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. Define intruder and state its types.(Definition 2 Marks, Types 2marks)

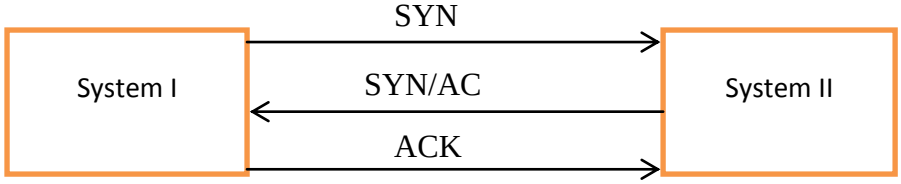
An intruder is a person that enters territory that does not belong to that person. Intruders try to intrude into the privacy of the network.

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

a) **Masquerader:** A user who does not have the authority to use a computer, but penetrates into a system to access a legitimate user's account is called a masquerader. It is generally an external user.
b) **Misfeasor:** There are two possible cases for an internal user to be called as a misfeasor:
   1) A legitimate user, who does not have access to some applications, data or resources, accesses them.
   2) A legitimate user, who has access to some applications, data or resources, misuses these privileges.
c) **Clandestine user:** An internal or external user who tries to work using the privileges of a supervisor user to avoid auditing information being captured and recorded is called as a clandestine user.

ii. Explain Denial of service attack with neat labeled diagram.(Diagram 2Marks, Explanation 2Marks)

Denial of service (DOS) attack: This attack make an attempt to prevent legitimate users from accessing some services, which they are eligible for. For instance, an unauthorized user might send too many login requests to a server using random user ids one after the other in quick succession, so as to flood the network and deny other legitimate users from using the network facilities:



System I wants to communicate with System II by sending SYN packet. Then System II will send back SYN/ACK if it wants to communicate or it is able to accept the request and send ACK packet to System I. This is the normal process, but attacker will send fake requests of communication. These requests will be answered by target system and waits for responses, which will never come because request is fake.

iii. Describe at least four responsibilities of individual user.
Four responsibilities of individual user: (any four points 1 mark each)

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.

iv. State and explain any 4 password selection policies/strategies. (1Mark each)
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.

b) Attempt any One of the following:

i. Describe secure code technique and buffer overflow.
Secure coding techniques and buffer overflow: (3marks for each)
Securing coding is the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities. Defects, bugs and logic flaws are consistently the primary cause of commonly exploited software vulnerabilities. Through the analysis of thousands of reported vulnerabilities, security professionals have discovered that most vulnerabilities stem from a relatively small number of common software programming errors. By identifying the insecure coding practices that lead to these errors and educating developers on secure alternatives, organizations can take proactive steps to help significantly reduce or eliminate vulnerabilities in software before deployment. Following are some techniques for secure coding:

- Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software vulnerabilities.
- Compile code using the highest warning level available for your compiler and eliminate warnings by modifying the code.
- Create software architecture and design your software to implement and enforce security policies.
- Keep the design as simple and small as possible .Complex designs increase the likelihood that errors will be made in their implementation, configuration, and use.
- Good quality assurance techniques can be effective in identifying and eliminating vulnerabilities.
- Develop and/or apply a secure coding standard for your target development language and platform.

Buffer overflow: In computer security and programming, a **buffer overflow** is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety, similar to a buffer over-read.

Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. This may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited.

Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type) is within the boundaries of that array. Bounds checking can prevent buffer overflows

Consider another scenario where you try to fill a buffer (on stack) beyond it's capacity

```
char buff[10] = {0};
strcpy(buff, "This String Will Overflow the Buffer");
```

As you can see that the strcpy() function will write the complete string in the array 'buff' but as the size of 'buff' is less than the size of string so the data will get written past the right boundary of array 'buff'. Now, depending on the compiler you are using, chances are high that this will get unnoticed during compilation and would not crash during execution. The simple reason being that stack memory belongs to program so any buffer overflow in this memory could get unnoticed.

So in these kind of scenarios, buffer over flow quietly corrupts the neighbouring memory and if the corrupted memory is being used by the program then it can cause unexpected results.

ii. Explain the steps for hardening windows operating system.(1 mark for each point)

1. Rename administrator account: The built in administrator account and administrator group has the greatest number of default permissions and privilege as well as the ability to change their permissions and privileges. The object is to prevent an intruder from gaining control over the computer and administrator rights from the built in administrator account. To accomplish this rename the administrator account, change its description and password-protect it.
2. Using strong password: pick a password atleast 8 character long. Windows will accept a max of 127 characters. Use upper and lower case letters, numbers and try to use special characters also.

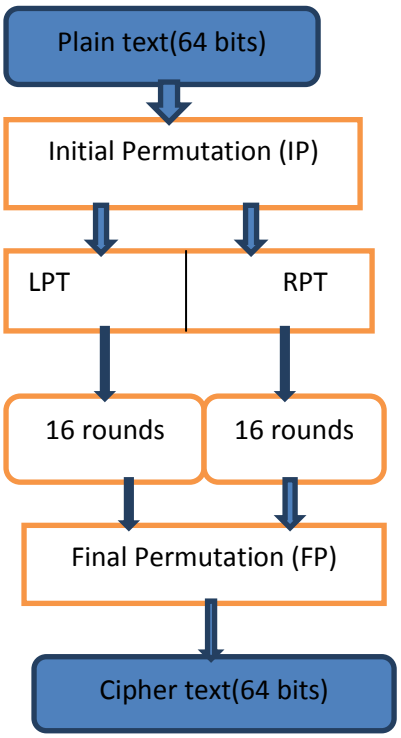
3. Use NTFS file systems: When windows XP or 2000 is installed, it should be installed in a separate partition formatted with the NTFS file system rather than older FAT file system.NTFS allow you to configure which users have access to which data, who can perform what kind of operation and allows you to encrypt files and data.
4. Disable all unnecessary services: windows system will serve one main purpose (web server, mail server).once you have strong with what the main purpose of the system will be then disable a service which is not necessary for that purpose.
5. Restrict permissions on files and access to the Registry: The windows registry must be protected to ensure that entries are not modified or deleted.
6. Remove unnecessary programs: ay application or utility which is not required should be removed.
7. Apply latest patches, hotfixes and service packs: make sure that the o.s. and all applications have the latest vendor supplied patches applied.
8. Remove unnecessary user accounts.

Q.2. Attempt any TWO of the following:

a) Describe data encryption standard algorithm with neat labeled diagram.

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)**

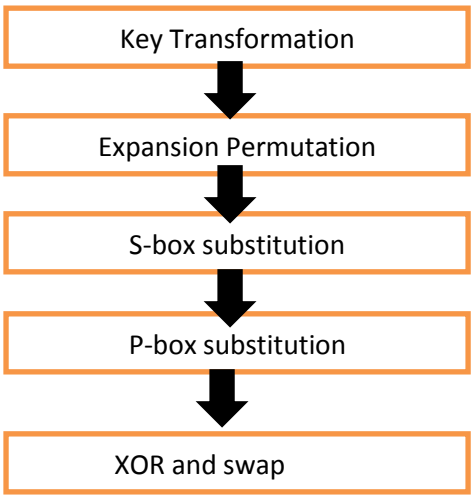
The process diagram as follows **(1 mark)**



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.

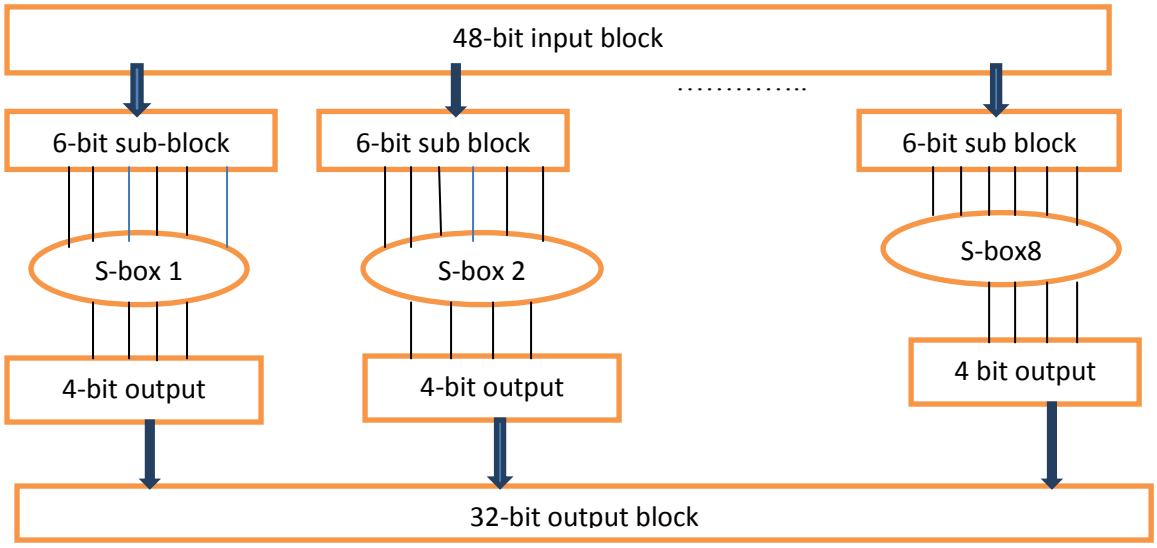
Details of one round in DES



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 a4-bit output as shown below:



Step 4:P-box permutation: The output of S-box consists of 32 bits. These 32 bits are permuted using a P-box.
It involves simple permutation. For eg., a 16 in the first block indicates that the bit at position 16 of the original input moves to bit at position 1 in the output and a 10 in the block number 16 indicates that the bit at the position 10 of the original input moves to bit at position 16 in the output.

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Step 5: XOR and swap:
The LPT of the initial 64-bit plain text block is XORed with the output produced by P-box permutation. The result of this XOR operation becomes the new RPT.The old right half (RPT) becomes the new left half, in the process of swapping.
Final permutation: At the end of 16 rounds, the Final Permutation is performed only once (simple transposition).

b) State secure electronic transaction and its purpose. Summarize various participants in SET and their roles.(2 Marks)

SET is an open encryption and security specification that is designed for protecting credit card transactions on the Internet. SET services can be summarized as follows:

1) It provides a secure communication channel among all the parties involved in an e-commerce transaction.
2) It provides authentication by the use of digital certificate.
3) It ensures confidentiality, because the information is only available to the parties involved in a transaction and that too only when and where necessary.

Various participants in SET and their roles: **(1 mark 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: A merchant is a person or an organization that wants to sell goods or services to cardholders.
3) Issuer: The issuer is a financial institution (bank) that provides a payment card to a card holder. The issuer is responsible for the payment of the cardholder's debt.
4) Acquirer: This is a financial institution that has a relationship with merchants for processing payments card authorizations and payments.
5) Payment gateway: It processes the payment messages on behalf of the merchants. Payment gateway act as an interface between SET and existing card payment network for payment authorizations .The merchant exchanges SET messages with the payment gateway over the Internet. The payment gateway in turn connects to the acquirer's systems using a dedicated network line.
6) Certification authority (CA): This is an authority that is trusted to provide public key certificates to cardholders, merchants and payment gateways.

c) Demonstrate Deffi-Hellman algorithm with a suitable example.
(4 marks for description and 4 marks for example)

Deffi-Hellman key exchange algorithm can be used only for key agreement, but not for encryption or decryption of messages.
Description of the algorithm: Assume that Alice and Bob want to agree upon a key to be used for encryption/decryption of messages that would be exchanged between them.

1) Alice and Bob agree on two large prime numbers, n and g. these two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.
2) Alice chooses another large random number x, and calculate A such that:
3) $A=g^x \bmod n$
4) Alice sends the number A to Bob.
5) Bob sends the number B to Alice.
6) A now computes the secret key K1 as follows:

$K1 = B^X \bmod n$

7) B now computes the secret key K2 as follows:

$K2 = A^Y \bmod n$

Example:

1. Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.

Let n = 11, g = 7

2. Alice chooses another large random number x, and calculates A such that :

$A = g^X \bmod n$

Let x = 3. Then, we have, $A = 7^3 \bmod 11 = 343 \bmod 11 = 2$

3. Alice sends the number A to Bob.

Alice sends 2 to Bob

4. Bob independently chooses anotherlarge random integer y and calculates B such that:

   $B = g^y \bmod n$
   Let y = 6. Then, we have, $B = 7^6 \bmod 11 = 117649 \bmod 11 = 4$

5. Bob sends the number B to Alice

   Bob sends 4 to Alice
6. A now computes the secret key K1 as follows:

   $K1 = B^X \bmod n$
   We have, $K1 = 4^3 \bmod 11 = 64 \bmod 11 = 9$

7. B now computes the secret key K2 as follows:

   $K2 = A^y \bmod n$
   We have, $K2 = 2^6 \bmod 11 = 64 \bmod 11 = 9$
   Thus, K1=K2=9 both keys are matched.

Q.3) Attempt any four of the following: (16m)

a) State the definition of attack to computer system/security and explain encryption attack.

Definition of attack:- (2m)

In computer and computer networks an **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Security attack refers to a process whereby a person compromises your computer by installing harmful malicious software in your computer without your knowledge. These malicious software includes viruses, spywares, adwares, and trojan horses. These software often deletes certain vital files on your computer, making your computer to function abnormally, spying on your online surfing habits, and cause advertisements to pop up on the screen.

Encryption attack:- (2m)

Cryptography is the art and science of writing secret message and encryption is the process of transforming plaintext into cipher text, which is in unreadable format known using a specific technique or algorithm.

In encryption process key is used by many encryption techniques. The one key is used in a mathematical process to jumble the original message to unreadable cipher text and other is used to decrypt cipher text to re-crate the original plain text. The length of the key directly Relates to the strength of the encryption.

Cryptanalysis is the process of attempting to break a cryptographic system. This is an attack on the specific method used to encrypt the plaintext. There are many ways cryptographic systems can be compromised.

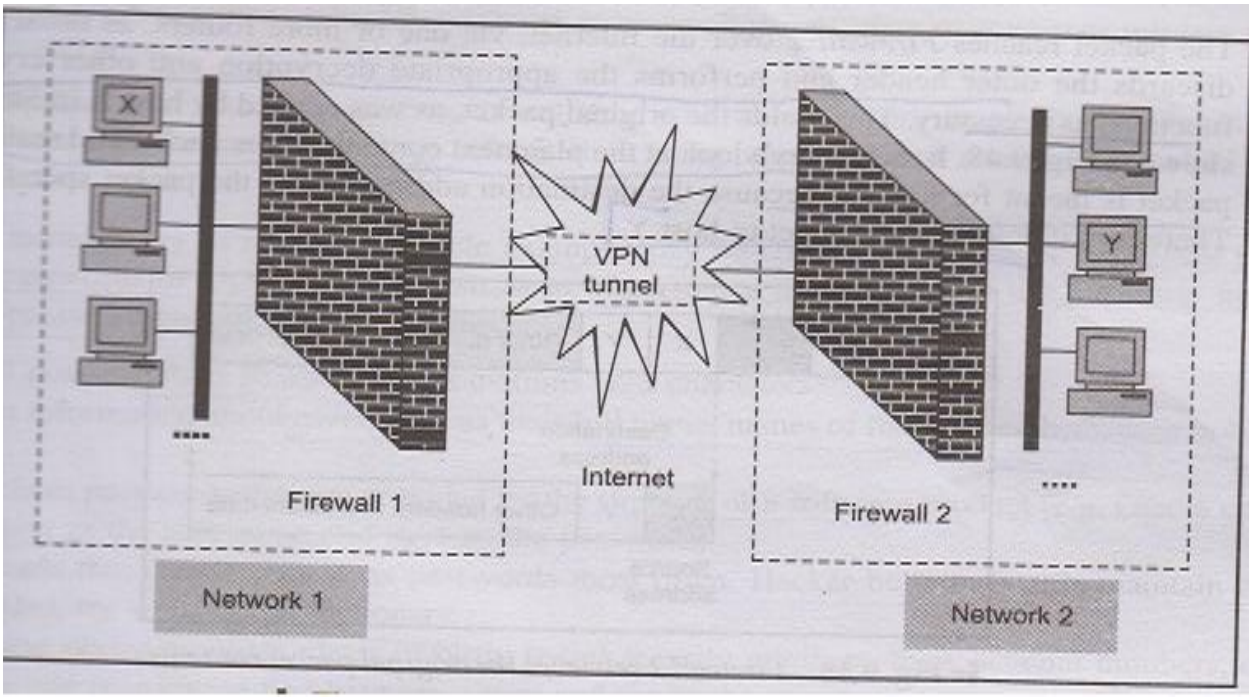
b) Illustrate with neat Labeled virtual Private Network. (1m-diag. & 3m- theory)

A VPN (virtual private network) is a network that uses a public telecommunication infrastructure, such as the internet, to provide remote offices or individual users with secure access to their organization's network

A VPN is a mechanism of employing encryption, authentication, and integrity protection so that the public network can use as private network.

A VPN can connect distant networks of an organization, or it can be used to allow travelling users to remotely access the organization's internet e.g. private network.

A VPN is a mechanism to create a private network over a public network like internet. It depends on the use of virtual connections, these connections are temporary, and do not have any physical presence. They are made up of packets.



Suppose an organization has two networks, Network 1 and Network 2, which are physically separate from each other and user want to connect them, using VPN approach. In such case we set up two firewalls, Firewall 1 and Firewall 2.The encryption and decryption are performed by firewalls. Network 1 connects to the Internet via a firewall named Firewall 1 and Network 2 connects to the Internet with its own firewall, named Firewall 2.

The important points here is that two firewall are virtually connected to each other via internet with the help of a VPN tunnel between two firewalls.

c) Describe the process of biometric authentication with neat labeled diagram for finger print. (1m-diag. & 3 m-theories)

- Access controls are not the only methods to limit the unauthorized access to the system. Some new approach is to utilize something unique about the individual, like their fingerprints to identify them. The something-you-are method is known as biometrics.

- Depending on the application and objective, different "form factors" are more appropriate. The major biometric form factors today are:

1) Handprint
2) Fingerprint
3) Retina
4) Voice/speech
5) Handwriting Signature
6) Face
7) Movement patterns (i.e. typing, walking, etc)

Fingerprint:-

- Fingerprint biometrics involves a finger sixe identification sensor with a low-cost biometric chip.
- Fingerprint provides the best option for most uses of biometric verification, especially attached to specific computer and network assets.
- The relatively small size and low cost aloe them to be easily incorporated into devices and are fairly reliable.
- Many pc manufacturers are experimenting with integrating the devices either on keyboards, mice, or the actual computer case.
- Some banks are starting to implement simple fingerprint recorders to provide more security in check cashing operations. This is simply taking a snapshot of the fingerprint to aid in tracking and prosecuting check fraud.

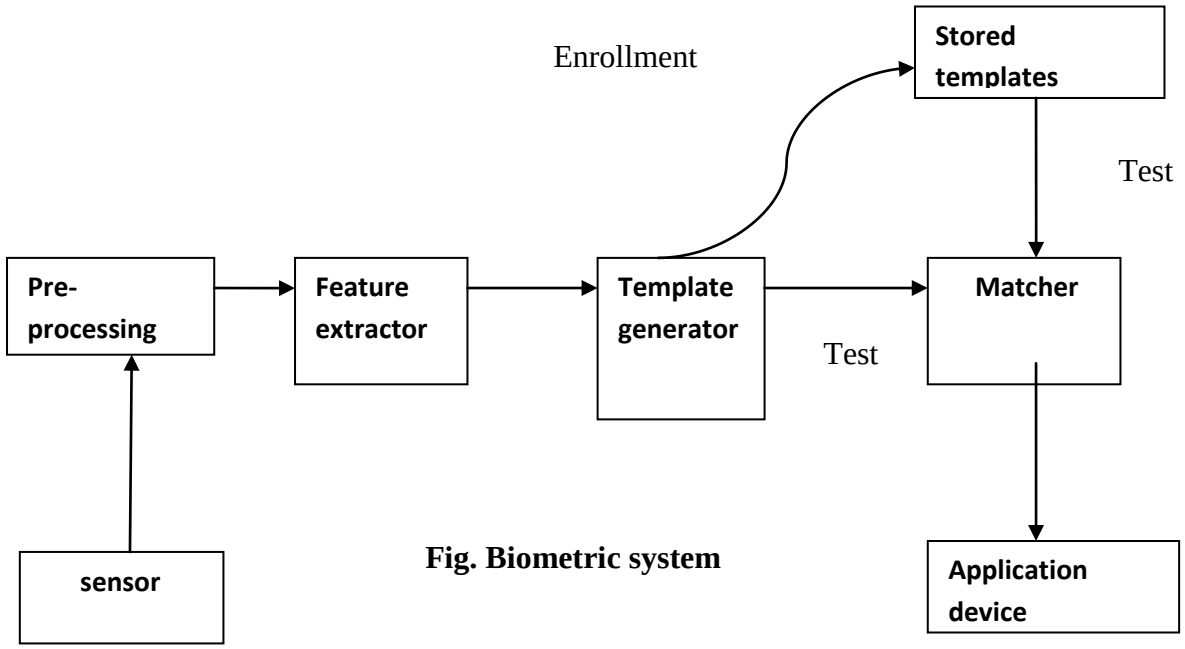
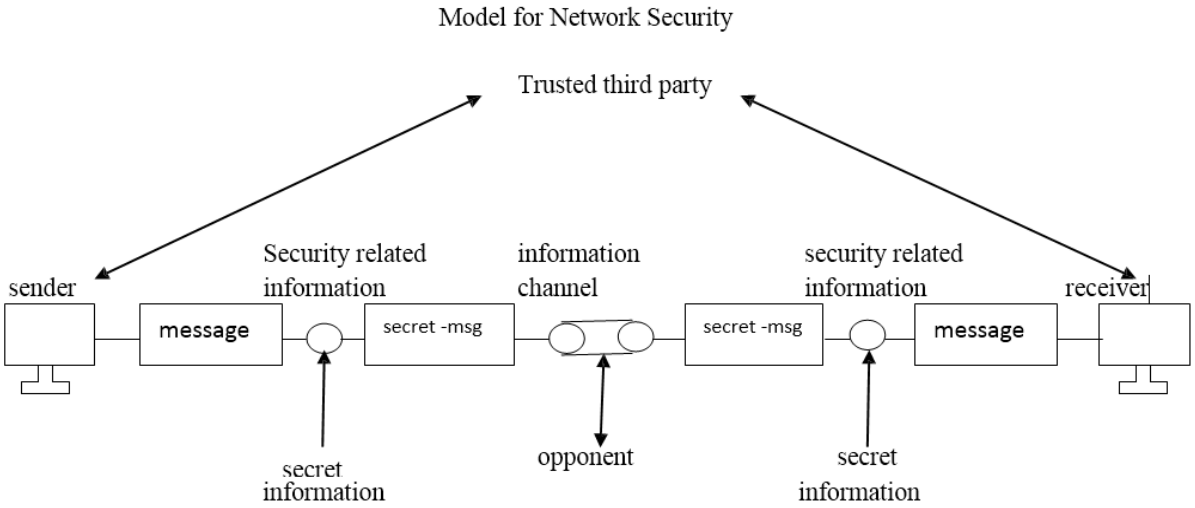


Fig. Biometric system

d) Describe the 'model for network security' and enlist its layers.

Model for Network Security: (1m-diag. & 2m-theory & 1m-listing layers)



- A message is to be transferred from one party to another via Internet.
- Sender & receiver are principals of transaction and must cooperate for exchange to take place.
- An information channel is established by defining a route through Internet from source to destination with the help of communication protocol like TCP/IP.
- Techniques for providing security have following components:-
- A security related transformation on information to be sent.
- The secret information shared by two principals should be secret.
- A trusted party is required to achieve secure transmission.
- This is responsible for distributing secret information between two principals.

Model shows four basic tasks:

1. Design algorithm in such a way that an opponent cannot defeat its purpose. This algorithm is used for security related information.
2. Generate secret information that can be used with algorithm.
3. Develop method for distributing and sharing of secret information.
4. Specify a protocol which can be used by two principals that make use of security algorithm and secret information to achieve a security service.

- **OSI Layer for security model defines seven layers (1m)**

a. Authentication
b. Access control
c. Non repudiation
d. Data integrity
e. Confidentiality
f. Availability or Assurance
g. Notarization or Signature

e) Describe Components of a good password :(1 mark for each point, any four)

1. Password should be at least eight characters in length.
2. Password should have at least three of the following four elements:
   - i. One or more upper case letters (A-Z)
   - ii. One or more lower case letters (a-z)
   - iii. One or more numerical (0to9)
   - iv. One or more special character (!, @,#,$,&,:,.,;,?)
3. Password should not consist of dictionary words.
4. Password should not at all be the same as login name.
5. Password should not consist of user's first or last name, family members name, birth dates, pet names, pin and mobile numbers.

Q.4

a) Attempt any three of the following. (12m)

i. List the basic principles of computer security. Explain any four of them in details.

Basic principles of computer security are: (1 marks for each point)

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

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.

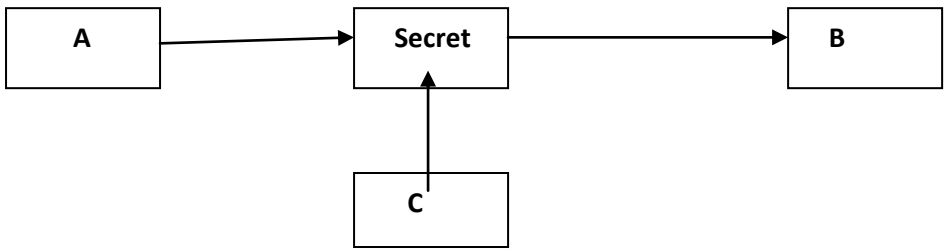


Fig. Loss of confidentiality

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.**

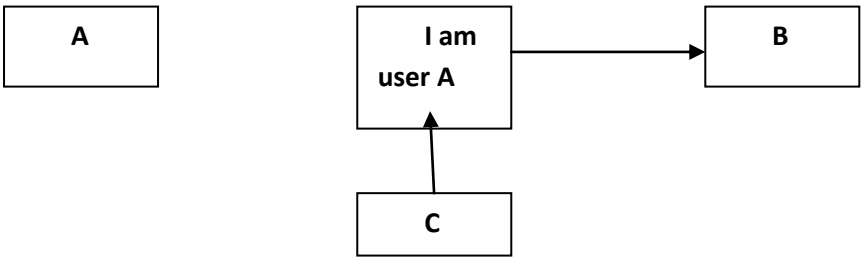


Fig. absence of authentication

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**.

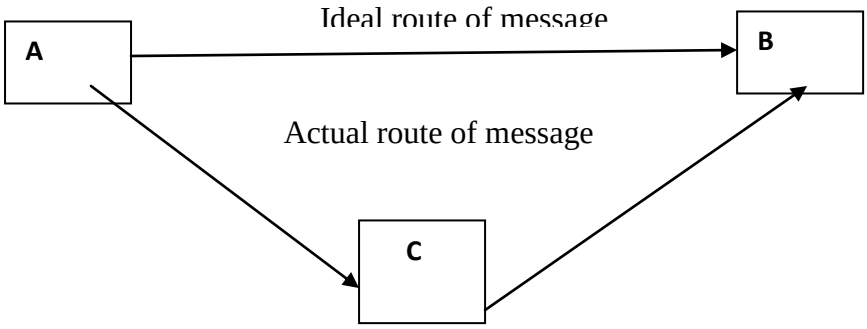


Fig. Loss of Integrity

4. Non-repudiation: there is a situation where a user sends a message and later on refuses that he had sent that message.
For example, user A could send a fund transfer request to bank B over internet. After the bank performs the funds transfer as per A's instruction, A could claim that he never sent the funds transfer instruction to bank! Thus, A repudiates or denies her funds transfer instruction. The principle of Non-repudiation defeats such possibilities of denying something, having done it.
Non-repudiation does not allow the sender of a message to refute the claim of not sending that message.

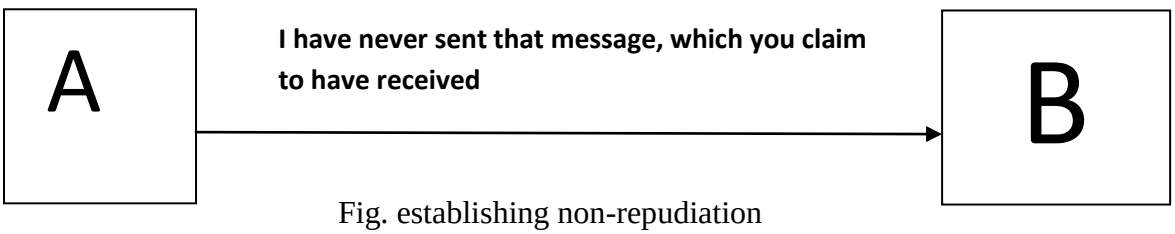


Fig. establishing non-repudiation

ii. Define following terms. (1m for each point)

1) **Snifling:** sniffing is also known as **snooping**. a network sniffer is a hardware or software device that is used to observe traffic as it passes through a network on a shared broadcast media.

   These devices can be used to view all traffic, or it can target a specific protocol, services, or even string of characters like logins.

2) **Spoofing:** spoofing is making data similar to it has come from a different source. This is possible in TCP/IP because of the friendly assumptions behind the protocols.

   There are several forms of spoofing: 1) e-mail spoofing
   2) IP address spoofing
   3) URL spoofing

3) **Worms:** a worm is similar to virus but it does not modify a program. Instead, it replicates itself again and again to target computer and makes the target computer very slow, finally coming to halt.
   A worm attack attempts to make the computer or the network under attack unusable by eating all its resources.
4) **backdoor and trapdoor:** backdoor are the methods used by the software developers to make sure that they can gain access to an application even if something were to happen in the future to prevent normal access methods.Backdoor are more commonly used to refer to programs that an attacker install after gaining unauthorized access to a system to ensure that they can have unrestricted access to the system, even if the initial access method is discovered and blocked.

5) **Trapdoors** are the bits of the code embedded in the program to quickly gain access at a later time (i.e. during testing time).

   A trap door is a secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedures. Trap doors have been used legitimately for many years by programmers to debug and test programs. Trap doors become threats when they are used by unscrupulous programmers to gain unauthorized access.

iii. Describe SSL protocol in web security.

Secure socket layer (SSL) is an internet protocol for secure exchange of information between a web browser and a web server. It provides two basic security services: authentication and confidentiality.

SSL has three sub protocols:-

1. Handshake protocol: (2m)

It is the first sub protocol used by client and server to communicate using an SSL-enabled connection.

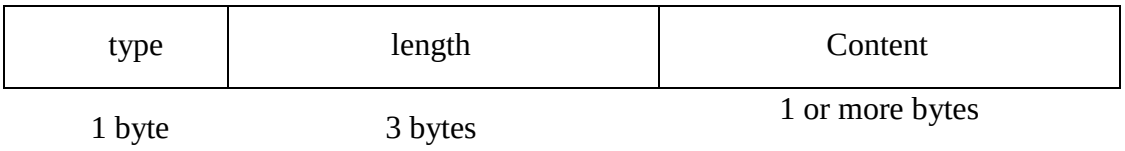


Fig. format of handshake message protocol.

As shown in the fig., each handshake message has three fields, as follows:

a) **Type:** this field indicates one of the ten possible message types. These tem message types are as follows

Message type	parameters
Hello request	none
Client hello	Version, random number, session id, cipher suite, compression method
Server hello	Version, random number, session id, cipher suite, compression method
certificate	Chain of X.509V3 certificates
Server key exchange	Parameters, signature
Certificate request	Type, authorities
Server hello done	none
Certificate verify	signature
Client key exchange	Parameters, signature
finished	Hash value

b) **Length**: this field indicates the length of the message in bytes
c) **Content**: this field contains parameters associated with this message, depending on the message type, as listed in above table.
The handshake protocol is actually made up of four phases:
1. Established security capabilities
2. Server authentication and key exchange
3. Client authentication and key exchange
4. Finish

2. Record protocol: (1m)

The record protocol in SSL comes into the picture after a successful handshake is completed between the client and server. That is after the client and server have optionally authenticated each other and have decided what algorithm to use for secure information exchange; we enter into SSL record protocol.

This protocol provides two services to an SSL connection, as follows
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.

Operations of record protocol are:

1. Application data
2. Fragmentation
3. Compression
4. Addition of MAC
5. Encryption
6. Append header

3. Alert protocol: (1m)

When either the client or server detects an error, the detecting party sends an alert message to the other party. If the error is fatal, both the parties immediately close the SSL connection.

Both the parties also destroy the session identifiers, secrets 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 connection. Instead, the parties handle the error and continue.

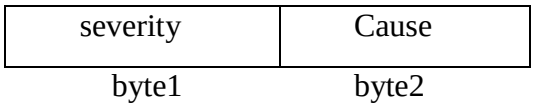


Fig. alert protocol message format

Each alert message contains two bytes. The first byte signifies the type of error. If it is a warning, this byte contains 1. If the error is fatal, this byte contains 2. The second byte specifies the actual error.

iv. Enlist threats to web security. Describe any three of them in details.

The main types of threats to web systems are listed below: **(any 3 point - 2m)**

Physical

Physical threats include loss or damage to equipment through fire, smoke, water & other fire suppressants, dust, theft and physical impact. Physical impact may be due to collision or the result of malicious or accidental damage by people. Power loss will affect the ability for servers and network equipment to operate depending upon the type of back-up power available and how robust it is.

Malfunction

Both equipment and software malfunction threats can impact upon the operations of a website or web application. All assets required for the operation of the web system must be identified to be able to evaluate the threats. Malfunction of software is usually due to poor development practices where security has not been built into the software development life cycle.

Malware

Malware, or malicious software, comes in many guises. Web servers are popular targets to aid distribution of such code and sites which have vulnerabilities that allow this are popular targets.

Spoofing

Spoofing where a computer assumes the identity of another and masquerading where a user pretends to be another, usually with higher privileges, can be used to attack web systems to poison data, deny service or damage systems.

Scanning
Scanning of web systems are usually part of network or application fingerprinting prior to an attack, but also include brute force and dictionary attacks on username, passwords and encryption keys.

Eavesdropping
Monitoring of data (on the network, or on user's screens) may be used to uncover passwords or other sensitive data.

Following table shows the type of security threats faced using the web (**2marks)**

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic Checksums
Confidentiality	• Eavesdropping on the Net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web Proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus threats • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic Techniques

B) Attempt any one of the following. (06 mark)

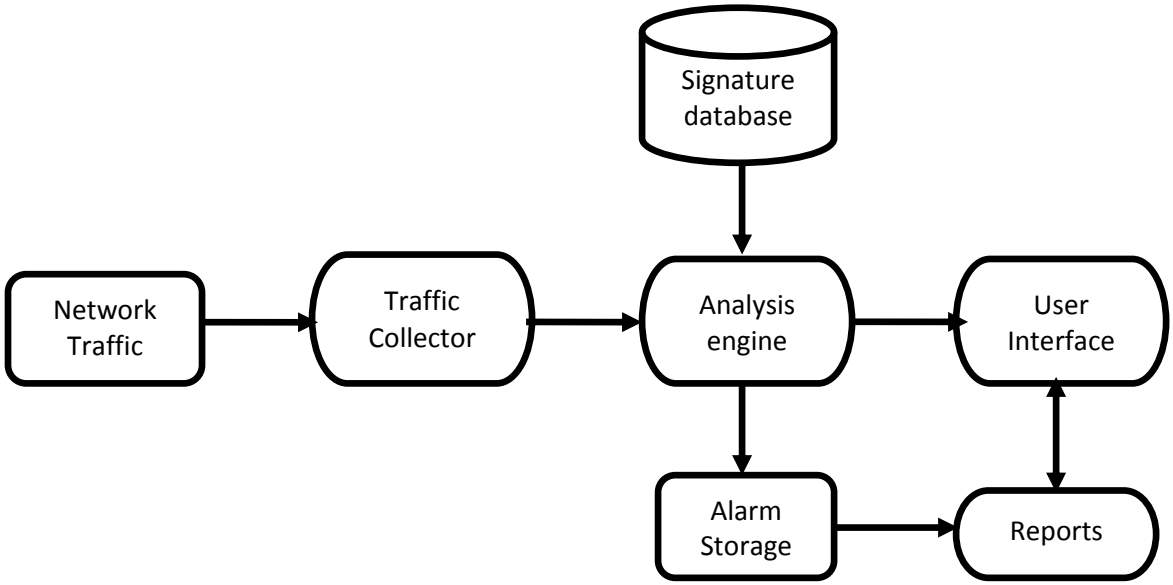
i. Describe network based IDS with neat labeled diagram.(fig- 2marks and theory- 4marks)

Network-Based IDS (NIDS)

- Network-based IDS focuses on network traffic – the bits & bytes traveling along the cables & wires that interconnect the system.
- A Network IDS should check the network traffic when it passes & it is able to analyze traffic according to protocol, type, amount, source, destination, content, traffic already seen etc.
- Such an analysis must occur quickly, & the IDS must be able to handle traffic at any speed the network operates on to be effective.
- Network-based IDSs are generally deployed so that they can monitor traffic in & out of an organization's major links like connection to the internet, remote offices, etc.
- Network-based IDSs looks for certain activities like:
    - Denial of service attacks
    - Port scans or sweeps
    - Malicious content in the data payload of a packet or packets
    - Vulnerability scanning

- Trojans, viruses, or worms
- Tunneling
- Brute-force attacks

- The logical layout of network-based IDS is shown in following Fig.



ii. Explain following terms with examples.

1) Piggy.backing
2) Shoulder surfing
3) Dumper diving
(For each point 2 marks)

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

2) **Shoulder surfing** is a similar procedure in which attackers position themselves in such a way as-to be-able to observe the authorized user entering the correct access code or data.
   Both of these attack techniques can be easily countered by using simple procedures to

ensure nobody follows you too closely or is in a position to observe your actions.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine. Shoulder surfing can also be done long-distance with the idea of binoculars or other vision-enhancing devices.
To prevent shoulder surfing, experts recommend that you shield paper work or your keypad from view by using your body or cupping your hand.

3) **Dumpster diving:-**Dumpster is diving is the process of going through a target's trash in order to find little bits of information.
In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network.
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.
To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company should establish disposal policy.

Q. 5 Attempt any Two of the following:

a) Describe IP security and authentication header mode of IP security with suitable sketch(s).

Definition: The protocol for providing security at IP level called as IP security. (IPSec)
IPSec provides the capabilities to secure communications across a LAN, across private & public WANs & across the Internet.
Advantages & applications:
Secure remote internet access:
Using IPsec, we can make a local call to our internet services provider (ISP) so as to connect to our organization network in a secure fashion from our house or hotel from there; we can access the corporate network facilities or access remote desktop/servers.

1. **Secure branch office connectivity:**
   Rather than subscribing to an expensive leased line for connecting its branches across cities, an organization can set up an IPsec enabled network to securely can't all its branches over internet.
2. **Set up communication with other organization:**
   Just as IPSec allow connectivity between various branches of an organization, it can also be used to connect the network of different organization together in a secure & inexpensive fashion.

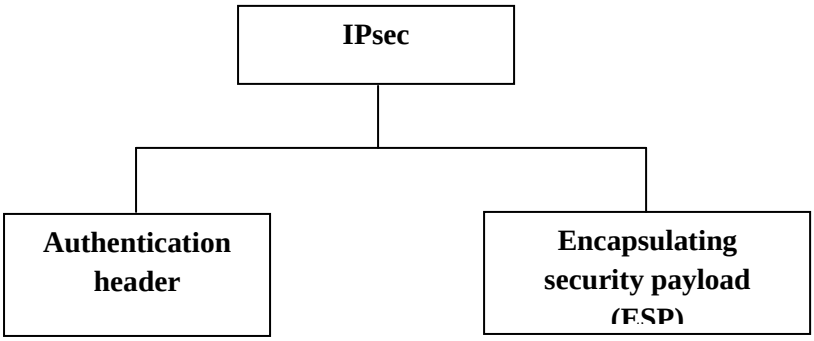
Main advantages of IPSec:

- ✓ IPsec is transparent to end users.
  There is no need for an user training key, key issuance or revocation.
- ✓ When IPsec is configured to work with firewall, it becomes the only entry-exit paint for all traffic, making it extra secure.
- ✓ IPsec works at network layer. Hence no change are needed to upper layers or router, all outgoing & incoming traffic gets protected.
- ✓ IPsec allow travelling staff to have secure access to the corporate network

- ✓ IPsec allows interconnectivity between branches/ offices in a very inexpensive manner.

Basic Concept of IPsec Protocol:

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



1. Authentication header(AH):

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

b) List the contents of digital certificate. Describe major steps of digital certificate creation. (2 marks for contents & 6 marks for steps)note: diagram is optional

1. Version number
2. Subject
3. Public key
4. Issuer
5. Serial Number
6. Validity
7. Certificate usage
8. Signature Algorithm
9. Extensions

Steps involved in obtaining digital certificate

1. The user registers for a digital certificate through a Web Based form.

2. Once all data is inserted into the form. The browser initiates key generation process. This will often require random input values (This may be acquired by Random Mouse Movements, keystrokes Or by extracting specific information from within the system itself.

3. These random values are inserted into cryptographic algorithm that used to generate a public/private key pair.

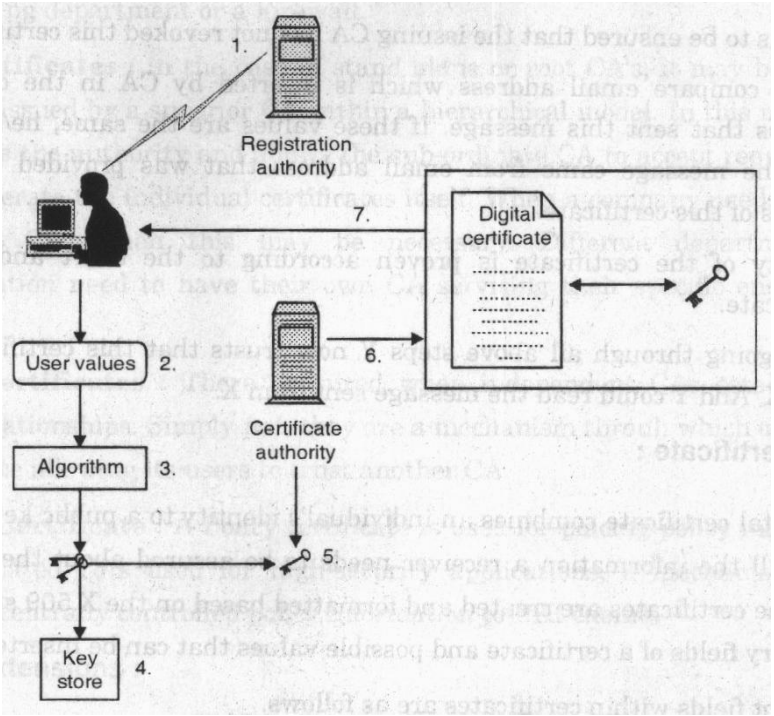
4. The key pair is stored in a key store on the workstation. If the key is being created for the first time, the application should request a password from the user that will be used to access and use the keys.

5. The public key is attached to the certificate registration form and both are forwarded to the RA (Registration Authority) for processing. HA is only responsible for Registration process. Once

RA is done with his processing copy of the public key and other identifying information is sent to the CA (Certificate Authority).

6. The CA generates the Digital Certificate containing the public key and the other identifying information.

7. The new certificate is sent to the user.



c) Describe E-mail security in detail. (2 marks for initial explanation & 2 marks for explanation of any 3 protocols)

E-mail (Electronic mail) is widely used application on the internet.

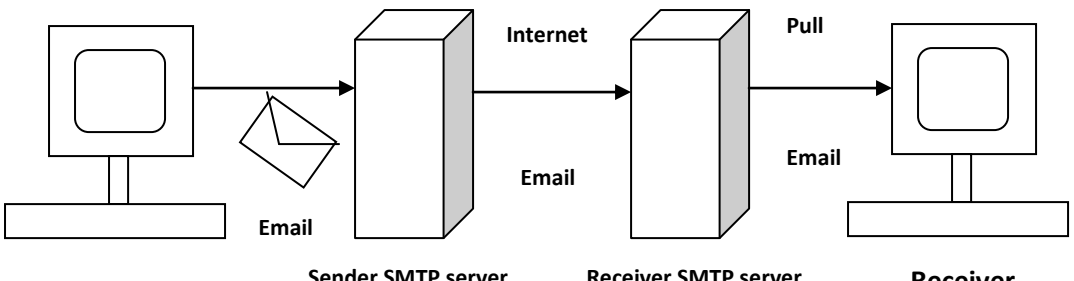
User using Email, user can send a text messages, pictures , videos & sounds

Now a day's security of Email messages has become extremely important issue.

To provide E-mail security some following Email protocols are used: 1) SMTP 2) PEM 3) PGP 4) S/MIME

SMTP- Simple Mail Transfer Protocol is used for email communication SMTP is "request/response" based, which means email send from client to server.

This server actually transfers messages to receiver's SMTP sever. SMTP's mail job is carry email message between sender & receiver.



- Email communication consists of following steps.
- At the sender's end, an SMTP server takes messages by user computer.
- At the sender's end the SMTP sever at the sender's then transfer's message to SMTP server of receivers.
- The receivers computer drags the email message from SMTP server at the receiver's end, using POP (post office protocol) or IMAP (Internet Mail Access Protocol)

Pop is post office protocol is built like SMTP, but POP is used only to retrieve email. It uses plain text to communicate & it SMTO answer/ reply mechanism.

PEM (Privacy Enhanced Mail)

PEM supports three main cryptographic functions of encryption, non-repudiation & integrity.

PEM operation:

1. Canonical conversion
2. Digital Signature
3. Encryption
4. Base 64 Encoding

Step 1: Canonical conversion PEM transforms each email message into an abstract, canonical representation means email message into an abstract, canonical representation means email message travels in a uniform, independent format.

Step 2: Digital Signature – In this step it starts by creating message digest using algorithm MD2 or MDS & created message encrypted with senders private key to form digital signature.

Step 3: Here original email & digital signature are encrypted with symmetric key for this DES or DES-3 algorithm is used.

Step 4: Base -64 Encoding: This process transforms arbitrary binary input into printable character.

over Internet using keys.

PGP

PGP is a popular program used to encrypt & decrypt e-mails over the Internet.

- It can also be used to send an encrypted digital signature that lets the receiver verify the sender's identity & know that the message was not changed in route.

PGP is the most widely used privacy-ensuring program by individuals & is also used by many co-operations.

- Developed by Phillip R. Zimmermann in 1991.
- PGP can also be used to encrypt files being stored so that they are unreadable by other users or intruders.

How it works?

1. **Authentication:**
   - The sender creates a message.
   - SHA -1 is used to generate 160 bit hash code of the message .
   - The Hash code is encrypted using sender's private key & result is pretended to the message.
   - The receiver uses sender's public key to decrypt & recover the hash code.
   - The receiver generates a new hash code for the message & compares it with the decrypted hash code. If match is found then the message is accepted as authentic.

2. Confidentialty:

- Another basic service provided by PGP is confidentiality , which is provided by encrypted message to transmitted or to be stored locally as file.
- The sender generates a message & a random 128 bit number to be used as session key for this message only.
- The message is encrypted with session key.
- The session key is encrypted using the recipients public key & is pretended to the message .
- The receiver with its private key to decrypt & recover the session key.
- The session key is used to decrypt message.

SECURE MULTIPURPOSE INTERNET MAIL EXTENSION (S/MIME):

The traditional email system using the SMTP protocol are text based ,which means that a person can compose a text message using an editor & then send it over internet to another recipient . However, in modern era, exchanging only text message is not quite sufficient.
People want to exchange multimedia files, document in various arbitrary format, etc.
To cater these, the Multipurpose Internet Mail Extensions (MIME) system extends the basic email system by permitting users to send binary files using the basic email system.

- A MIME email message contains a normal Internet text message along with some special headers & formatted sections of text.
- Each such a section can hold an ASCII – encoded portion of data. Each section starts with an explanation as to how the data flows should be interpreted/decoded at the recipients' send. The recipient's email system uses this explanation to decode the data.
- When we enhance the basic MIME system to provide security features ,it is called as Secure Multipurpose Internet Mail Extensions(S/MIME)
- S/MIME provides the following cryptographic security services for electronic messaging applications: Authentication, Message Integrity & non-repudiation of origin & privacy & data security.

S/MIME functionality:

S/MIME is quite similar to PGP, similar to PGP, similar to PGP S/MIME provides digital signature & encryption of email message. S/MIME prefers the usage of the following cryptographic algo.

- For digital signatures- Digital Signature Std.(DSS)
- For encrypting the symmetric session keys- Diffie –Hellman
- For either digital signature or for encrypting the symmetric session keys- RSA
- For symmetric key encryption – DES-3

S/MIME process the email message along with the other security related data , such as the algorithms used & digital certificates to produce what is called as "Public Key Cryptography Standard (PKCS) Object"

Q.6. Attempt any four of the following:

a) Enlist any four consequences when the system is accessed by non- employee.

1. If an attacker can get physical access to system then there are many chances of obtaining enough information to enter into computer systems & networks.
2. If the organization does not impose good password policies then password & important information can be attacked.
3. Physical access provides an easy opportunity for user to look for the infrequent piece of critical information carelessly left out.
4. The devices like cell phones with built-in cameras, an individual can easily take a photograph of information without being understandable to employees.

b) List and explain various security topologies. (1 mark for listing ,Explanation of any two points ,each carry 1 1/2 marks)

Security topology is a logical map that depicts the interconnectivity between security devices and security domains that host these networks.

list:

1. security zones
2. DMZ
3. Internet
4. Intranet
5. VLAN
6. Security Implication
7. Tunnelling

Internet explorer includes five predefined zone: Internet, local Intranet, trusted sites, restricted sites & my computers

1) **Types of security zone**

1. Internet zone

This zone contains web sites. These sites are not on your computer or on your local internet or that are not already assigned to another zone. The default security level is medium.

2. Local Internet zone

By default, the local internet zone contains all network connection that were established by using a universal naming convention (UNC) path example: http:// local. The default security level for local internet is set to medium.

3. Trusted sites zone

- This zone contains web sites that you trust as safe
- When you add web sites to trusted sites zone, you believe that files you download or that you run from the web sites will not damage your computer r data.
- But there are no web sites that are assigned to trusted site zone. So security level is set to low.

4. Restricted site zone:

This zone contains web site to restricted sites zone, you believe that you download or run from website may damage your computer or your data. By default, there are no web sites that are assigned to restricted sites zone & security level is high. The restricted sites zone contains web sites that are not on your computer or on your local internet. The default security zone is medium.

2) DMZ:

In computer network, a DMZ (demilitarized zone) is a computer host or small network inserted as "neural zone" between company's private network & outside network.

It prevents outsider servers from getting direct access to server.

In a typical DMZ configuration for a small company, a separate computer or host in network term receives request from users within private network for access to web sites or other companies accessible on public network.

3) Internet:

Internet is network that can be used to transfer email, financial record, files, remote access etc. from one network to another.

- Internet is not a single network.
- Such a large mesh allows that user infinite ability to communicate between different systems.
- Everyone can have access to this network so it is somewhat difficult to impose computer security policies, so it is considered as un-trusted as un-trusted system.
- www term is frequently used with internet. It is HTTP based service; this can have different actual service & includes files, images, audio, video & even viruses & worms.

4) Intranet:

Intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area & also use leased lines in the wide area network.

Typically, an intranet includes connections through one or more gateway computers to the outside Internet.

The main purpose of intranet is to share company information & computing resources among employees.

An intranet can also be used to facilitate working in groups & for teleconferences.

An intranet uses TCP/IP,HTTP, and other internet protocol.

5) VLAN : Virtual local area network are method of using a single switch & dividing it into multiple broadcast domain and/or multiple broadcast domain and/or multiple network segments.

VLAN technology also allows having several VLANs over single switch in such a manner that all the LANs will operate in parallel & may not even aware of each other.

TYPES:

1. Port based VLANs
2. MAC based VLANs
3. Protocol Based VLANs
4. IP subnet Based VLANs

c) State meaning of following terms.

i. Hot fix
ii. Updates
iii. Patch
iv. Service pack

(Each point carries 1 mark)

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

Updates: User or system administrator is constant stream of updates designed to correct problems, replace sections of code, or even add new features to an installed operating system .

It includes following s/w updates: 1.Hotfix 2.Patch 3.Service pack

Patch: This term is generally applied to more formal, larger s/w updates that may address several or many s/w problems.

Patches often contain improvement or additional capabilities & fixes for known bugs.

Service pack:

Usually this term is given to a larger collection of patches & hot fixes that are rolled into a single ,rather large package.

Service packs are designed to bring a system up to the latest known, good level all at once ,rather than requiring the user or system administrator to download several of updates separately.

d) Explain the following.

i. Hashing

ii. Stagnography

(Each point carries 2 marks)

i. **Hash function**: A hash functions are one of the most commonly used encryption methods.

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

A hash value his generated by a function H of the form

h=H(M)

where M is variable length message & H(M) is the fixed length value.

ii. **Steganography:** Steganography is a technique of hiding a secret message within an ordinary message & the extraction of it at its destination.

Steganography takes cryptography a step further by hiding an encrypted message so that no one suspects it exists.

In modern digital steganography, data is first encrypted & then inserted using special algorithm ,into redundant data that is part of particular file format such as JPEG image.

Steganography has number of drawbacks like as it requires a lot of overhead to hide a relatively few bits of information.

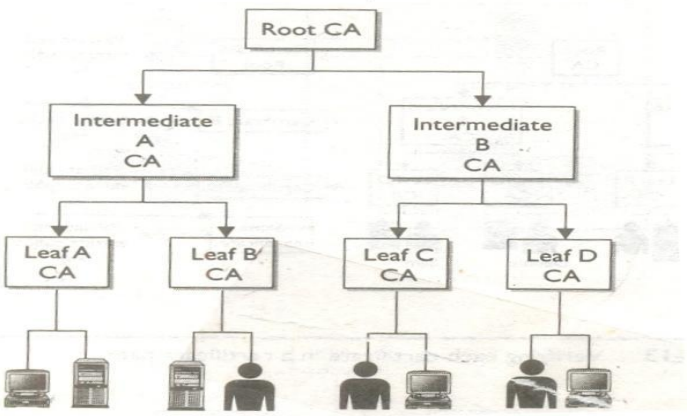
Once system is discovered ,it becomes worthless.

Alternative for this is ,first encrypt the message & then hide using steganography.

e) State and explain any two trust models. (1 mark for definition & 1 1/2 mark for each model , Any two model)

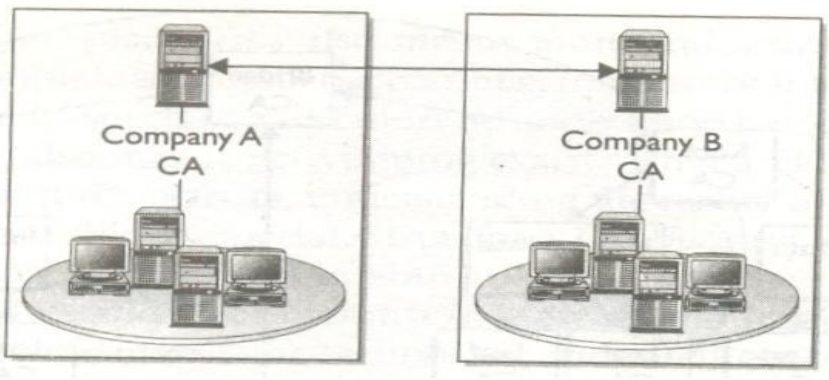
A trust model is a construct of system, personnel, applications, protocols, technologies & policies that work together to provide a certain level of protection.

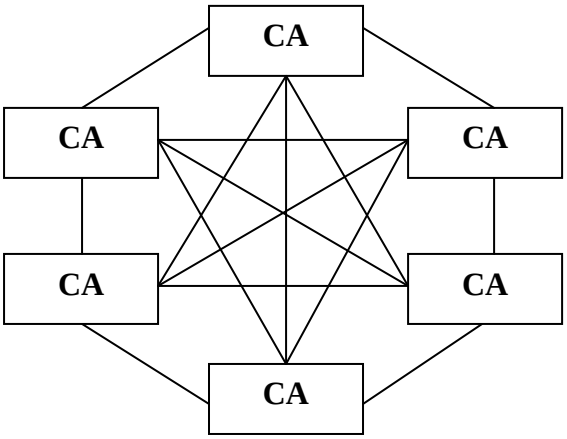
Hierarchical Model:



In Hierarchical structure contains a root CA, intermediate CAs & end-entities. The configuration is that of an inverted tree as shown in fig. The root CA is trust anchor for all other entities in this infrastructure & it generates certificates for the intermediate CAs ,which in turn generate certificates for the leaf CAs,& the leaf CAs generate certificates for end-entities like as users ,network devices, applications. As shown in diagram there is no bidirectional trust-they are all unidirectional trusts as indicated by one-way arrow. Since no other entity can certify & generate certificates for the root CA. It creates a self-signed certificate. This means that the certificate issuer & subject fields hold the same information, both representing the root CA & root CA‟s public key is what will used to verify this certificate when that time comes.
This root CA certificate & public key is distributed to all entities within this trust model.

Peer to Peer trust model:
In Peer-to-Peer trust model one CA is not subordinate to another CA & there is no established trusted anchor between the CAs involved. Fig. illustrates peer-to-peer trust model. The two different CAs will certify the public key for each other, which creates a bidirectional trust. This is referred to as cross certification, since the CAs are not receiving their certificates & public keys form superior CA, but instead they are creating them for each other. Main drawback of this model is scalability. Each CA must certify every other CA that is participating & bidirectional trust path must be implemented as shown in Figure. -Figure represents a fully connected mesh – architecture that each CA is directly connected to & has a bidirectional trust relationship with every other CA.





Hybrid Trust model:

In companies when there is need arises of properly communication with outside partners , suppliers and customers in an authorized & secured manner, it can be difficult to use either the hierarchical or peer to peer trust model.The different model types have to be combined in many implementations to provide the level of trust & necessary communication lines.

In a hybrid trust model, the two companies have their own internal hierarchical models and are connected through a peer-to-peer model using cross certification.

The other option in hybrid configuration is implementation of a bridge CA as shown in fig.

The role of bridge CA is, it is responsible for cross-certificates for all connected CAs & trust domains. The bridge is not considered as a root or trust anchor, but just entity that generates & maintains the cross certification for the connected environments.