Winter – 14 EXAMINATION

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.1.

a) Attempt any Three of the following:

i. Describe the need for computer security.

(1 Mark – for this statement)

(1 Marks each for explanation of following points, example optional)

The need of computer security has been threefold: confidentiality, integrity, and availability—the "CIA" 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.

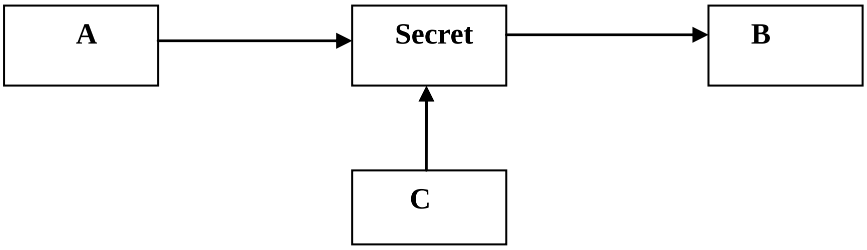


Fig. Loss of confidentiality

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.**

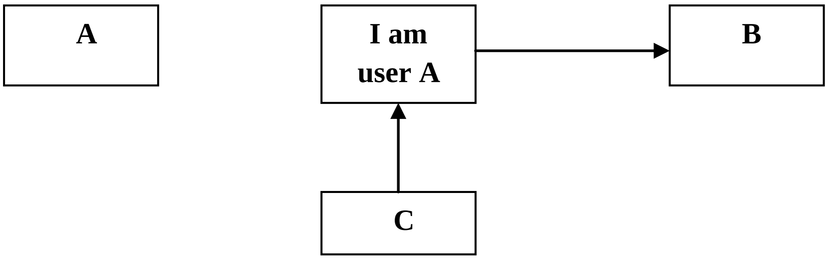


Fig. absence of authentication

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**.

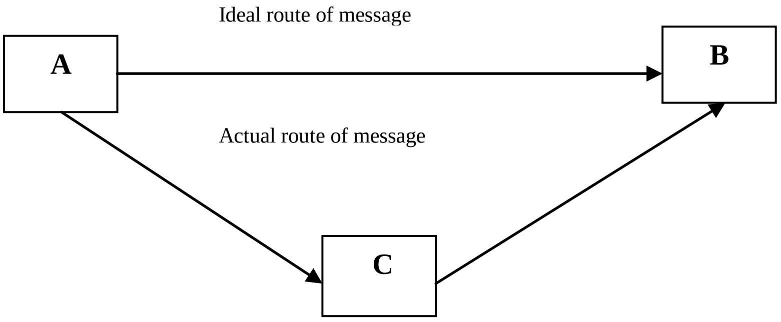


Fig. Loss of Integrity

ii. Explain any four the password selection strategies.(***4 marks for 4 points*****)**

The major security problems are because of user is not following established security policies.

- User always chooses a password that is easy to remember but easier passwords are easy to crack by attacker but when user choose difficult passwords that again it is difficult to remember.
- To make the job of attacker difficult organization encourage their users to use mixture of upper case & lower character & also include numbers & special symbols in their passwords. This may make the guessing of password difficult.

Organization also includes additional policies & rules related to password selection.

- In the organization, user may frequently change their passwords.
- Password should not written down on paper & do not kept in purse or wallet because if attacker get physical access then they will find a password of user somewhere in drover or desk ,inside of desk calendar.

- Many users have many accounts & password to remember. Selecting different password for each account, following the guidelines mentioned above for character selection & frequency of changes, aggravates the problem of remembering the passwords. This results that the users frequently use the same password for all accounts. If user does this, then one of account is broken, all other accounts are subsequently under threat. Good password selection & protection is applied to electronic world also.

OR

There are four basic techniques to reduce guessable passwords:

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.

iii. Define the following terms: (*each 1Mark*)

1. Cryptography
2. Crypt analysis
3. Plain text
4. Cipher text.

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. **Plain text**: Plain text or clear text significance that can be understood by sender, the recipient & also by anyone else who gets an access to that message.

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

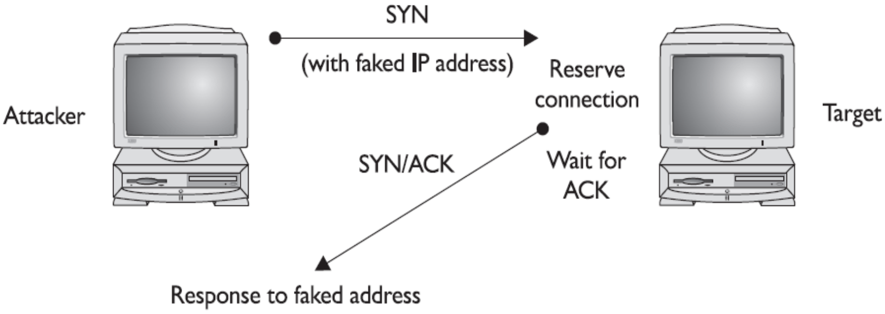
iv. Describe SYN flooding attack with diagram. (*1 marks for diagram, 3 marks for explanation)*

Denial of service (DOS) attacks can exploit a known vulnerability in a specific application or operating system, or they may attack features (or weaknesses) in specific protocols or services. In this form of attack, the attacker is attempting to deny authorized users access either to specific information or to the computer system or network itself.

The purpose of such an attack can be simply to prevent access to the target system, or the attack can be used in conjunction with other actions in order to gain unauthorized access to a computer or network.

SYN flooding is an example of a DOS attack that takes advantage of the way TCP/IP networks were designed to function, and it can be used to illustrate the basic principles of any DOS

attack.SYN flooding utilizes the TCP three-way handshake that is used to establish a connection between two systems.
In a **SYN flooding attack**, the attacker sends fake communication requests to the targeted system. Each of these requests will be answered by the target system, which then waits for the third part of the handshake. Since the requests are fake the target will wait for responses that will never come, as shown in Figure .



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

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

b) Attempt any one of the following:

i. Define the term virus and describe the different phases of virus.

(2 –marks for term virus & 1-mark for each phase)

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.
During the lifecycle of virus it goes through the following four phases:
1. **Dormant phase:** The virus is idle and activated by some event.
2. **Propagation phase:** It places an identical copy of itself into other programs or into certain system areas on the disk.
3. **Triggering phase:** The virus is activated to perform the function for which it was intended.
4. **Execution phase:** The function of virus is performed.

ii. Explain the following terms:

1) Deleted file recovery

2) Formatted partition recovery.

(*3 marks for each point)*

1) Deleted file recovery:

When we delete a file on the disk having FAT32 or NTFS (new technology file system) file system, its content is not erased from the disk but only reference to file data in file allocation Table or master table is marked as deleted. It means that we might be able to recover deleted files or make it visible for file system again.

Methods of data recovery from deleted file or File /data recovery process:

There are various data/file recovery tools available these tools find & recover recoverable deleted files from NTFS & FAT.

These tools usually operate as per following process steps:

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

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

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

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

2) Formatted partition recovery:

Formatting refers to dividing the disk in accordance with certain principles, allowing computer to store and search files. Formatting disk is to eliminate all files on disk.

There are various formatted partition recovery tool available .Although every tool will have different GUI & method of recovery. These tools usually operate as per following process steps:

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.

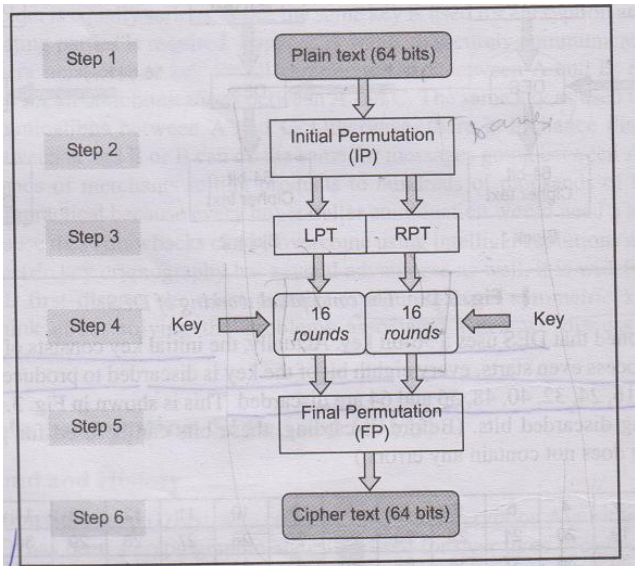
Step 3: Then the founded data will be displayed on the screen & you can get a preview of it. Then select the file or directory that you want to recover & save them to a healthy drive.

Q.2. Attempt any Two of the following:

a) Draw the flow diagram of DES algorithm and explain each step in detail.

The Data Encryption Standard is generally used in the ECB, CBC, or the CFB mode.DES is a block cipher . It encrypts data in blocks of size 64 bits each. That is, 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text.DES is based on the two fundamental attributes of cryptography: substitution and transposition ***(1 mark)***

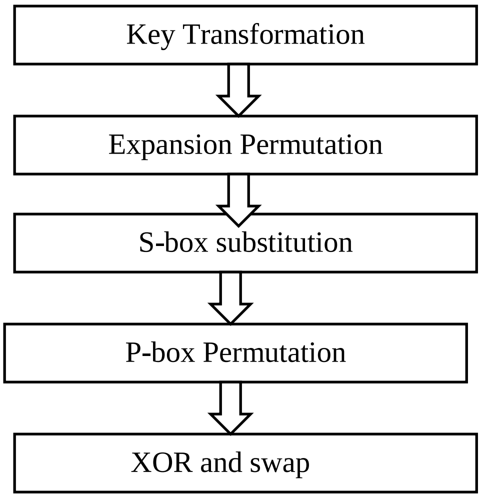
The process diagram as follows **(1 mark)**



Explanation of each step (1mark each=6 marks)

Initial Permutation (IP): It happens only once. It replaces the first bit of the original plain text block with the 58th bit of the original plain text block, the second bit with the 50th bit of original plain text block and so on. The resulting 64-bits permuted text block is divided into two half blocks. Each half block consists of 32 bits. The left block called as LPT and right block called as RPT.16 rounds are performed on these two blocks.

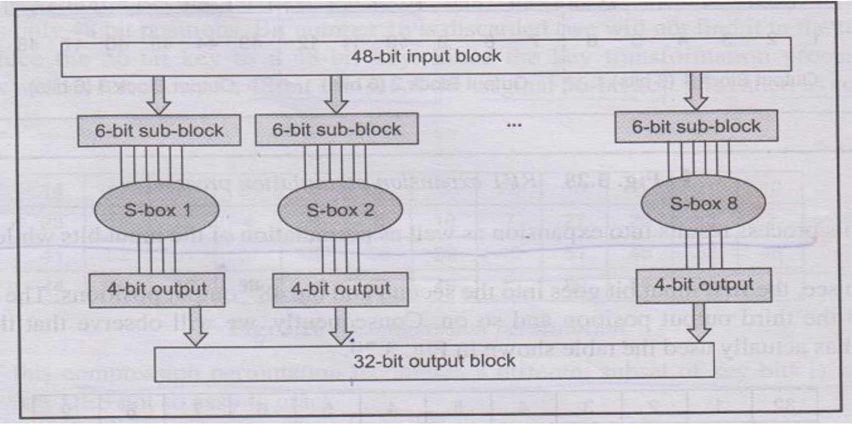
Details of one round in DES



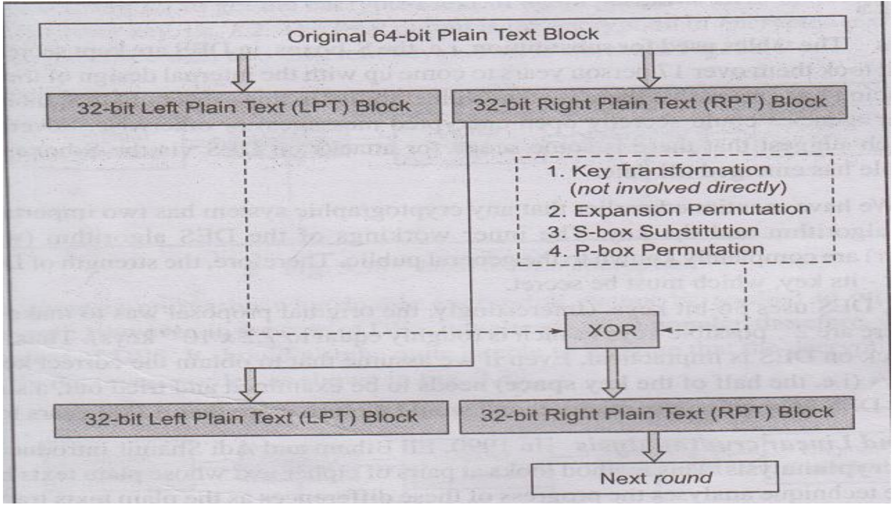
Step 1 : key transformation: the initial key is transformed into a 56-bit key by discarding every 8th bit of initial key. Thus ,for each round , a 56 bit key is available, from this 56-bit key, a different 48-bit sub key is generated during each round using a process called as key transformation

Step 2: Expansion permutation: During Expansion permutation the RPT is expanded from 32 bits to 48 bits. The 32-bit RPT is divided into 8 blocks, with each block consisting of 4-bits. Each 4-bits block of the previous step is then expanded to a corresponding 6-bit block, per 4-bit block, 2 more bits are added. They are the repeated 1st and 4th bits of the 4-bit block. The 2nd and 3rd bits are written as they were in the input. The 48 bit key is XORed with the 48-bit RPT and the resulting output is given to the next step.

Step 3: S-box substitution: It accepts the 48-bits input from the XOR operation involving the compressed key and expanded RPT and produces 32-bit output using the substitution techniques. Each of the 8 S-boxes has a 6-bit input and a 4-bit output. The output of each S-box then combined to form a 32-bit block, which is given to the last stage of a round.



Step 4: P- box permutation: the output of S-box consists of 32-bits. These 32-bits are permuted using P-box.
Step 5: XOR and Swap: The LPT of the initial 64-bits plain text block is XORed with the output produced by P box-permutation. It produces new RPT. The old RPT becomes new LPT, in a process of swapping.


Original 64-bit Plain Text Block
32-bit Left Plain Text (LPT) Block
32-bit Right Plain Text (RPT) Block
1. Key Transformation
(not involved directly)
2. Expansion Permutation
3. S-box Substitution
4. P-box Permutation
XOR
32-bit Left Plain Text (LPT) Block
32-bit Right Plain Text (RPT) Block
Next round

Final Permutation: At the end of 16 rounds, the final permutation is performed. This is simple transposition. For e.g., the 40th input bit takes the position of 1st output bit and so on.

b) Define access control and describe DAC, MAC and RBAC access control model.

(2 marks- definition, 2-marks for each access control)
Access is the ability of a subject to interest with an object. Authentication deals with verifying the identity of a subject. It is ability to specify, control and limit the access to the host system or application, which prevents unauthorized use to access or modify data or resources.
Various access controls are:
- Discretionary Access control (DAC): Restricting access to objects based on the identity of subjects and or groups to which they belongs to , It is conditional, basically used by military to control access on system. UNIX based System is common method to permit user for read/write and execute
- Mandatory Access control (MAC): It is used in environments where different levels of security are classified. It is much more restrictive. It is sensitivity based restriction, formal authorization subject to sensitivity. In MAC the owner or User cannot determine whether access is granted to or not. i.e. Operating system rights. Security mechanism controls access to all objects and individual cannot change that access.
- Role Based Access Control (RBAC): Each user can be assigned specific access permission for objects associated with computer or network. Set of roles are defined. Role in-turn assigns access permissions which are necessary to perform role.

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

c) Gives the step for verification of a digital certificate.
Steps for verification of a digital certificate ***:(1 mark for each step)***
Suppose Y receives digitally signed message from X, who he does not know or trust. X has included his digital certificate with message, which has his public key embedded within it. Before Y can be sure of the message from X, he has to go through following steps:
1) Y will see that which CA signed X's certificate and compares it to the list of CAs he has configured.
2) If X's certificate is in the list of trusted CAs, then he will pass X's certificate through hashing algorithm which will result in Message digest A.
3) Every certificate has a different encrypted Message digest value embedded within it, which is a Digital signature. Y takes CA's public key and decrypts the embedded Digital signature value which is called decrypted DS value B.
4) If value A & B matches then Y can be assured that this CA have actually created a certificate.
5) Y needs to be ensured that the issuing CA has not revoked this certificate.
6) Y will compare email address which is inserted by CA in the certificate with the address that sent this message. If these values are the same he can be assured that the message came from email address that was provided during registration process of certificate.
7) Validity of certificate is proven according to start and stop date of the certificate.
8) Y trusts that this certificate is legal and belongs to X.Y could read the message.

Q.3. Attempt ant Four of the following:

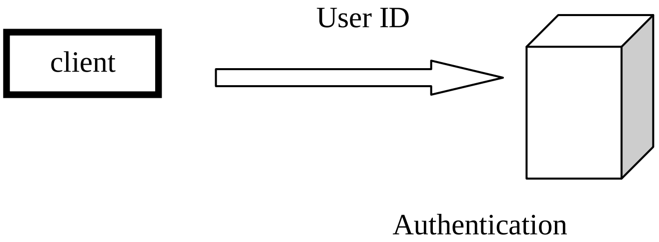
a) Describe overview of Kerberos with diagram.

Kerberos is a network authentication protocol and it is designed to provide strong authentication for client server applications. It uses secret key cryptography. It is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information system. ***(1 mark)***

There are four parties involved in the Kerberos protocol **(3 marks)**

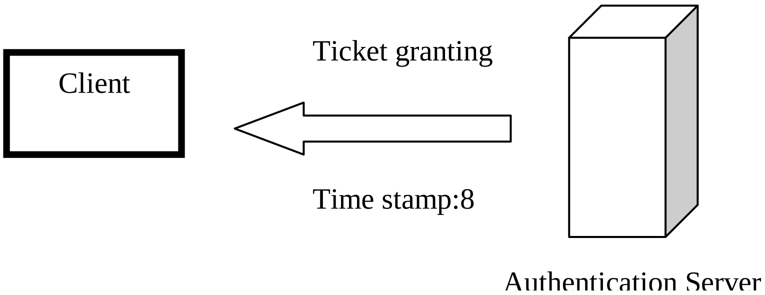
- The client workstation
- Authentication Server(AS)
- Ticket Granting Server(TGS)
- The server offering services such as network printing, file sharing.

1) The AS, receives the request from the client and then AS verifies the client. This is done by just looking into a simple database of the user's ID.

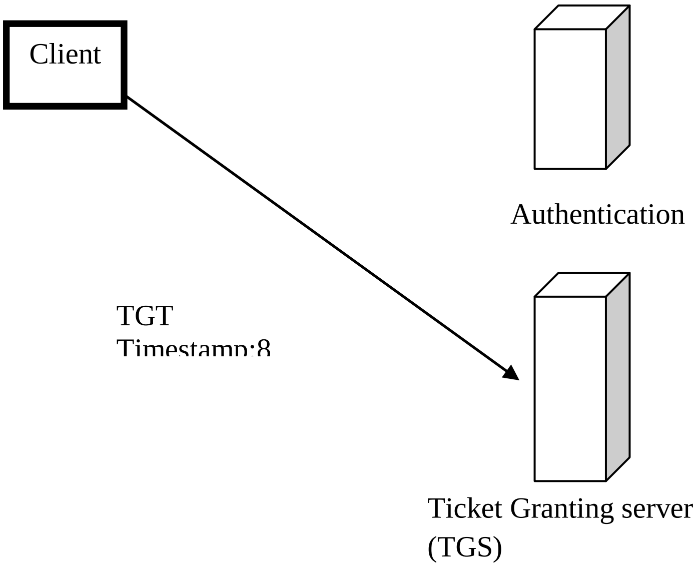


2) After verification, a time stamp is created. It will put the current time in user session with an expiry date. Then the encryption key is created. The timestamp tells that after 8 hours the encryption key is useless.

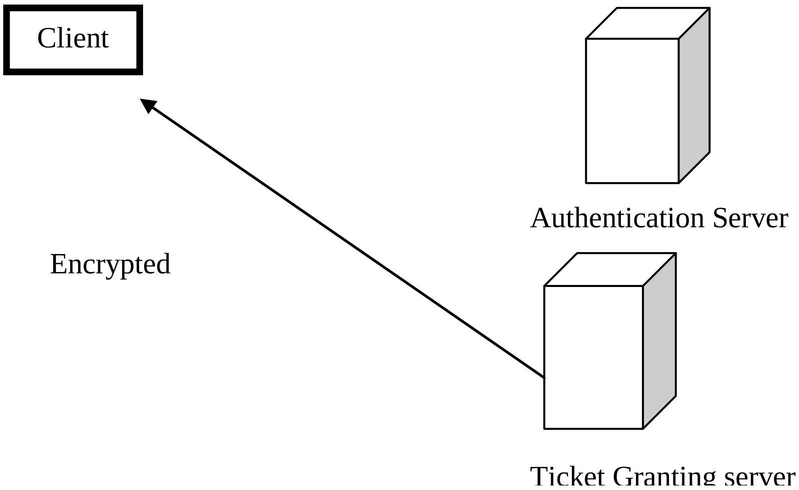
3) The key is sent back to the client in the form of a ticket-granting ticket (TGT).It is a simple ticket which is issued by the authentication server(AS) and used for authenticating the client for future reference.



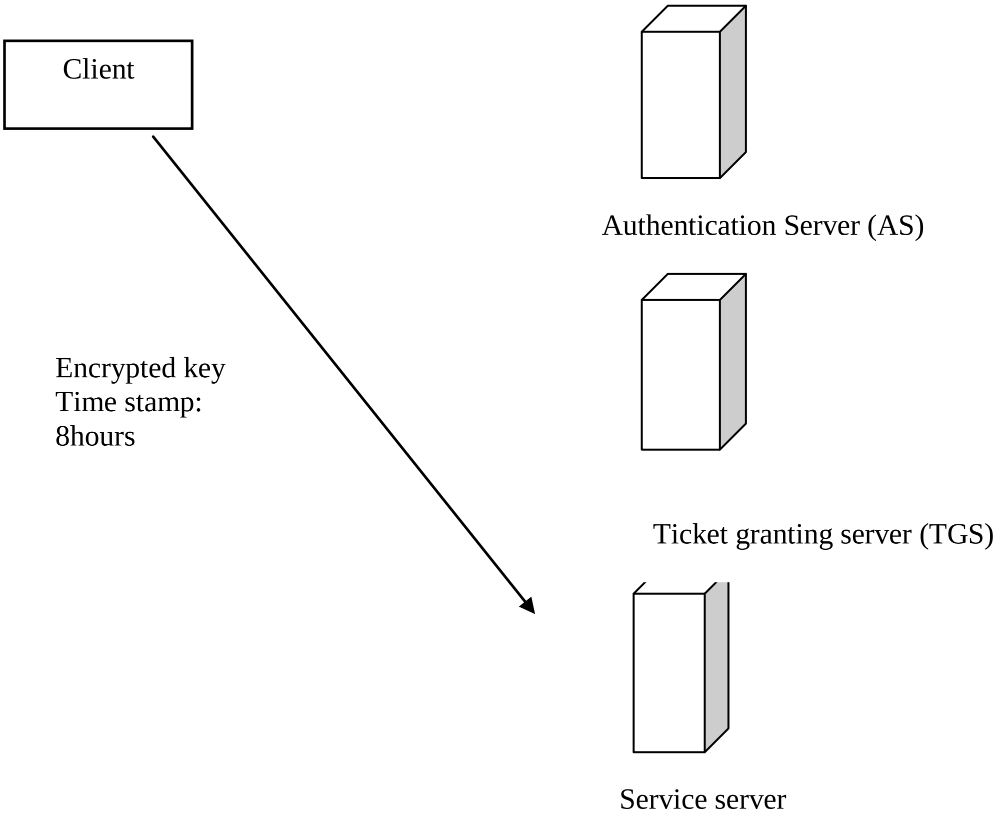
Then the client submits this TGT to the ticket granting server (TGS), for authentication.



4) TGS creates an encrypted key with a time stamp and grants a service ticket to the client.

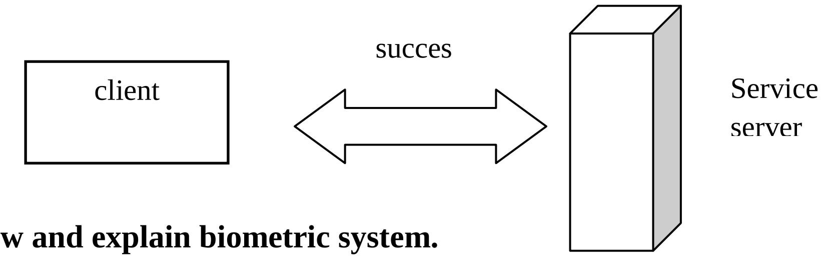


5) Then the client decrypts the ticket, intimate the TGS that is done and sends its own encrypted key to the service server or application.

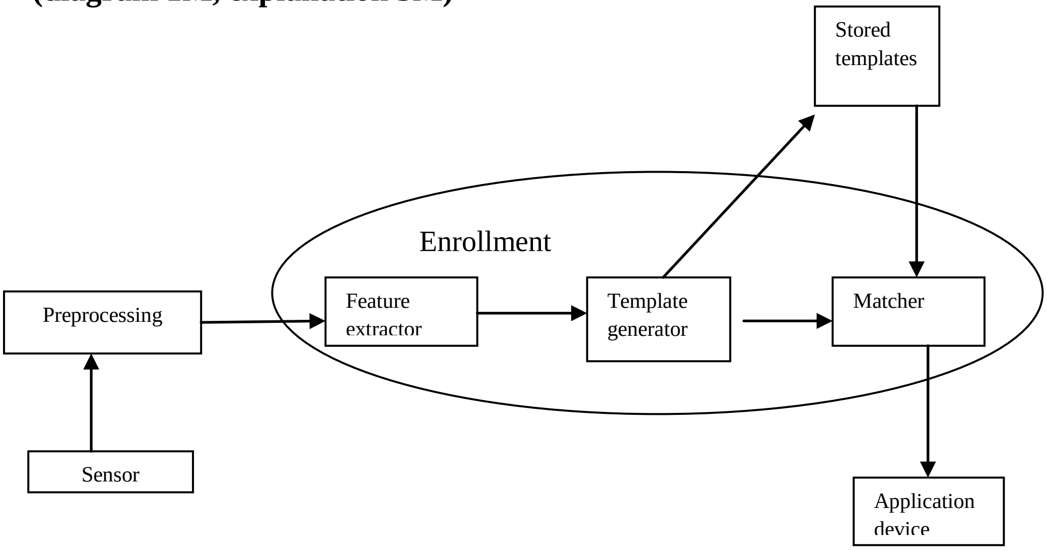


The service server decrypts the key send by the client and checks the validity of the time stamp. If timestamp is valid, the service server contacts the key distribution center to receive a session which is returned to the client.

6) The client then decrypts the ticket. If the key is still valid then the communication is initiated between client and server.



b) Draw and explain biometric system. (diagram 1M, explanation 3M)



Biometric refers study of methods for uniquely recognizing humans based upon one or more intrinsic **physical** or **behavioral** characteristics. 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. Physiological are related to shape of the body. For example finger print, face recognition, DNA, palm print, iris recognition and so on. Behavioral are related to the behavior of a person.

For example typing rhythm, gait, signature and voice.

The first time an individual uses a biometric system is called an enrollment. During the enrollment, biometric information from an individual is stored. In the subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment.

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 preprocessing.
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 enrollment 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) What are the techniques for transforming plain text to cipher text? Explain any one in detail.

(Explanation of any one is allowed) (Marks 2) for example.

Transforming plain text to cipher text is the science of encrypting information scheme is based on algorithms.

Different techniques are: **(2 marks)**

1. Substitution technique
a) Caesar cipher
b) Modified version of Caesar cipher
c) Mono-alphabetic cipher
d) Vigenere's cipher
2. Transposition technique
a) Rail fence
b) Route cipher
c) Columnar cipher
3. Steganography
4. Hashing
5. Symmetric and asymmetric cryptography
6. DES (data encryption standard)

Caesar cipher:

It is proposed by Julius Caesar. In cryptography Caesar cipher also known as caesar's cipher/code, shift cipher/code.

It is one of the simplest and most widely known encryption techniques.

It is a type of substitution technique in which each letter in the plain text is replaced by a letter some fixed number of position down the alphabet.

For example, with a shift of 3, A would be replaced by D, B would became E, and so on as shown in the table below.

Plain text	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher text	D	E	F	G	H	I	J	K	L	M	N	O	P

Plain text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Using this scheme, the **plain text "SECRET"** encrypts as
Cipher text "VHFUHW" .
To allow someone to read the cipher text, you tell them that the **key is 3**

Algorithm to break Caesar cipher:

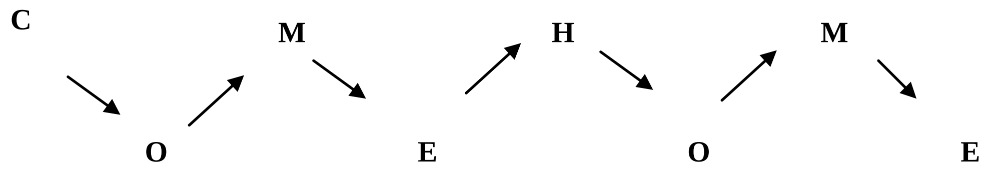
1. Read each alphabet in the cipher text message, and search for it in the second row of the table above.
2. When a match in found, replace that alphabet in the cipher text message with the corresponding alphabet in the same column but the first row of the table. (For example, if the alphabet cipher text is J, replace it with G).
3. Repeat the process for all alphabets in the cipher text message.

Or

Rail Fence Technique algorithm:

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

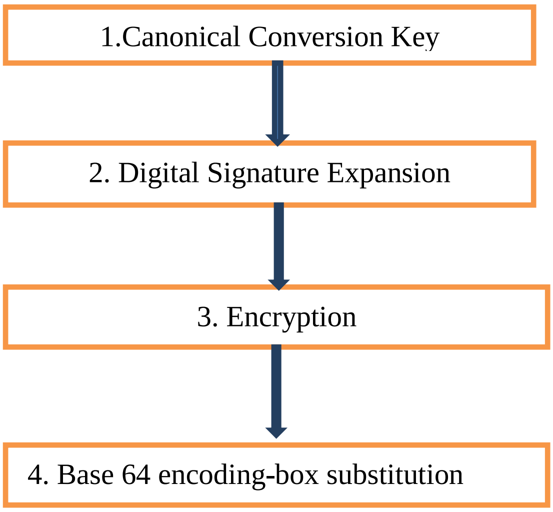
The cipher text for the plain text COME HOME as follows:



Cipher text is CMHMOEOE

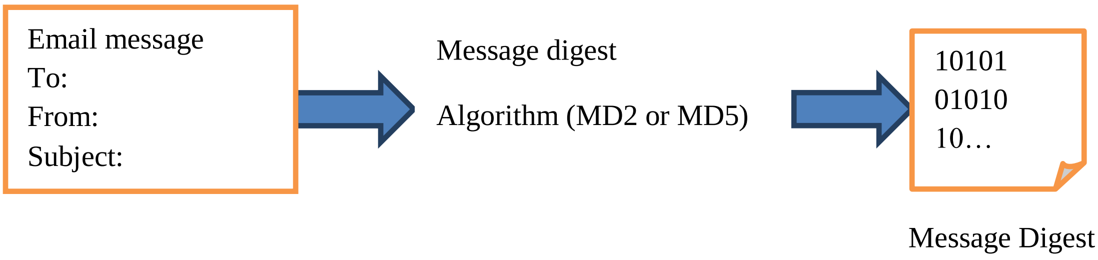
d) Describe the working principle of PEM email security.

PEM supports the 3 main cryptographic functions of encryption, nonrepudiation and message integrity. The steps involved in PEM operation as follows. ***(1 mark for each step)***


1.Canonical Conversion Key
2. Digital Signature Expansion
3. Encryption
4. Base 64 encoding-box substitution

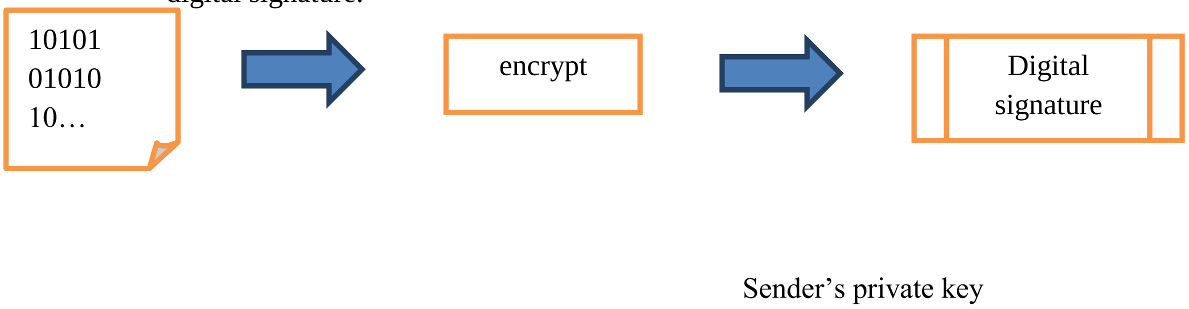
Step 1: canonical conversion: there is a distinct possibility that the sender and the receiver of an email message use computers that have different architecture and operating systems.PEM transforms each email message into an abstract, canonical representation. This means that regardless of the architecture and the operating system of the sending and receiving computers, the email travels in a uniform, independent format.

Step 2: Digital signature



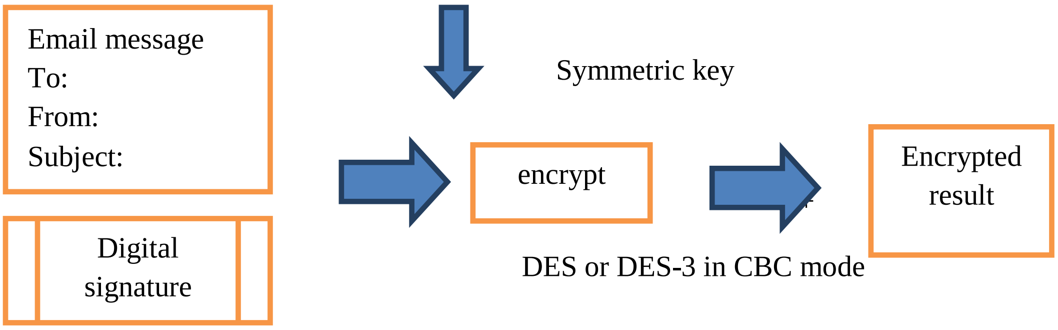
-It starts by creating a MD of email message using an algorithm such as MD2 or MD5.

- The MD thus created is then encrypted with sender's private key to form the sender's digital signature.

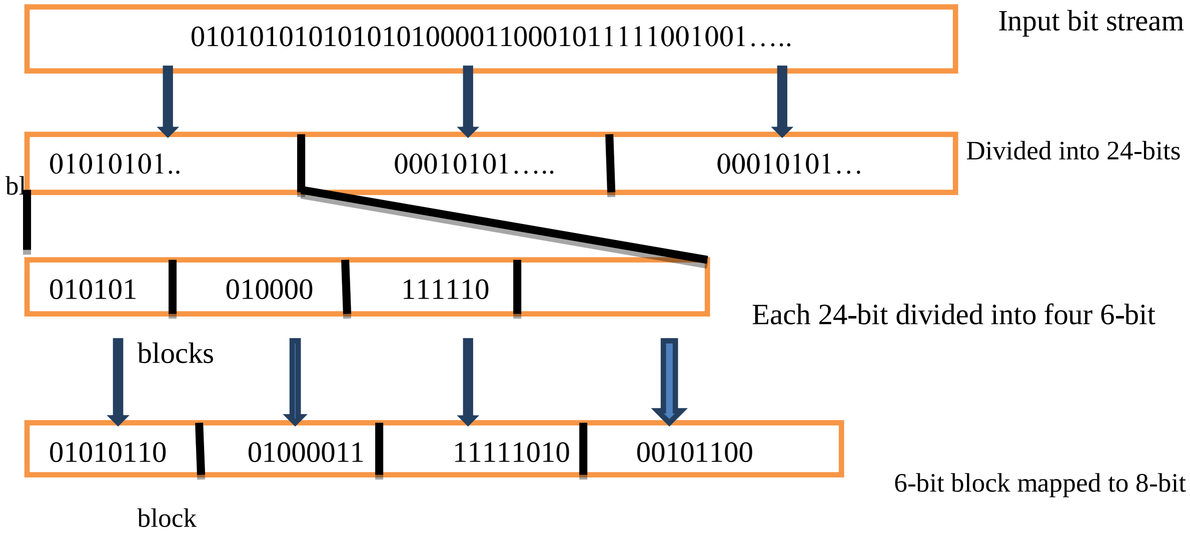


Step 3-encryption:

The original email and the digital signature are encrypted together with a symmetric key



Step 4: Base- 64 encoding-This process transforms arbitrary binary input into printable character output. The binary input is processed in blocks of 3 octets or 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.



e) Describe:

i. Application patches

ii. Upgrades.

i) Application patches (2marks)

As o.s continues to grow and introduce new functions, the potential for problems with the code grows as well. It is almost impossible for an operating system vendor to test its product on every possible platform under every possible platform under every possible circumstance, so functionality and security issues do arise after an o.s. has been released. Application patches are likely to come in three varieties: hot fixes, patches and upgrades.

Application patches are supplied from the vendor who sells the application. Application patches can be provided in many different forms like can be downloaded directly from the vendor's web site or FTP site or by CD. Application patches are probably come in three varieties: hot fixes, patches and upgrades.

ii) Upgrades (2 marks)

These are another popular method of patching applications, and they are likely to be received with a more positive role than patches. The term upgrade has a positive implication-you are moving up to a better, more functional and more secure application. The most vendors will release upgrades for fixes rather than any new or enhanced functionality.

Q.4.

a) Attempt any Three of the following:

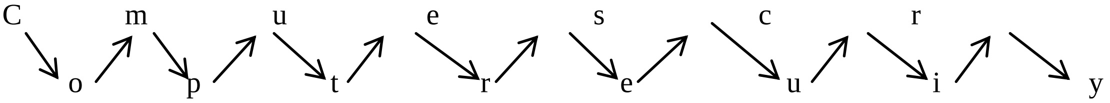
i. Consider a plain text "Computer Security" encrypt it with the help of rail fence Technique also write the algorithm.

(2 marks for encryption and 2 marks for algorithm)

Rail Fence Technique algorithm:

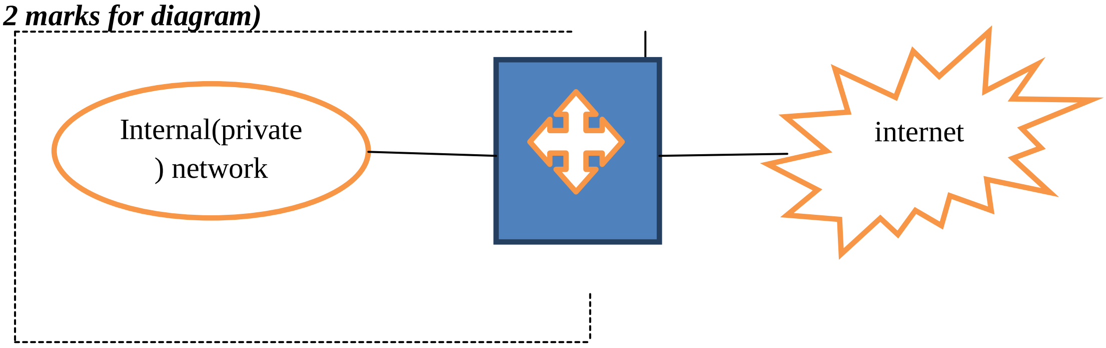
3. Write down the plain text message as a sequence of diagonals.
4. Read the plain text written in step1 as a sequence of rows.

The cipher text for the plain text Computer security as follows:

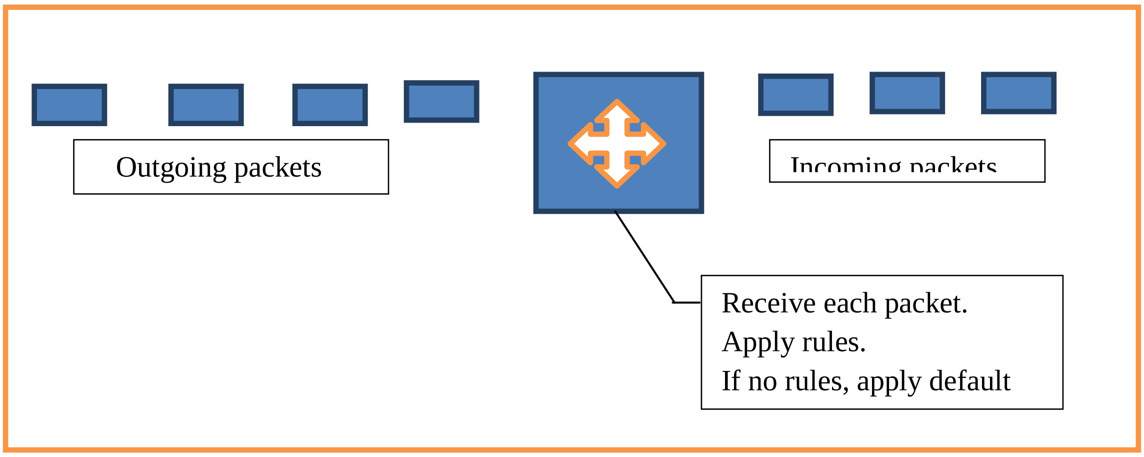


Cipher text: cmuescroptreuiy

ii.* Describe packet filtering router firewall with neat diagram.*(2 marks for explanation and 2 marks for diagram)



Packet filter



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.

A packet filter performs the following functions.

1. Receive each packet as it arrives.
2. 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.
3. 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.

iii. Describe the following w.r.t. cyber laws:

1) IT act 2000

2) IT act 2008

1) IT act 2000*(2 marks):*

According to Indian cyber laws, Information technology is the important law and it had passed in Indian parliament in year 2000.This act is helpful to encourage business by use of internet. Due to misuse of internet and increase of cybercrime, the Govt. of India made an act for safeguarding the internet users.

The main objectives of this act are as follows.

1. To provide legal recognition to the transaction that can be done by electronic way or by using internet.
2. To provide legal recognition to digital signature used in transaction.
3. To provide facilities like filling of document online relating to admission or registration.
4. To provide facility to any company that they can store their data in electronic storage.
5. To provide legal recognition for bankers and other companies to keep accounts in electronic form.

2) <u>IT act 2008*(2 marks):*</u>

It is the Information Technology Amendment Act,2008.the act was developed for IT industries, control e-commerce, to provide e-governance facility and to stop cybercrime attacks.

Following are the characteristics of IT ACT 2008:

a) This act provide legal recognition for the transaction i.e. Electronic Data Interchange(EDI) and other electronic communications.

b) This Act also gives facilities for electronic filling of information with the Government agencies.

c) It is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

iv. What is secure electronic transaction? Enlist and describe any four components of SET.

<u>Secure electronic Transaction</u> is an open encryption and security specification that is designed for protecting credit card transactions on the Internet. It is a set of security protocols and formats that enable the users to employ the existing credit card payment infrastructure on the internet in a secure manner.(1 mark)

Components of SET *(1 mark)*

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

Describe any <u>four</u> *(1/2 mark for each)*

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.

b) Attempt any ONE of the following:

i. **Compare Insider and Intruders of four points and describe who is more dangerous.*(4marks for any 4 points)***

Intruders	Insiders
Intruders are authorized or unauthorized users who are trying access the system or network.	Insiders are authorized users who try to access system or network for which he is unauthorized.
They are hackers or crackers	Insiders are not hackers.
Intruders are illegal users.	Insiders are legal users.
Less dangerous than insiders	More dangerous than Intruders.
They have to study or to gain knowledge about the security system	They have a knowledge about the security system.
They do not have access to system.	They have easy access to the system because they are authorized users.
Many security mechanisms are used to protect system from Intruders.	There is no such mechanism to protect system from Insiders.

Describe who is more dangerous. (2 marks)

Insiders are more dangerous than intruders because:

i) The insiders have the access and necessary knowledge to cause immediate damage to an organization.

ii) There is no security mechanism to protect system from Insiders. So they can have all the access to carry out criminal activity like fraud. They have knowledge of the security systems and will be better able to avoid detection.

ii. Describe:

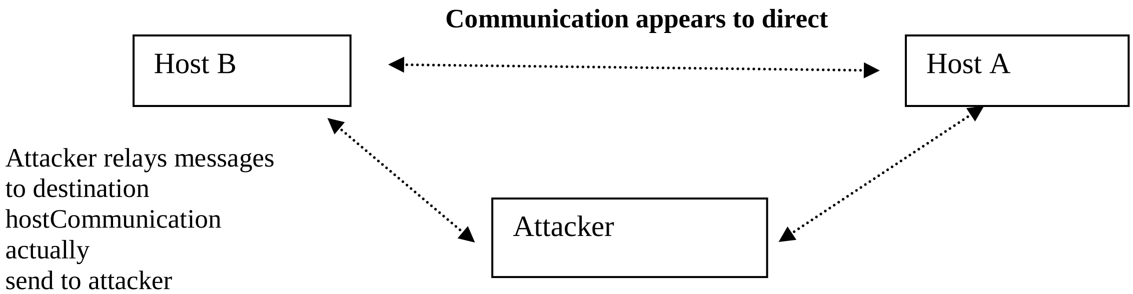
1. Man in the middle attack

2. Replay attach with diagrams.

i) Man in the middle attack:(3 marks)

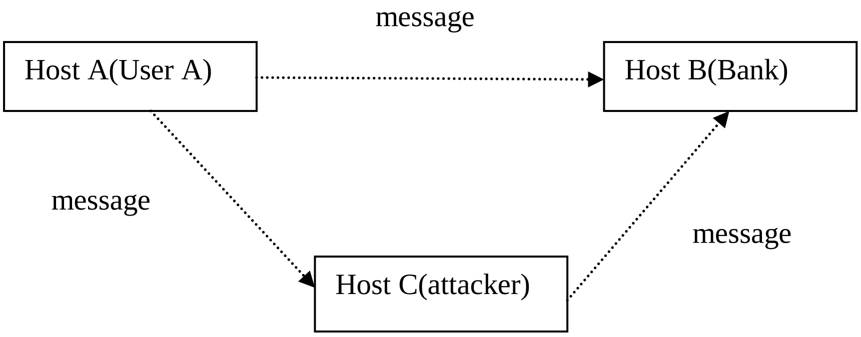
A man in the middle attack occurs when attackers are able to place themselves in the middle of two other hosts that are communicating in order to view or modify the traffic. This is done by making sure that all communication going to or from the target host is routed through the attacker's host.

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.



i) Replay attack with diagram(3 marks)

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.



Q.5. Attempt any Two of the following:

a) Describe the role of people in security.

Role of people in security ***(each point 1 Mark, 8 point)***

a) Password selection:

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

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

3) It should not consist of dictionary words. Etc.

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

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

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

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

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

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

h) Individual user responsibilities:

i) Lock the door of office or workspace.

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

iii) Secure storage media which contains sensitive information.

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

b) Describe the components of HIDS with neat diagram. State its advantages and disadvantages.(*2 marks explanation , diagram 2 marks, 2 Advantages, Disadvantages 2 Marks)*

Intrusion detection system (IDS):

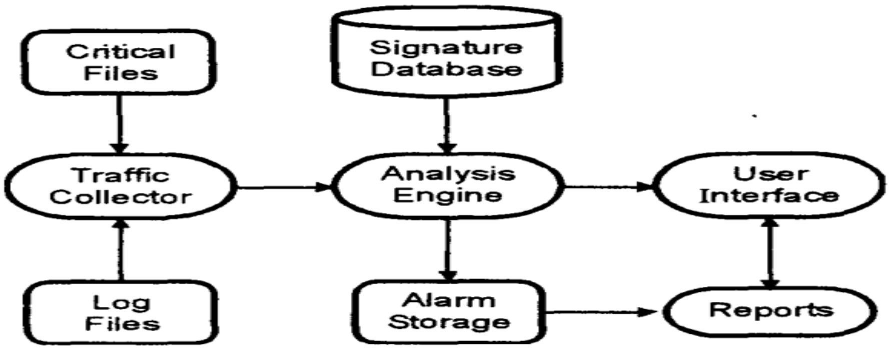
An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.

1. **HIDS**

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

   HIDS is looking for certain activities in the log file are:

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



Basic Components HIDS:

1. Traffic collector:

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

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

2. Analysis Engine:

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

3. Signature database:

It is a collection of patterns & definitions of known suspicious or malicious activity.

4. User Interface & Reporting:

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

Advantages:

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

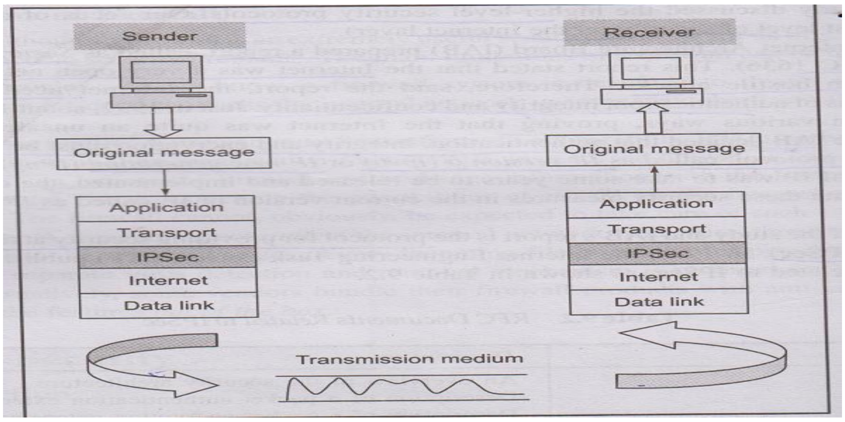
Disadvantages:

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

c) What is IP sec? Draw and explain the AH format of IP sec.

IPSec architecture: The overall idea of 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

Diagram and Theory ***(2 mark)***

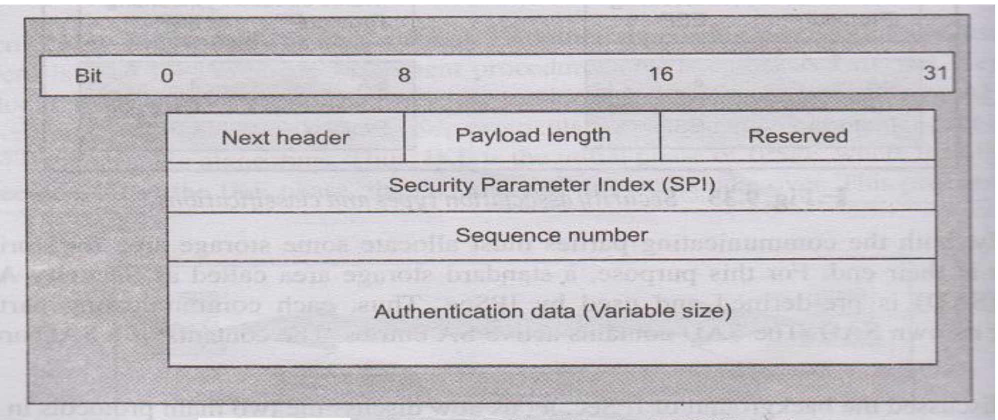


IPSec actually consists of two main protocols a) Authentication Header (AH):
b) Encapsulating Security Payload (ESP):

a) Authentication Header (AH) ***(2 marks)***

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.

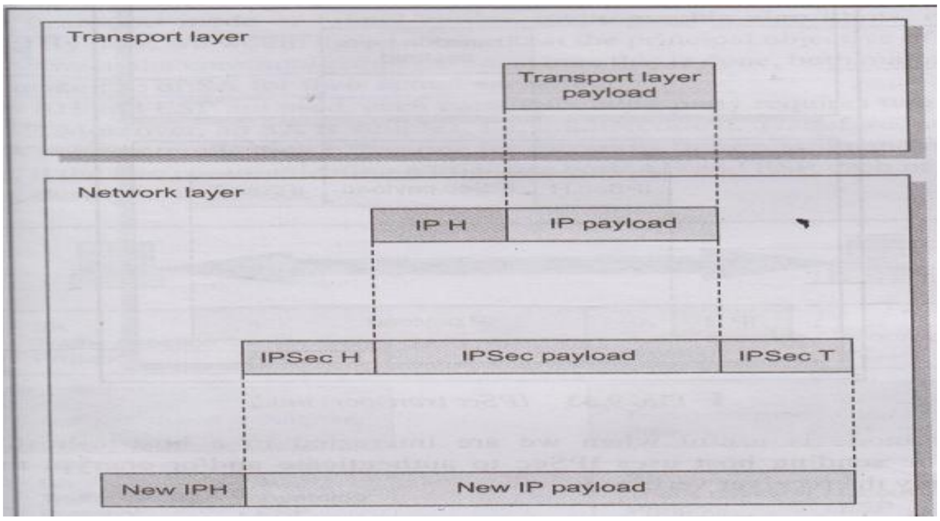
Diagram


Bit
0
8
16
31
Next header
Payload length
Reserved
Security Parameter Index (SPI)
Sequence number
Authentication data (Variable size)

Authentication Header (AH) format

Modes of operation (4 marks)
Both AH and ESP works in two modes:
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.

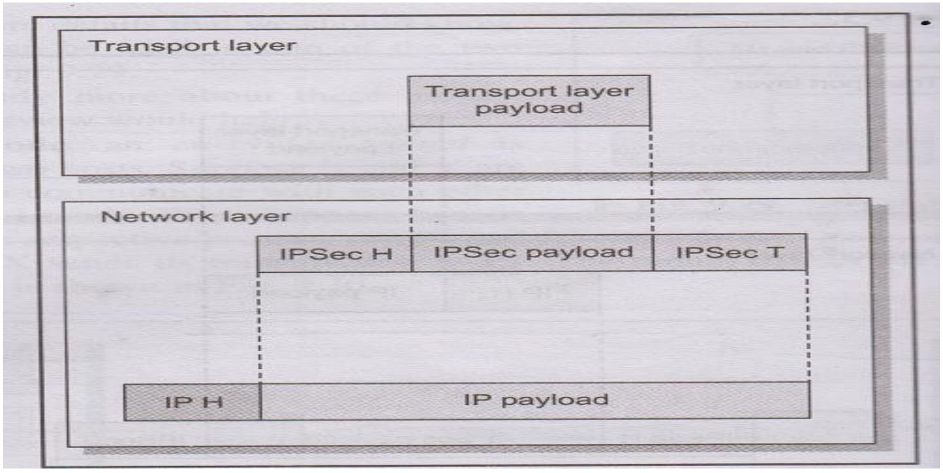
Diagram



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.

Diagram



Q.6. Attempt any FOUR of the following:

a) State any four different types of problems occur due to installation of unauthorized software/hardware.*(1 mark for each)*

1. Installing unauthorized software from internet may create backdoors in your system or network which can be used to access a system by avoiding normal security mechanism.

2. When we are installing various games from the internet, the problems with such a download is that users don't know from where the software originally came and what may be hidden inside it?

3. Accessing and downloading data from unofficial sites can create virus problem into your system as well in entire network.

4. Unauthorized hardware device and software product is not capable to protect your system/network due to lack in security functionality.

b) Describe Caeser's cipher technique. Write its algorithm with an example.
(Algorithm 2 marks Explanation 2 marks)

Caesar cipher:
It is proposed by Julius Caesar. In cryptography, Caesar cipher also known as Caesar's cipher/code, shift cipher/code.
It is one of the simplest and most widely known encryption techniques.
It is a type of substitution technique in which each letter in the plain text is replaced by a letter some fixed number of position down the alphabet.

For example, with a **shift of 3**, A would be replaced by D, B would became E, and so on as shown in the table below.

Plain text	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher text	D	E	F	G	H	I	J	K	L	M	N	O	P

Plain text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

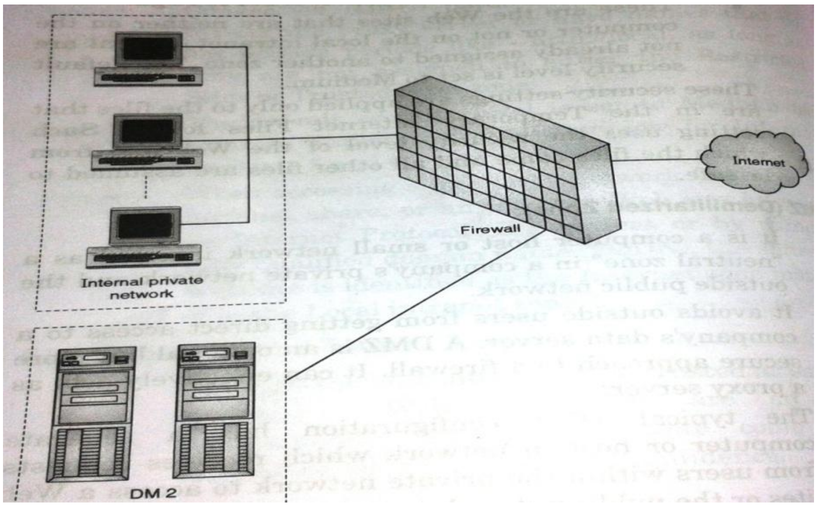
Using this scheme, the **plain text "SECRET"** encrypts as
Cipher text "VHFUHW" .
To allow someone to read the cipher text, you tell them that the **key is 3**

Algorithm to break Caesar cipher:

1. Read each alphabet in the cipher text message, and search for it in the second row of the table above.
2. When a match in found, replace that alphabet in the cipher text message with the corresponding alphabet in the same column but the first row of the table.
(For example, if the alphabet cipher text is J, replace it with G).
3. Repeat the process for all alphabets in the cipher text message.

c) **Describe DMZ with suitable diagram.**
(Diagram 1 mark , Explanation 3 marks)

DMZ (Demilitarized Zone)



It is a computer host or small network inserted as a "neutral zone" in a company's private network and the outside public network.

It avoids outside users from getting direct access to a company's data server. A DMZ is an optional but more secure approach to a firewall. It can effectively acts as a proxy server.

The typical DMZ configuration has a separate computer or host in network which receives requests from users within the private network to access a web sites or public network. Then DMZ host initiates sessions for such requests on the public network but it is not able to initiate a session back into the private network. It can only forward packets which have been requested by a host.

The public network's users who are outside the company can access only the DMZ host.
It can store the company's web pages which can be served to the outside users. Hence, the DMZ can't give access to the other company's data.

By any way, if an outsider penetrates the DMZ's security the web pages may get corrupted but other company's information can be safe.

d) Describe:
i. Hacking
ii. Cracking
(2 marks for each)

(i) **Hacking:**

Hacking is one of the most well-known types of computer crime. A hacker is someone who find out and exploits the weaknesses of s computer systems or networks.
Hacking refers to unauthorized access of another's computer systems. These intrusions are often conducted in order to launch malicious programs known as viruses, worms, and Trojan horses that can shut down hacking an entire computer network.
Hacking is also carried out as a way to talk credit card numbers, intent passwords, and other personal information.
By accessing commercial database, hackers are able to steal these types of items from millions of internet users all at once.
There are different types of hackers:

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

(ii) **Cracking:**

In the cyber world, a cracker is someone who breaks into a computer system or network without authorization and with the intention of doing damage.
Crackers are used to describe a malicious hacker.
Crackers get into all kinds of mischief like he may destroy files, steal personal information like credit card numbers or client data, infect the system with a virus, or undertake many others things that cause harm.
Cracking can be done for profit, maliciously, for some harm to organization or to individuals.
Cracking activity is harmful, costly and unethical.

e) Explain secure socket layer and describe the SSL protocol stack with neat diagram.
(Diagram 1 mark, Explanation of blocks 3 marks)

SSL:

SSL is a commonly used internet protocol for managing the security of a message transmission between web browser and web server.

SSL is succeeded by transport layer security (TLS) and it is based on SSL.

SSL uses a program layer which is located between internet's hypertext transfer protocol (http) and transport control protocol (TCP) layers.

SSL is included as part of both the Microsoft and Netscape browsers and most web server products.

SSL provides two levels of security services, authentication and confidentiality. SSL is logically a pipe between web browser and web server.

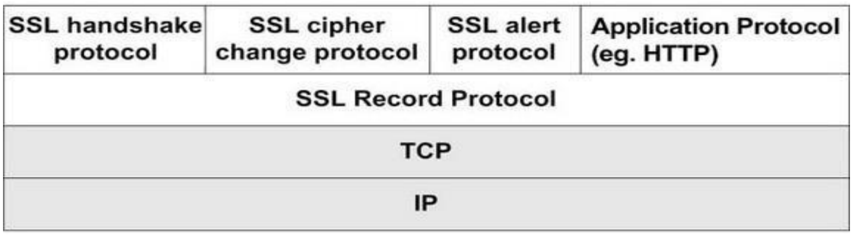


Fig. SSL protocol stack

1. Handshake protocol:

This protocol allows the server and client to authenticate each other.

Also, it will allow negotiating an encryption and MAC algorithm.

This protocol is used before transmitting any application data. Basically, this protocol contains a series of messages exchanged by client and server.

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

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

2. Record protocol:

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

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

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

3. Alert protocol: when either the client or the server detects an error, the detecting party sends an error message to other party.

If the error is fatal, both the parties immediately close the SSL connection. Both the parties also destroy the session identifiers, secret and keys associated with this connection before it is terminated.

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