/programs to other computer systems.	It can use a network to replicate itself to other computer systems without user intervention.
Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	Usually not. Worms usually only monopolize the CPU and memory.
Virus is slower than worm.	Worm is faster than virus
E.g. Macro virus, Directory virus, Stealth Virus	E.g. Code red

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

a) Explain individual user responsibilities in computer security.
(Eachpoint 1M, any 8 points)

Ans. Individual user responsibilities in computer security are:

a) Lock the door of office or workspace.
b) Do not leave sensitive information inside your car unprotected.
c) Secure storage media in a secure storage device which contains sensitive information.
d) Shredding paper containing organizational information before discarding it.

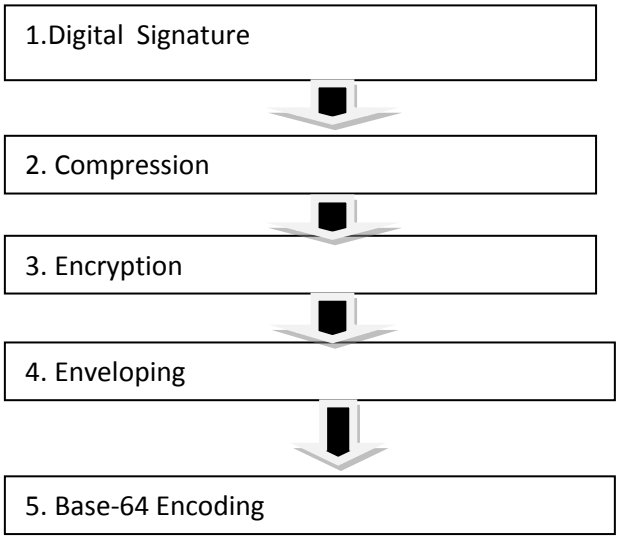
e) Do not expose sensitive information to individuals that do not have an authorized need to know it.
f) Do not discuss sensitive information with family members.
g) Be alert to, and do not allow, piggybacking, shoulder surfing or access without the proper identifications.
h) Establish different procedures to implement good password security practice that employees should follow.

b) What is PGP? How PGP is used for email security?
(Explanation of PGP2M, Diagram 2M, Working 4M)

Ans.

PGP is Pretty Good Privacy. It 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.

How PGP works



There are five steps as shown in fig.

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

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

c) Explain characteristics, working, design principle and limitation of firewall.
(Characteristics 1M, Diagram 1M, working 2M, design principle 2M and Limitation of firewall 2M)

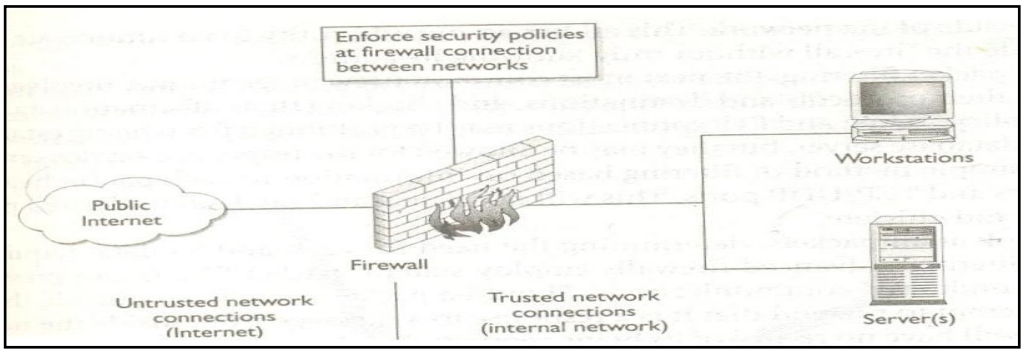
Ans.

Characteristics:

1. All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
2. Only authorized traffic (defined by the local security police) will be allowed to pass
3. The firewall itself is immune to penetration (use of trusted system with a secure operating system)

Design Principal:

A **firewall** is a networking device – hardware, software or a combination of both– whose purpose is to enforce a security policy across its connection. It is much like a wall that has a window: the wall serves to keep things out, except those permitted through the window.



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

- Packet filtering router
- Circuit level gateways
- Application Gateways/ Proxy Server.
- Network Address Translation (NAT)

One of the most basic security function provided by a firewall is Network Address Translation (NAT). This service allows you to mask significant amounts of information from outside of the network. This allows an outside entity to communicate with an entity inside the firewall without truly knowing its address.

Basic Packet Filtering, the most common firewall technique, looking at packets, their protocols and destinations and checking that information against the security policy.

Telnet and FTP connections may be prohibited from being established to a mail or database server, but they may be allowed for the respective service servers.

This is a fairly simple method of filtering based on information in each packet header, like IP addresses and TCP/UDP ports. This will not detect and catch all undesired packet but it is fast and efficient.

A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing traffic of network by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a brigade between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

Limitations:

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

Q.6) Attempt any four: **16M**

a) Describe dumpster diving with its prevention mechanism.
(Concept 3M, Prevention mechanism 1M)

Ans.

Dumpster diving: 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. One common place to find this information, if the attacker is in the vicinity of target is to go through the target's thrash in order to find little bits of information that could be useful. The process of going through target's thrash is known as "**dumpster diving**".

The search is carried out in waste paper, electronic waste such as old HDD, floppy and CD media recycle and trash bins on the systems etc.
If the attacker is lucky, the target has poor security process they may succeed in finding user ID's and passwords. If the password is changed and old password is discarded, lucky dumpster driver may get valuable clue.

To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company should establish disposal policy.

b) Explain the term steganography with example.
(Term – 1M, Concept- 2M, Example 1M)

Ans..

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.

c) Describe the concept of Kerberos.
(Explanation with Diagrams of different steps 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.

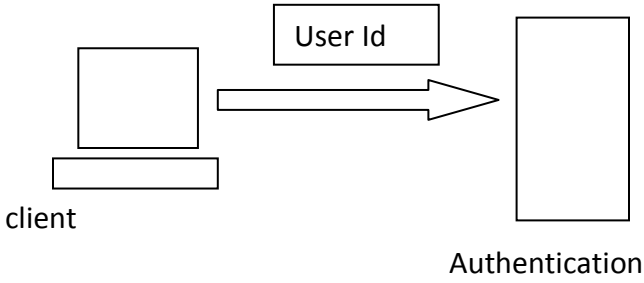
How Kerberos does works?

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.

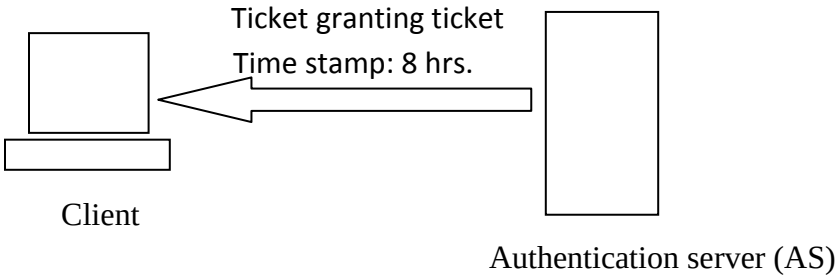
When working with the encryption key, the details are actually sent to a key distribution center (KDC), instead of sending the details directly between each computer.

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.

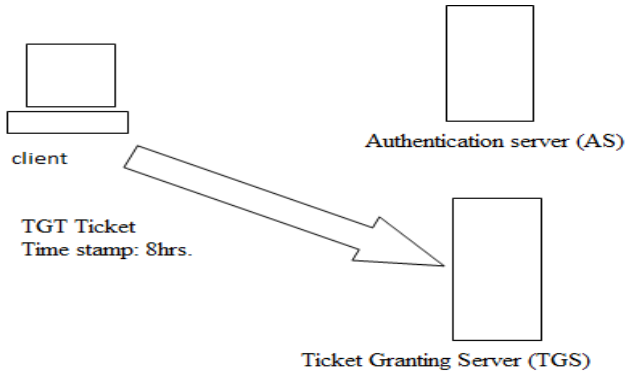


2. Upon verification, a timestamp is crated. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours. The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless. (This is used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

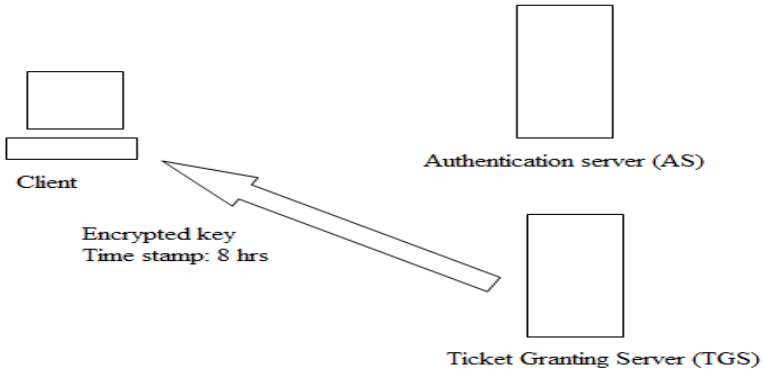


3. The key is sent back to the client in the form of a ticket-granting ticket, or TGT. This is a simple ticket that is issued by the authentication service. It is used for authentication the client for future reference.

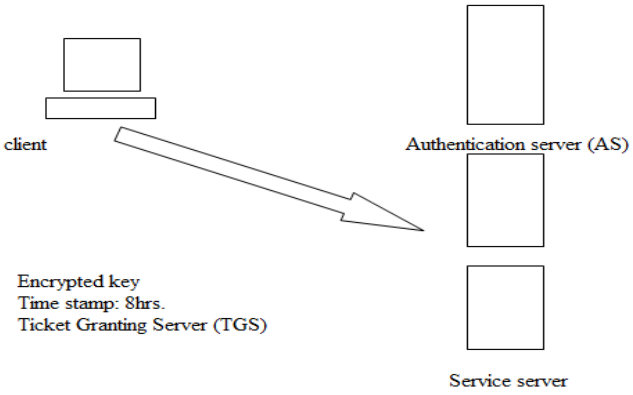
4. The client submits the ticket-granting ticket to the ticket-granting server, or TGS, to get authenticated.



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

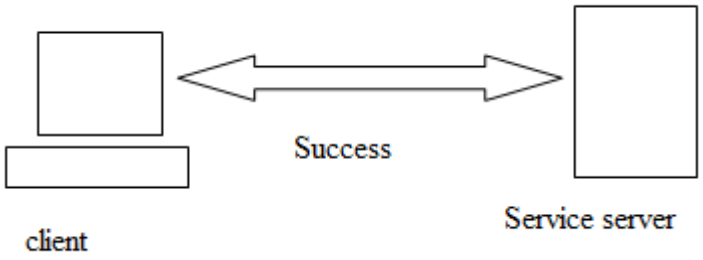


6. The client decrypts the ticket, tells the TGS it has done so, and then sends its own encrypted key to the service.



.

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.

d) Describe IT Act 2008

(Any four features of IT Act 2008- 2M, any four amendments-2M)

Ans.

It is introduced with many additional features of IT Act 2000:

They have amplified the existing provisions or introduced new provisions**.**

- 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.

Features of I.T. Amendment Act 2008:

- 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.

e) What is TLS? What are two layers of TLS?
(Explanation-2M, Layers-2M)

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:

- **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

- **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.