Q.1(a) Attempt any THREE of the following : [12]

Q.1(a) (i) Describe the basic principles of computer security. [4]

Ans.: The need of computer security has been threefold: confidentiality, integrity, and availability the "CIA" of security. Confidentiality, Integrity, Availability, Availability, Authentication, Other elements are Authorization, Non-repudiation, Access control and accountability.

(i) Confidentiality

The goal of confidentiality is to ensure that only those individuals who have the authority can view a piece of information, the principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message.

Example of compromising the Confidentiality of a message is shown in fig.

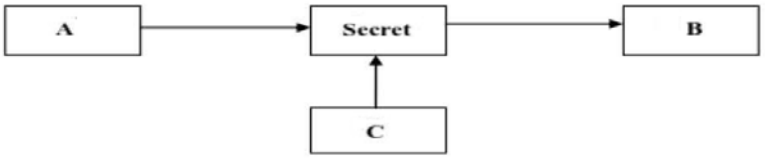


Fig.: Loss of confidentiality

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

(ii) Authentication

Authentication helps to establish proof of identities. The Authentication process ensures that the origin of a message is correctly identified. Authentication deals with the desire to ensure that an individual is who they claim to be. For example, suppose that user C sends a message over the internet to user B. however, the trouble is that user C had posed as user A when he sent a message to user B. how would user B know that the message has come from user C, who posing as user A?

This concept is shown in fig. below.

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

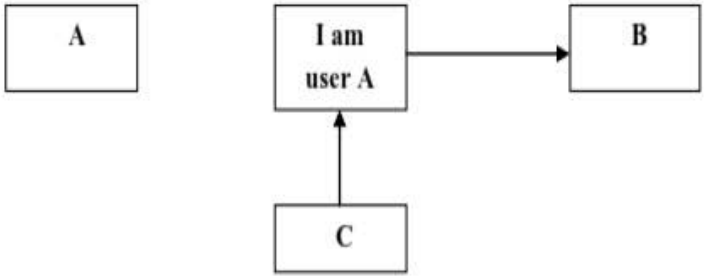


Fig.: Absence of authentication

(iii) Integrity

Integrity is a related concept but deals with the generation and modification of data. Only authorized individuals should ever be able to create or change (or delete) information. When the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.

For example, here user C tampers with a message originally sent by user A, which is actually destined for user B. user C somehow manages to access it, change its contents and send the changed message to user B. user B has no way of knowing that the contents of the message were changed after user A had sent it. User A also does not know about this change.

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

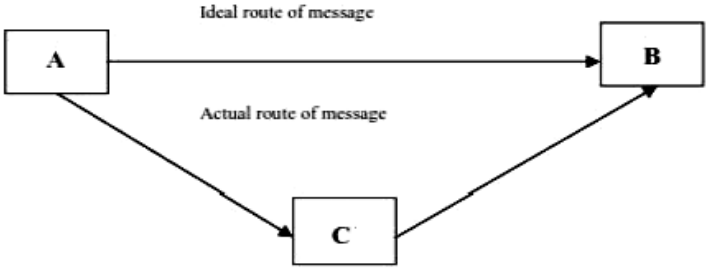


Fig.: Loss of Integrity

(iv) Availability

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

Q.1(a) (ii) What is shoulder surfing? How it can be prevented? **[4]**

Ans.: **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.

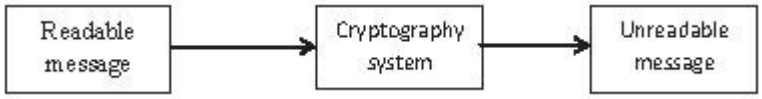
Q.1(a) (iii) Compare symmetric and asymmetric key cryptography. **[4]**

Ans.:

Sr. No.	Symmetric Encryption	Asymmetric Encryption
(i)	If the same key is used for encryption and decryption, the encryption is called as Symmetric Key Encryption.	If two different keys are used in cryptographic mechanism, wherein one key is used for encryption and another, different key is used for decryption; such encryption is called as Asymmetric Key encryption.
(ii)	Speed is fast.	Slower in speed.
(iii)	Size of cipher text is usually the same or less than that of the plain text.	Cipher text size is usually greater than that of the plain.
(iv)	Number of keys used is the square of the number of participants.	Number of keys used is same as the number of participants.
(v)	Key exchange is a major problem (hence, algorithms like the Diffie-Hellman Key Exchange algorithm are used).	Key exchange is no problem.
(vi)	More storage space required.	Less storage space required.

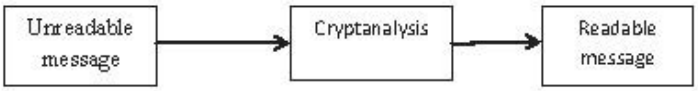
Q.1(a) (iv) Explain the terms : Cryptography, Cryptanalysis and Cryptology. [4]

Ans.: (i) Cryptography: Cryptography is art & science of achieving security by encoding messages to make them non-readable.



(ii) 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.

(iii) Cryptology: It is originated from the Greek logos, means hidden words. This technique is used in cryptography for generating secured information.

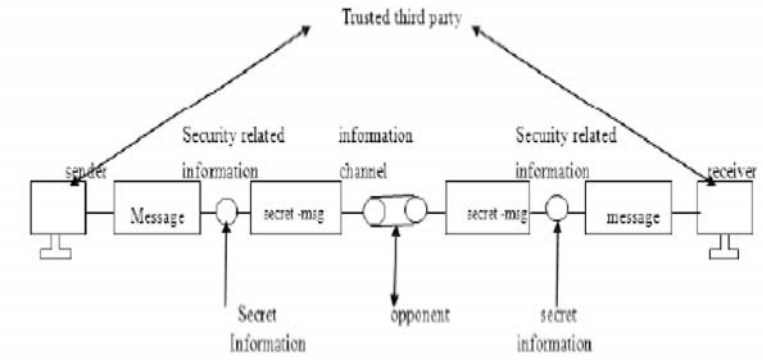


Q.1(b) Attempt any ONE of the following : [6]

Q.1(b) (i) Describe with the neat diagram model for security. [6]

Ans.:

OR



A message is to be transferred from one use to another user in secret form using this security system it can be two or more parties accessing information via Internet. Sender & receiver are principals of transaction and must cooperate for exchange to take place.

Model shows four basic tasks:

(i) Design algorithm in such a way that an opponent cannot defeat its purpose. This algorithm is used for security related information.

(ii) Generate secret information that can be used with algorithm.

(iii) Develop method for distributing and sharing of secret information.

(iv) Specify a protocol which can be used by two principals that make use of security algorithm and secret information to achieve a security service. An information channel is established by defining a route through Internet from source to destination with the help of communication protocol like TCP/IP or using normal PC to PC communication through any media.

Techniques for providing security have following components:

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

OR

Model for security:

(i) 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 Confidentially of a message is shown in figure.

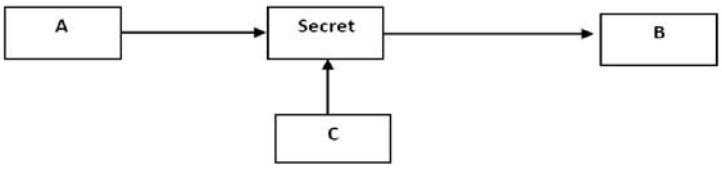


Fig.: Loss of confidentiality

- 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.

(ii) 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.

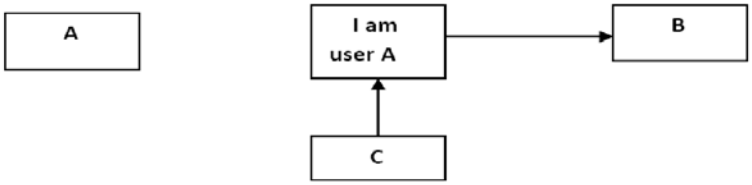


Fig.: Absence of authentication

(iii) 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.

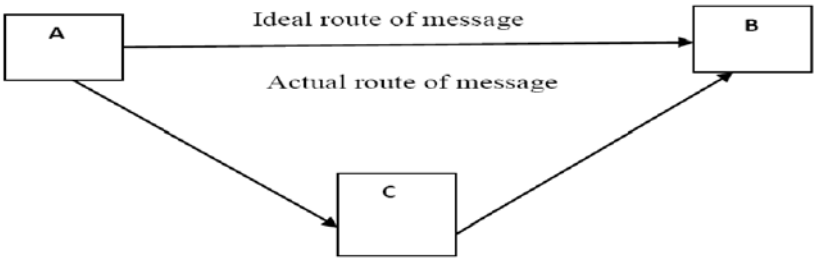


Fig.: Loss of Integrity

Q.1(b) (ii) Explain data recovery tools and data recovery procedures. [6]

Ans.: Following are the reasons why data recovery through software applications is the easiest way to recover the lost files.

- Data recovery softwares are easily available online.
- It provides help by video tutorials.
- It has user friendly, self-explanatory interface.
- It requires less memory.
- Many data recovery applications are compatible with all major operating systems.
- Several data recovery software applications are offering free trials.
  As a demand of data recovery software, a sequence of such softwares was released to search and recover lost data like :
  (i) NTFS data recovery tool
  (ii) FAT data recovery tool
  (iii) Digital camera data recovery tool
  (iv) Removable media data recovery tool
  (v) Memory card data recovery tool
- Data recovery software works by scanning the storage device for lost file systems, specific file types and specific signatures in deleted files.
- Once scanning is complete, the application prompts the user for available recovery options and it tells that the file has not been overwritten. So the accidently deleted files or data lost due to formatting, can be recovered through software applications.
- If a file or data was lost due to malware or virus infection, there are two possibilities.
  - If the virus overwrote the files with other data, then parts of the file or the whole file may be lost.
  - If the virus/malware simply erased data, the data is still there, but inaccessible through ordinary means.
- In these cases, removing the virus should be the first priority, however, it is better if the virus removal is done through a live disk of installation of antivirus software onto the storage device. Still there is a necessity to install something and then do it on a separate partition.
- File recovery also depends a lot on the file system in the storage device. NTFS is considered by experts to have the highest chance of data recovery.
- FAT provides average chances of data recovery and UFS provides low chances.

When the file is lost due to any reason, the following tips will come in handy

(i) System Admin : in case if PC is on a network, then admin may have backups or copies of files. Some organizations refers backup periodically, so there may still be a chance of avoiding the file recovery processes and gaining a copy of the file.

(ii) Disk Recovery tool : if a partition is lost or a disk has been rendered inaccessible, it needs to be brought back to working condition before data can be recovered. Lost file recovery through data recovery software can only work if the disk is accessible and in working condition.

(iii) Disk Image : Create a disk image and save it on a separate device so that it is possible to recover files from that image. There are several free software utilities available

online that can help to create a disk image. Create a disk image, put it on a separate device and run the data recovery software on it.

(iv) Save recovered files at different location : if the multiple files are recovered and saved on the same location it means overwriting lost data. If a disk image is created prior to running data recovery software, it can minimize the risk of accidental over-writing.

Q.2 Attempt any TWO of the following : [16]

Q.2 (a) Explain threat to security in detail w.r.t. virus, worms, intruders, insiders. [4]

Ans.: Threats create vulnerabilities in computer system or network.

Following are threats to security.

(i) Virus & worms
(ii) Intruders
(iii) Insiders
(iv) Criminal organization
(v) Terrorists
(vi) Information warfare
(vii) Avenues of attack
(viii) Steps in attack

Virus

Computer Virus attach itself to a program or file enabling it to spread from one computer to another, leaving infection as it travels from PC to PC or over network. It copies itself into previously uninfected programs or files, and executes over other source of attack. It can cause the loss or alteration of program or data and can compromise confidentiality. It is almost attached with executable files,

Steps are:

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

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

Worms:

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

Intruders :

- Extremely patient as time consuming More dangerous than outsiders
- Outsiders Insiders
- Keep trying attacks till success As they have the access and knowledge to cause immediate damage to organization
- Individual or a small group of attackers.
- Next level of this group is script writers, i.e. Elite hackers are of three types: Masquerade, Misfeasor, Clandestine user is misuse of access given by insiders directly or indirectly access the organization.
- They may give remote access to the Organization
- Intruders are authorized or unauthorized users who are trying access the system or network.
- They are hackers or crackers

- Intruders are illegal users.
- Less dangerous than insiders They have to study or to gain knowledge about the security system
- They do not have access to system.
- Many security mechanisms are used to protect system from Intruders.

Insiders:

- More dangerous than outsiders As the have the access and knowledge to cause immediate damage to organization
- They can be more in numbers who are directly or indirectly access the organization.
- They may give remote access to the organization.
- Insiders are authorized users who try to access system or network for which he is unauthorized.
- Insiders are not hackers.
- Insiders are legal users.
- More dangerous than Intruders.
- They have knowledge about the security system.
- They have easy access to the system because they are authorized users.
- There is no such mechanism to protect system from Insiders.

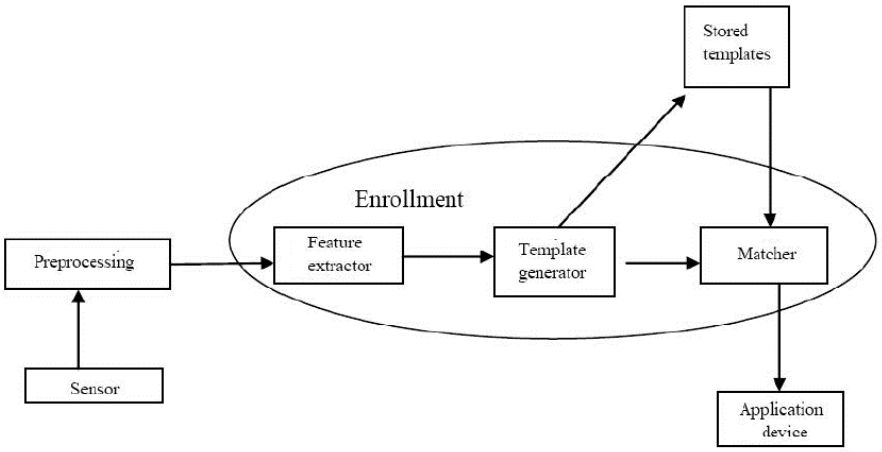
Insiders are more dangerous than intruders because:

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

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

Q.2 (b) Describe Biometric security mechanism with suitable diagram. [4]

Ans.:



- **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 enrolment, 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. Preprocessing
  2. Sensor
  3. Feature extractor
  4. Template generator
  5. Matcher
  6. Stored templates
  7. Application device
  8. Enrolment

Step 1 : The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data.

Step 2 : The 2nd block performs all the necessary preprocessing.

Step 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.

Step 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.

List of various biometrics used for computer security:

- Finger print
- Hand print
- Iris scan
- Face recognition
- DNA recognition
- Voice pattern
- Signature recognition
- Keystrokes

Example:

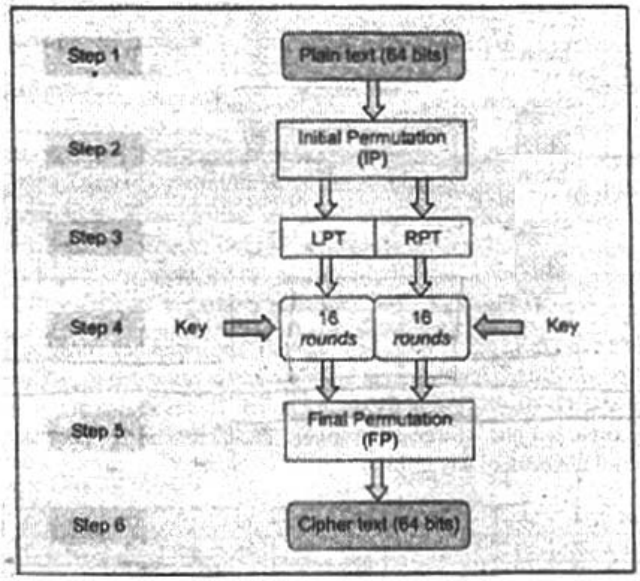
Fingerprint registration & verification process

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

Q.2 (c) Describe DES Algorithm with suitable diagram. [4]

Ans.: 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.

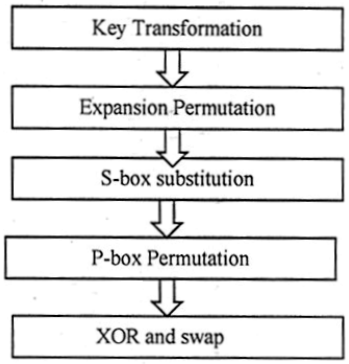
The process diagram as follows :



Explanation of each step

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

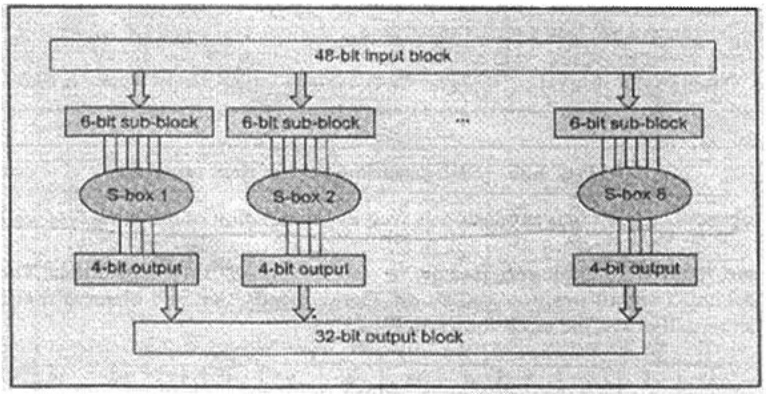


Step 1 : key transformation: the initial key is transformed into a 56-bit key by discarding every 8th bit of initial key. Thus, for each round, a 56 bit key is available, from this 56-bit key, a different 48-bit sub key is generated during each round using a process called as key transformation.

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.

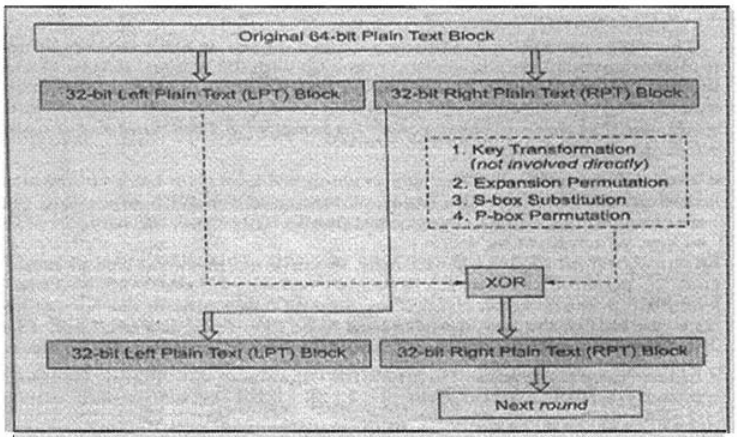
Each 4-bits block of the previous step is then expanded to a corresponding 6-bit block, per 4-bit block, 2 more bits are added. They are the repeated 1st and 4th bits of the 4-bit block. The 2nd and 3rd bits are written as they were in the input. The 48 bit key is XORed with the 48-bit RPT and the resulting 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.



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.

Q.3 Attempt any FOUR of the following : [16]

Q.3 (a) Explain the concept of Kerberos. [4]

Ans.: Kerberos is a network authentication protocol. This is developed by MIT. It's taken from mythology; Kerberos was a three headed dog who guards gates of Hades. It is secure method for authentication of request for a service in a computer network. It provides strong authentication for client/server application by using secret-key cryptography. From Kerberos allows a user request an encrypted "Ticket" from an Authentication process that can be used to request a particular service from server. The user password does not have to pass through the network.

It Consists of:

- User
- Authentication service and
- Ticket granting server
- Service server

Working of Kerberos:

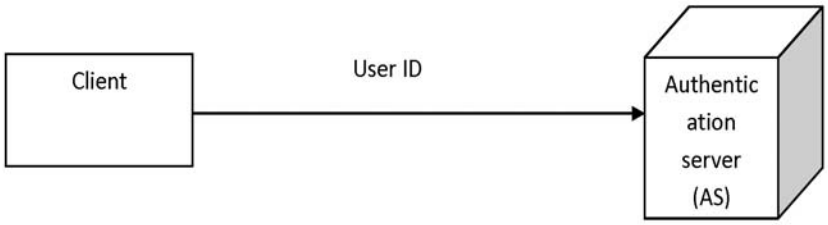
User want to access server, it needs a Kerberos ticket before request.

- Request Authentication from request Authentication server (AS), It creates "session key encryption key "based on your password, its effectively a Ticket-granting ticket.

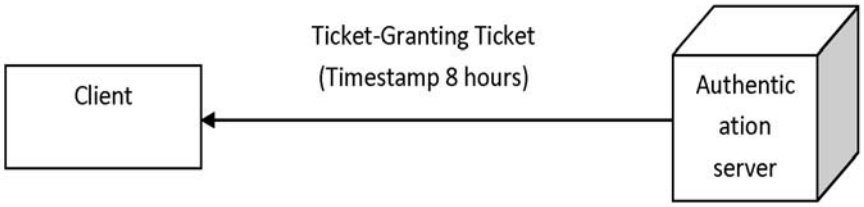
- User sends his/her ticket granting ticket to ticket granting server(TGS), it may be physically same server as Authentication server, Now TGT returns the ticket that can be sent to the server for the requested service.
- The service rejects the ticket or accepts it to perform service.
- Ticket received from TGT is a Time-stamped, It allows user to make additional request using same ticket within a certain time period without re-authentication. This improves security as ticket is granted for limited time period.

Diagrams

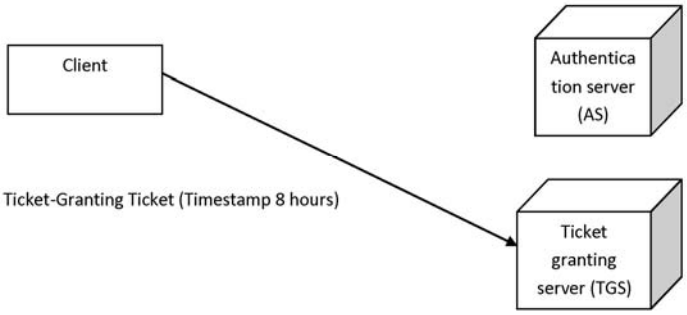
(i) Authentication service receives the request by client and verifies that the client is indeed the authentic computer. It's valid for time-stamp allotted (i.e. 8 hours).



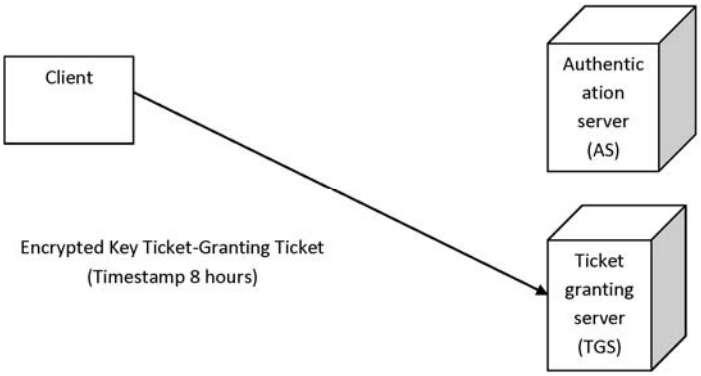
(ii)



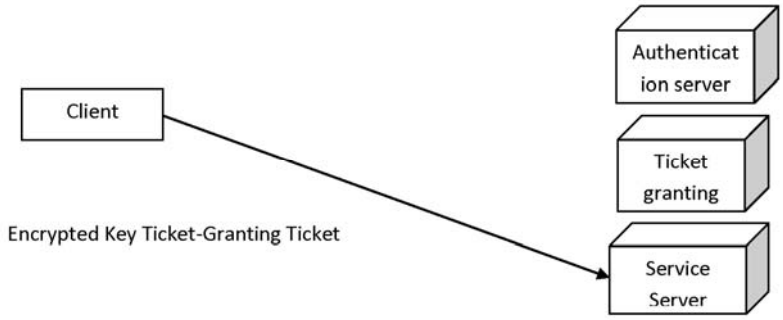
(iii)



(iv)



(v)



(vi)

Q.3 (b) Describe different password selection criteria. **[4]**

Ans.: **Password:** Password is a secret word or expression used by authorized persons to prove their right to access, information, etc.

Components of good password:

(i) It should be at least eight characters long.
(ii) It should include uppercase and lowercase letters, numbers, special characters or punctuation marks.
(iii) It should not contain dictionary words.
(iv) It should not contain the user's personal information such as their name, family member's name, birth date, pet name, phone number or any other detail that can easily be identified.
(v) It should not be the same as the user's login name.
(vi) It should not be the default passwords as supplied by the system vendor such as password, guest, and admin and so on.

Policies for Password selection:

User education

Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords. This user education strategy is unlikely to succeed at most installations, particularly where there is a large user population or a lot of turn over. Many users will simply ignore the guidelines. Others may not be good judges of what is a strong password. For example, many users believe that reversing a word or capitalizing the last letter makes a password un-guessable.

Computer-generated passwords

Passwords are quite random in nature. Computer-generated passwords also have problems. If the passwords are quite random in nature, users will not be able to remember them. Even if the password is pronounceable, the user may have difficulty remembering it and so be tempted to write it down. In general, computer-generated password schemes have a history of poor acceptance by users. FIPS PUB 181 defines one of the best-designed automated password generators. The standard includes not only a description of the approach but also a complete listing of the C source code of the algorithm. The algorithm generates words by forming pronounceable syllables and concatenating them to form a word. A random number generator produces a random stream of characters used to construct the syllables and words.

Reactive password checking

A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user. This tactic has a number of drawbacks. First it is resource intensive, if the job is done right. Because a determined opponent who is able to steal a password file can devote full CPU time to the task for hours or even days an effective reactive password checker is at a distinct disadvantage. Furthermore, any existing passwords remain vulnerable until the reactive password checker finds them.

Proactive password checking

The most promising approach to improooved password security is a proactive password checker. In this scheme, a user is allowed to select his or her password. However, at the time of selection, the system checks to see if the password is allowable and if not, rejects it. Such checkers are based on the philosophy that with sufficient guidance from the system, users can select memorable passwords from a fairly large password space that are not likely to be guessed in a dictionary attack. The trick with a proactive password checker is to strike a balance between user acceptability and strength. If the system rejects too many passwords, users will complain that it is too hard to select a password. If the system uses some simple algorithm to define what is acceptable, this provides guidance to password crackers to refine their guessing technique. In the remainder of this subsection, we look at possible approaches to proactive password checking.

Q.3 (c) List types of firewall. Explain packet filter with diagrams. [4]

Ans.: (i) Packet filtering firewall

- A packet filter applies a set of rules to each packet and based on the outcome, decides to either forward or discard the packet. It is also called as screening router or screening filter.
- Such a firewall implementation involves a router, which is configured to filter packets going in either direction. The filtering rules are based on a number of fields in the IP and TCP/UDP headers, such as source and destination IP addresses, IP protocol field, TCP/UDP port numbers (which identify the application which is using this packet, such as email, file transfer or WWW).

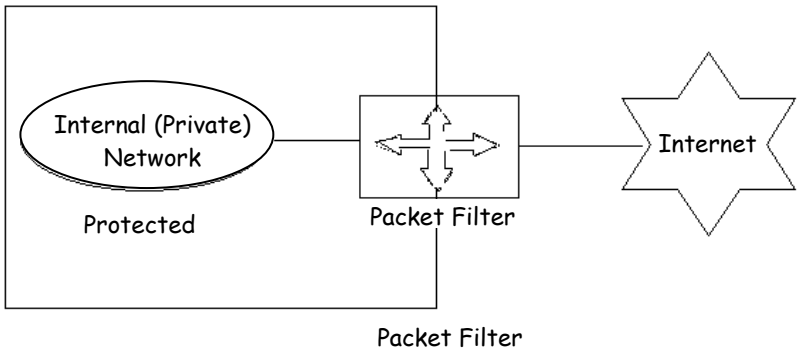


Fig.: 1

- Conceptually, a packet filter can be considered as a router that performs three main actions.
  (i) Receive each packet, (ii) Apply rules,
  (iii) If no rules, apply default rules.
- A packet filter performs the following functions :
  (i) Receive each packet as it arrives
  (ii) Pass the packet through a set of rules, bases on the contents of the IP and transport header fields of the packet. If there is a match with one of the set of rules, decide whether to accept or discard the packet based on that rule.

(iii) If there is no match with any rule, take the default action. The discard all packets or accept all packets.

Example of packet filter table

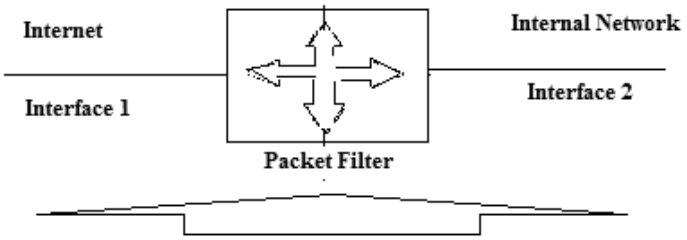


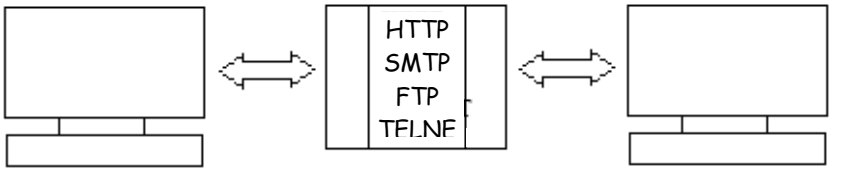
Fig. 2

- The rules specified in the packet filter work as follows.
  - Incoming packets from network 130.33.0.0 are not allowed. They are blocked as a security precaution.
  - Incoming packets from any external network on the TELNET server port (number 23) are blocked.
  - Incoming packets intended for a specific internal host 192.77.21.9 are blocked.
  - Outgoing packets intended for port 80 (HTTP) are banned. That is, this organization does not want to allow its employees to send requests to the external world (internet) for browsing the Internet.

Interface	Source IP	Source port	Destination IP	Destination Port
1	130.33.0.0	*	*	*
1	*	*	*	23
1	*	*	193.77.21.9	*
2	*	*	*	80

(ii) Application Gateways Firewall

- An application gateway is also called as a proxy server. This is because it acts like a proxy and decides about the flow of application level traffic.



Inside connection Application Gateway Outside connection

Fig.: 3

- Application gateways work as follows
  (i) An internal user contacts the application gateway using TCP/IP application, such as HTTP or TELNET.
  (ii) The application gateway asks the user about the remote host with which he user wants to set up a connection for actual communication (i.e. domain name or IP address). The application gateway also asks for user id and the password required to access the services of the application gateway.
  (iii) The user provides this information to the application gateway.
  (iv) The application gateway now accesses the remote host on behalf of the user and passes the packets of the user to the remote host.
  (v) From here onwards, the application gateway acts like a proxy of the actual end user and delivers packets from the user to the remote host and vice versa.

(vi) The application gateway has to manage the two sets of connection. One, from user to application gateway and two, from application gateway to the remote host.

(iii) Circuit gateway

- Circuit gateway operation is similar to Application gateway operation with a slight difference.
- A circuit gateway creates a new connection between itself and a remote host.
- The user is not aware of this and thinks that there is a direct connection itself and the remote host.
- The circuit gateway changes the source IP address in the packets from the end user's IP address to its own.
- This way, the IP addresses of the computers of the internal users are hidden from the outside world.

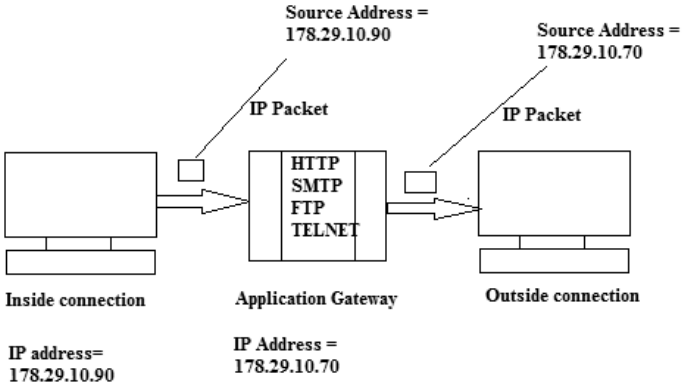


Fig. 4 : Circuit Gateway Operation

Q.3 (d) What is IP security? Describe authentication header mode of IP security. [4]

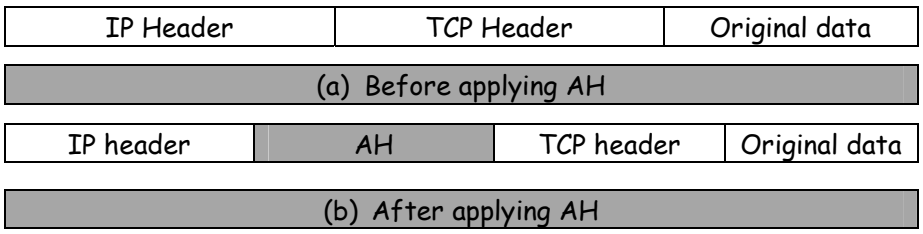
Ans.:

- The protocol for providing security at the IP level, is called as IP Security (IPSec).
- IPSec encrypts and seals the transport and application layer data during transmission. It also offers integrity protection for the Internet layer. However, the Internet header itself is not encrypted, because of which the intermediate routers can deliver encrypted IPSec messages to the intended recipient.

Two modes of IP Security :

(i) AH transport Mode

In the transport mode, the position of the Authentication Header (AH) is between the original IP header and the original TCP header of the IP packet.



(ii) AH tunnel mode

In the tunnel mode, the entire original IP packet is authenticated and the AH is inserted between the original IP header and a new outer IP header. The inner IP header contains the ultimate source and destination IP address, whereas the outer IP header possibly contains different IP addresses (e.g. IP addresses of the firewalls or other security gateway).

IP header	TCP header	Original data

(a) Before applying AH

New IP header	AH	Original IP header	TCP header	Original data

(b) After applying AH

Authentication Header (AH)

- The authentication Header (AH) protocol provides support for data integrity and authentication of IP Packets. The data integrity ensures that data inside IP packets is not altered during transit. The authentication service enables an end user to authenticate the user or the application at the other end and decide to accept or reject packets, accordingly. This also prevents the IP spoofing attacks.

Bit 0	8	16	31

Next header	Payload length	Reserved
Security Parameter Index (SPI)		
Sequence number		
Authentication data (Variable size)		

Authentication Header Format

Next Header	–	This 8 bit field identifies the type of header that immediately follows the AH.
Payload Length	–	This 8 bit field contains the length of the AH in 32-bit words minus 2.
Reserved	–	This 16-bit field is reserved for future use.
Security parameter index	–	This 32-bit field is used in combination with the source and destination addresses as well as the IPSec protocol used to uniquely identify the Security Association (SA) for the traffic to which a datagram belongs
Sequence number	–	This 32-bit field is used to prevent replay attacks.
Authentication data	–	This variable-length field contains the authentication data, called as the Integrity Check Value (ICV), for the datagram.

Q.3 (e) Explain the architecture of secure socket layer. **[4]**

Ans.:

- SSL has three sub-protocols, namely Handshake Protocol, the Record Protocol and the Alert protocol. These three protocols constitute the overall working of SSL.

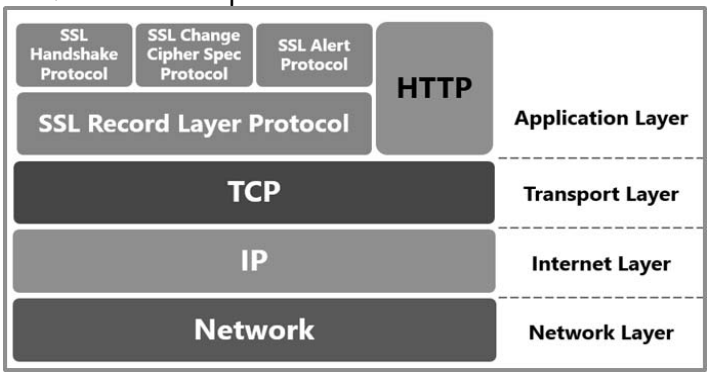


Fig. : 1

The Handshake Protocol

- This protocol of SSL is the first sub-protocol used by the client and the server to communicate using SSL-enabled connection.
- SSL handshake protocol message types :

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
Certificates	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

Each message has the following format :

Type	Length	Content
1 byte	3 bytes	1 or more bytes

- Handshake protocol is actually made up of four phases. These are :

(i) Establish security capabilities.
(ii) Server authentication and key exchange.
(iii) Client authentication and key exchange.
(iv) Finish

(i) Establish security capabilities

- This first phase is used to initiate a logical connection and the establish the security capabilities associated with that connection.

This consists of two messages, the Client hello and the Server hello.

Fields	Client hello	Server hello
Version	This field identifies the highest version of SSL that the client can support. It can be 2,3 or 3.1	This field identifies the lower of the version suggested by client and the highest supported bt the server.
Random	This is useful for the later, actual communication between the client and the server. It contains two subfields – (i) A 32 bit date-time field that identifies the current system date and time on the client machine. (ii) A 28 bit random number generated by the random number generator software built inside the client machine.	This field has the same structure as the Random field of the client. However the random value generated by the server is completely independent of the client's Random value
Session id	This is a session identifier. If this field contains a non zero value, it means that there is already a connection between the client. Zero value indicate that the client wants to create a new connection with the server.	If this value sent by the client was non zero, the server uses the same value. Otherwise, the server creates a new session id and puts it n this field.

Cipher suite	The list contains a list of the cryptographic algorithms supported by the client (RSA, Diffie-Hellman)	Contains a single cipher suite, which server selects from the list sent by the client.
Compression method	This field contains a list of compression algorithms supported by the client.	Contains a compression algorithm, which the server selects from the list sent earlier by the client.

(ii) Server Authentication and Key exchange

- Initiated by the server which is the sole sender of all the messages in this phase.
- The client is the sole recipient.
- Contains 4 steps :

– **Certificate :** the server sends its digital certificate and the entire chain leading upto root CA to the client. The client authenticates the server using server's public key.

– **Server Key Exchange :** is optional. It is used only if the server does not send its digital certificate. In this step, the server sends its public key to the client.

– **Certificate Request :** the server can request for the client's digital certificate. This step is optional.

– **Server Hello done :** this message indicates to the client that its portion of the hello message is complete. This indicates to the client that the client can now verify the certificates sent by the server and ensure that all the parameters sent by the server are acceptable. After sending this message, the server waits for the client response.

(iii) Client Authentication and Key Exchange

- The client initiates this third phase and is the sole sender of all the messages in this phase and the server is the sole recipient.
- This phase contains three steps :
  - **Certificate :** is optional. If the server has requested for the client certificate and client does not have one, then the client responds by sending 'No Certificate' message. Then the server decides to continue or not.
  - **Client Key exchange :** the client creates a 48-byte pre-master secret, and encrypts it with the server's public key and then sends this encrypted pre-master secret to the server.
  - **Certificate Verify :** is necessary only if the server had demanded the client authentication. Here, the client combines the pre-master secret with the random numbers exchanged by the client and the server earlier after hashing them together using MD5 and SHA-1 and signs the result with its private key.

(iv) Finish : the client initiates this phase of handshake protocol which the server ends. This phase contains four steps, the first two messages are from the client : Change cipher specs and Finished. The server responds back with two identical messages: Change cipher specs, Finished.

- Based on the pre-master secret that was created and sent by the client in the Client key exchange message, both the client and the server create a master secret. Before secure encryption or integrity verification can be performed on records, the client and server need to generate shared secret information known only to them. This is master secret which is used to generate keys and secrets for encryption and MAC calculations.
- Finally, the symmetric keys to be used by the client and the server are generated.

After this, the first step, Change cipher specs, is a confirmation from the client that all well from its end, which it strengthens with the Finished Message.

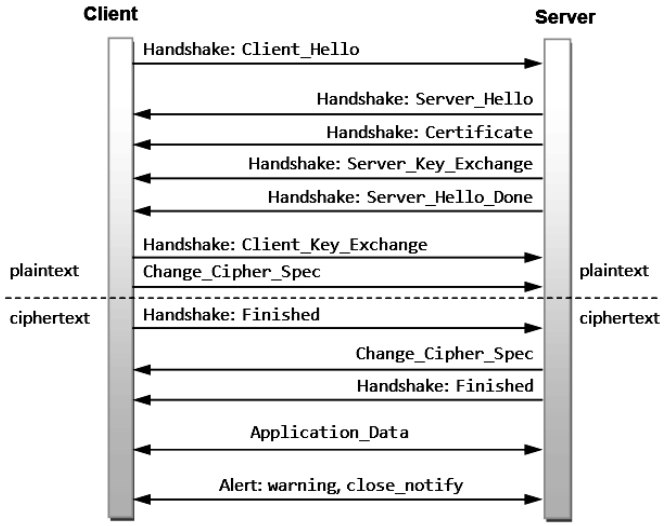


Fig. : 2

The Record Protocol and The Alert Protocol :

The Record Protocol

- The Record Protocol in SSL comes into picture after a successful handshake between the client and the server.
- This protocol provides two services to an SSL connection.
- **Confidentiality** : this is achieved by using the secret key that is defined by the handshake protocol.
- **Integrity** : the handshake protocol also defines a shared secret key (MAC) that is used for assuring the message integrity.
- Record protocol takes an application message as input. First, it fragments it into smaller blocks, optionally compresses each block, adds MAC, encrypts it, adds a header and gives it to the transport layer, where the TCP protocol processes it like any other TCP block. At the receiver's end, the header of each block is removed; the block is then decrypted, verified, decompressed into application message.

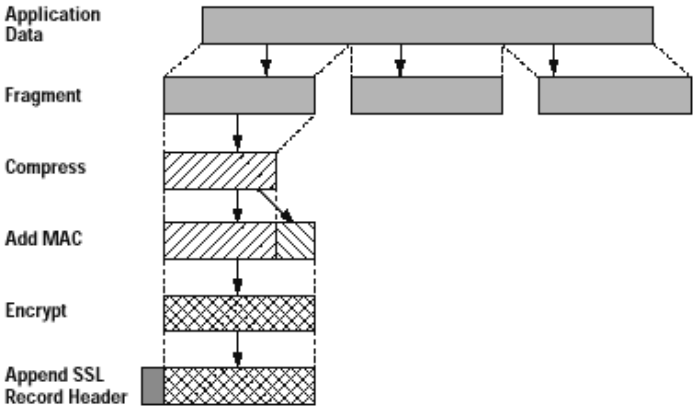


Fig. : 3

The Alert Protocol

- When either the client or the server detects an error, the detecting party sends an alert message to the other party. If the error is fatal, the parties immediately close the SSL connection. Both parties also destroy the session identifiers, secrets and keys associated with this connection before it is terminated.
- Each alert message consists of two bytes. The first byte signifies the type of error. If it is a warning, the byte contains 1. If the error is fatal, this byte contains 2. The second byte specifies the actual error.

Q.4 (a) Attempt any THREE of the following : **[12]**

Q.4(a) (i) Convert plain text into cipher text by using simple columnas technique of the following sentence : **[4]**

'ALL IS WELL FOR YOUR EXAM'

Ans.: ALL IS WELL FOR YOUR EXAM

The columnar transposition cipher is a transposition cipher that follows a simple rule for Mixing up the characters in the plaintext to form the cipher-text. It can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on its own. The cipher uses a columnar transposition to greatly improve its security.

Algorithm:

(i) The message is written out in rows of a fixed length.
(iii) Read out again column by column according to given order or in random order.
(iii) According to order write cipher text.

Example

The key for the columnar transposition cipher is a keyword e.g. MANGO.
The row length that is used is the same as the length of the keyword.
To encrypt a below plaintext

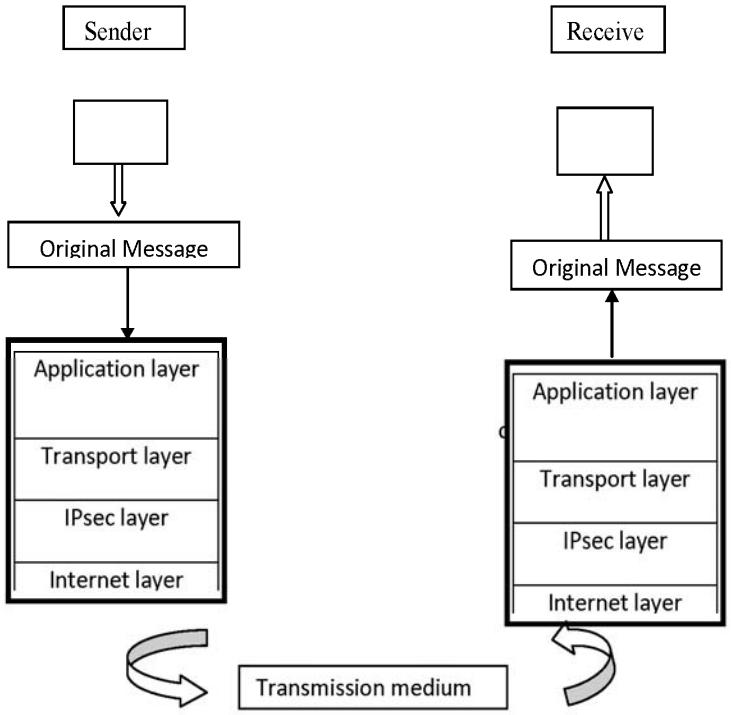
ALL IS WELL FOR YOUR EXAM

4	5	3	2	1
M	A	N	G	O
A	L	L	I	S
W	E	L	L	F
O	R	Y	O	U
R	E	X	A	M

The Encrypted text or Cipher text is:
SFUM ILOA LLYX AWOR LERE

Q.4(a) (ii) Describe IPsec configuration. **[4]**

Ans.:



IP sec overview :

- It encrypts and seal the transport and application layer data during transmission. It also offers integrity protection for internet layer.
- It sits between transport and internet layer of conventional TCP/IP protocol.

(1) Secure remote internet access:
Using IPsec 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; To access the corporate network facilities or access remote desktop/servers.

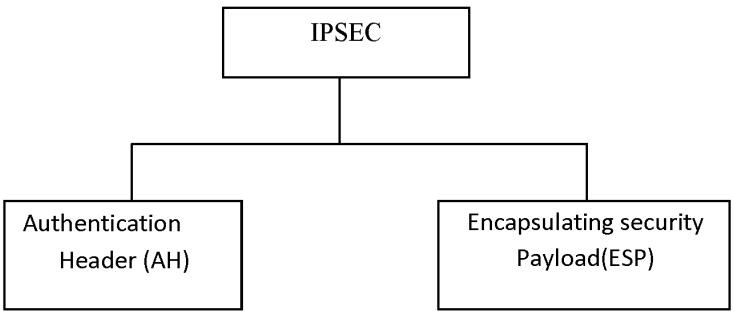
(2) Secure branch office connectivity:
Rather than subscribing to an expensive leased line for connecting its branches across cities, an Organization can setup an IPsec enabled network to securely can't al lits branches over internet.

(3) Setup 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.

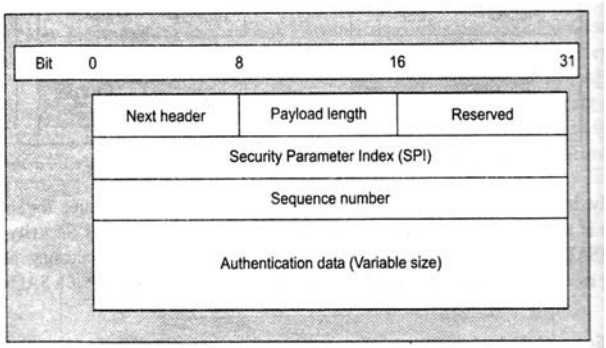
Main advantages of IPsec:

- 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 point for all traffic, making it extra secure.
- IPsec works at network layer. Hence no changes 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 in expensive manner.

Basic Concept of IPsec Protocol:
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 and 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.



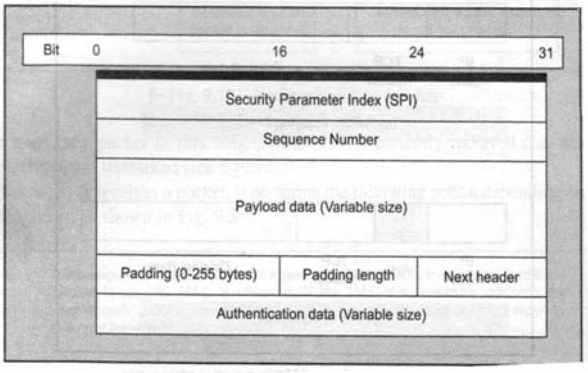
Authentication header (AH)
Authentication header is an IP Packet (AH) protocol provides authentication, integrity &an optional anti-reply service. The IPsec AH is a header in an IP packet. The AH is simply inserted between IP header & any subsequent packet contents no changes are required to data contents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



Authentication Header (AH) format

Encapsulation Header (ESP):

- Used to provide confidentiality, data origin authentication, data integrity.
- It is based on symmetric key cryptography technique.
- ESP can be used in isolation or it can be combined with AH.



Q.4(a) (iii) Describe pornography and software piracy related to cyber crime [4]

Ans.: Pornography

- Pornography is a very inhuman and serious cybercrime offence. It includes the following
  - Any photograph that can be considered obscene and /or unsuitable for the age of child viewer.
  - Film, video, picture.
  - Computer generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit construct.
- Internet is the most frequently used for such criminals to reach children and practice child sex abuse. The spreading use of internet and its easy accessibility to children has made them viable victim to cybercrime. There is a type of humans called pedophiles who usually allure the children by obscene pornographic contents and then they approach them for sex. Then they take their naked photographs while having sex. Such people sometimes misguide children telling that they are of the same age and win their confidence. Then they exploit the children either by forcing them to have sex or selling their pictures over internet.

Software piracy

- Software piracy means copying and using commercial software which is purchased by someone else.
- It is known as illegal duplication, distribution or use of computer software that includes making copies of software, installation of software, sharing, downloading and selling multiple copies of software to personal or work computers.
- Software piracy is the illegal or unauthorized way of copying or distribution of copyrighted software. Individual should understand that purchasing of any software itself includes purchasing of the license that allows him to use it.

- It tells the individual the ownership and copyright of the software and agreement which will not allow for making duplication of the software.
- Creating duplicate copies of software is an act of copyright infringement and its illegal.
- Giving unauthorized access to software or to the serial numbers of registered software can also be illegal.
- When individual purchases the software, he does not become the owner of the copyright. But, he is purchasing the right to use the software under certain restrictions forced by the copyright owner, typically the software publisher.

Ways to deal with / minimize Software Piracy

- Have a central location for software programs. Know which applications are being added, modified or deleted.
- Secure master copies of software and associate documentation, while providing faculty access to those programs when needed.
- Never lend or give commercial software to unlicensed users.
- Permit only authorized users to install software.
- Train and make staff aware of software use and security procedures which reduce likelihood of software piracy.

Q.4(a) (iv) What is an application hardening? How it can be achieved? [4]

Ans.: Application Hardening [4 marks]

Application hardening- securing an application against local and Internet-based attacks. In this you can remove the functions or components you do not need, restrict the access where you can and make sure the application is kept up to date with patches.

It includes :

(i) Application Patches

Application patches are supplied from the vendor who sells the application. They are probably come in three varieties: hot fixes, patches and up-grades.

Hotfixes : 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.

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.

Upgrades : Upgrades are another popular method of patching application and they are likely to be received with a more positive role than patches.

(ii) Web servers

Web servers are the most common Internet server-side application in use. These are mainly designed to provide content and functionality to remote users through a standard web browser.

(iii) Active directory

Active Directory allows single login access to multiple applications, data sources and systems and it includes advanced encryption capabilities like Kerberos and PKI.

Q.4 (b) Attempt any ONE of the following : [6]

Q.4(b) (i) What is Risk? How it can be analyzed? List various assets. [6]

Ans.:

- **A computer security risk** is any event or action that could cause a loss or damage to computer hardware, software, data, or information.
- Some breaches to computer security are accidental, but some are planned. Any illegal act involving a computer is generally referred to as a computer crime.
- Cybercrime refers to online or Internet-based illegal acts.

- Some of the more common computer security risks include Computer viruses, Unauthorized access and use of computer systems ,Hardware theft and software theft, Information theft and information privacy, System failure
- When performing risk analysis it is important to weigh how much to spend protecting each asset against the cost of losing the asset.
- It is also important to take into account the chance of each loss occurring.
- If a hacker makes a copy of all a company's credit card numbers it does not cost them anything directly but the loss in fine and reputation can be enormous.

An **asset** is any data, device, or other component of the environment that supports information-related activities.
Assets generally include
- hardware (e.g. servers and switches),
- software (e.g. mission critical applications and support systems)
- Confidential information.

Assets should be protected from unauthorized access, use, alteration, destruction, and/or theft, resulting in loss to the organization.

Q.4(b) (ii) State the types of attacks and describe Active and Passive attack with atleast one example each. [6]

Ans.: Passive Attack:

A **passive attack** monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks.

Passive attacks include
- traffic analysis,
- release of message contents
- monitoring of unprotected communications,
- decrypting weakly encrypted traffic,
- Capturing authentication information such as passwords.

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to obtain information that is being transmitted.
- The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
- A second type of passive attack, traffic analysis.
- Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.
- Passive attacks are very difficult to detect because they do not involve any alteration of the data.
- Typically, the message traffic is not sent and received in an apparently normal fashion and the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

- However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attack

- In an **active attack,** the attacker tries to bypass or break into secured systems.
- This can be done through stealth, viruses, worms, or Trojan horses.
- Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information.
- These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave.

Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

Active attacks can be divided into four categories:

- masquerade,
- replay,
- modification of messages,
- Denial of Service (DoS)

- A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.
- In replay attack, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning "Allow Ajay to read confidential accounts" is modified to mean "Allow Vijay to read confidential accounts."

Q.5 Attempt any TWO of the following : [16]

Q.5 (a) Explain the role of people with respect to password selection in detail. [8]

Ans.: Four Password selection strategies are:

(1) User education:

(i) Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords.

(ii) This user education strategy is unlikely to succeed at most installations, particularly where there is a large user population or a lot of turnover. Many users will simply ignore the guidelines.

(iii) Others may not be good judges of what is a strong password.

(iv) For example, many users believe that reversing a word or capitalizing the last letter makes a password un-guessable.

(2) Computer-generated passwords:

(i) Passwords are quite random in nature. Computer generated passwords also have problems.

(ii) If the passwords are quite random in nature, users will not be able to remember them. Even if the password is pronounceable, the user may have difficulty remembering it and so be tempted to write it down.

(iii) In general, computer-generated password schemes have a history of poor acceptance by users.

(iv) FIPS PUB 181 defines one of the best-designed automated password generators. The standard includes not only a description of the approach but also a complete listing of the C source code of the algorithm.

(v) The algorithm generates words by forming pronounceable syllables and concatenating them to form a word. A random number generator produces a random stream of characters used to construct the syllables and words.

(3) Reactive password checking:

(i) A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords.

(ii) The system cancels any passwords that are guessed and notifies the user.

(iii) This tactic has a number of drawbacks. First it is resource intensive, if the job is done right. Because a determined opponent who is able to steal a password file can devote full CPU time to the task for hours or even days an effective reactive password checker is at a distinct disadvantage.

(iv) Furthermore, any existing passwords remain vulnerable until the reactive password checker finds them.

(4) Proactive password checking:

(i) The most promising approach to improved password security is a proactive password checker.

(ii) In this scheme, a user is allowed to select his/her own password. However, at the time of selection, the system checks to see if the password is allowable and if not, rejects it.

(iii) Such checkers are based on the philosophy that with sufficient guidance from the system, users can select memorable passwords from a fairly large password space that of selection, the system checks to see if the password is allowable and if not, rejects it.

(iii) Such checkers are based on the philosophy that with sufficient guidance from the system, users can select memorable passwords from a fairly large password space that are not likely to be guessed in a dictionary attack.

(iv) The trick with a proactive password checker is to strike a balance between user acceptability and strength.

(v) If the system rejects too many passwords, users will complain that it is too hard to select a password.

(vi) If the system uses some simple algorithm to define what is acceptable, this provides guidance to password crackers to refine their guessing technique. In the remainder of this subsection, we look at possible approaches to proactive password checking.

Q.5 (b) What is Security topology ? Describe Security zone in detail. [8]

Ans.: **Security Topology** : is a logical map that depicts the interconnectivity between security devices, networks that are protected by security devices and security domains that host these networks. It serves as a foundation to create IPSec VPNs on the network and to configure firewall policies on the security devices.

Types of Security Zones

Internet Zone

- This zone contains Web sites that are not on your computer or on your local intranet, or that are not already assigned to another zone. The default security level is Medium.

Local Intranet Zone

- By default, the Local Intranet zone contains all network connections that were established by using a Universal Naming Convention (UNC) path, and Web sites that bypass the proxy server or have names that do not include periods (for example,

http://local), as long as they are not assigned to either the Restricted Sites or Trusted Sites zone.

- The default security level for the Local Intranet zone is set to Medium (Internet Explorer 4) or MediuS-low (Internet Explorer 5 and 6). Be aware that when you access a local area network (LAN) or an intranet share, or an intranet Web site by using an Internet Protocol (IP) address or by using a fully qualified domain name (FQDN), the share or Web site is identified as being in the Internet zone instead of in the Local intranet zone.

Trusted Sites Zone

- This zone contains Web sites that you trust as safe (such as Web sites that are on your organization's intranet or that come from established companies in whom you have confidence).
- When you add a Web site to the Trusted Sites zone, you believe that files you download or that you run from the Web site will not damage your computer or data. By default, there are no Web sites that are assigned to the Trusted Sites zone, and the security level is set to Low.

Restricted Sites Zone

- This zone contains Web sites that you do not trust. When you add a Web site to the Restricted Sites zone, you believe that files that you download or run from the Web site may damage your computer or your data. By default, there are no Web sites that are assigned to the Restricted Sites zone, and the security level is set to High.

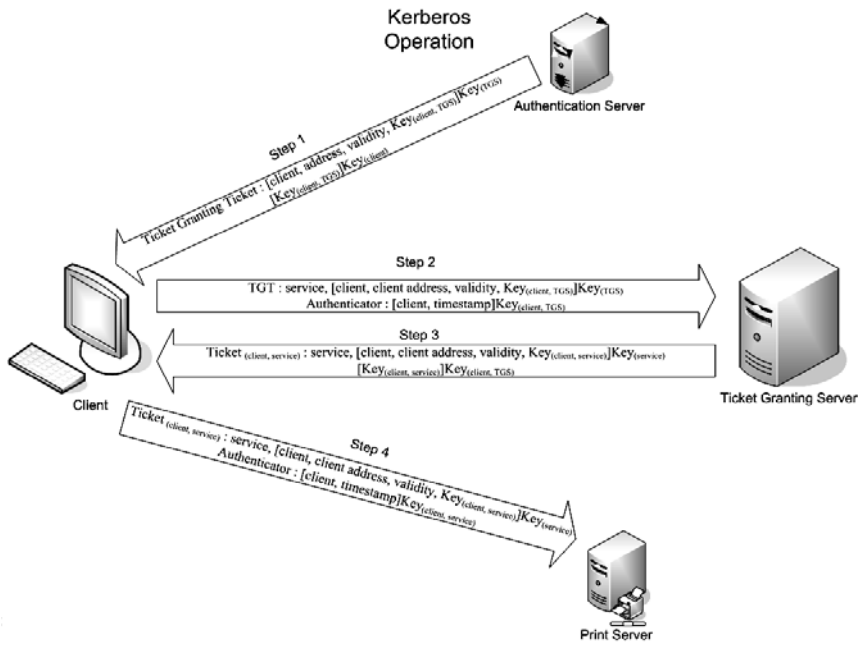
Q.5 (c) What is Kerberos? Explain with diagram different servers involved in Kerberos. [8]

Ans.:

- Many real life systems use an authentication protocol called as Kerberos.
- It is designed to allow workstations to use network resources in a secure manner.
- The servers used in Kerberos are
  - Authentication Server (AS) - Authenticates the user during Login
  - Ticket Granting Server (TGS) - Issues tickets to certify proof of Identity.

Authenticate Server (AS) : the job of AS is to authenticate every user at the login time. AS shares a unique secret password with every user.

Ticket Granting Server (TGS) : the job of TGS is to certify to the servers in the network that user is really what she claims to be.



Here's how the logon process works with Kerberos as the authentication method:
To log on to the network, the user provides an account name and password.

(i) The Authentication Server (AS) component of the KDC accesses Active Directory user account information to verify the credentials.
(ii) The KDC grants a Ticket Getting Ticket (TGT) that allows the user to get session tickets to access servers in the domain, without having to enter the credentials again (the TGT is good for 10 hours by default; this expiration period can be configured by the administrator). (Step 1 in the diagram)
(iii) When the user attempts to access resources on a server in the domain, the TGT is used to make the request. The client presents the TGT to the KDC to obtain a service ticket. (Step 2)
(iv) The Ticket Granting Service (TGS) component of the KDC authenticates the TGT and then grants a service ticket. The service ticket consists of a ticket and a session key. A service ticket is created for the client and the server that the client wants to access. (Step 3)
(v) The client presents the service ticket to create a session with the service on the server. The server uses its key to decrypt the information from the TGS, and the client is authenticated to the server. (Step 4)
(vi) If mutual authentication is enabled, the server also authenticates to the client.

Q.6 Attempt any FOUR of the following : [16]

Q.6 (a) What is piggybacking? How it can be prevented? [4]

Ans.: Piggybacking: It is the simple process of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building. An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card. i.e. Access of wireless internet connection by bringing one's own computer within range of another wireless connection & using that without explicit permission, it means when an authorized person allows (intentionally or unintentionally) others to pass through a secure door. Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge. It is the simple tactic of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building. An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card. 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.

Prevention:

(i) Piggybacking can be prevented by ensuring that encryption is enabled in router by using Wireless Encryption Protocol (WEP) or Wireless Protected Access (WPA) or WPA2.
(ii) Using a strong password for encryption key, consisting of at least 14 characters and mixing letters and numbers.

Q.6 (b) What is One Time Pad (OPT) security mechanism? [4]

Ans.: One time pad Security Mechanism: One time pad (Vernam Cipher) is the encryption mechanism in which the encryption-key has at least the same length as the plaintext and consists of truly random numbers. Each letter of the plaintext is mixed with one element from the OTP. This results in a cipher-text that has no relation with the plaintext when the key is unknown. At the receiving end, the same OTP is used to retrieve the original plaintext.

Steps for One time pad :

(i) The key should be as long as the message
(ii) Key and plain text calculated modulo 26

(iii) There should only be 2 copies of the key (1 for sender and 1 for receiver)

Example: Suppose Alice wishes to send the message "**HELLO**" to Bob In OTP assign each letter a numerical value: e.g. "A" is 0, "B" is 1, and so on. Here, we combine the key and the message using modular addition. The numerical values of corresponding message and key letters are added together, modulo 26. If key is "**XMCKL**" and the message is "**HELLO**", then the encrypted text will be "**EQNVZ**"

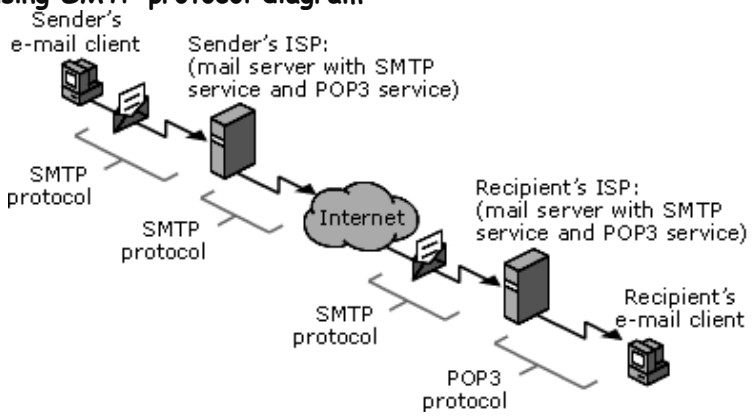
```
     H      E      L      L      O  message
   7 (H)  4 (E) 11 (L) 11 (L) 14 (O) message
+ 23 (X) 12 (M)  2 (C) 10 (K) 11 (L) key
= 30     16     13     21     25     message + key
=  4 (E) 16 (Q) 13 (N) 21 (V) 25 (Z) message + key (mod 26)
     E      Q      N      V      Z  → ciphertext
```

Fig.: One time pad

Q.6 (c) Explain e-mail security techniques (protocols). **[4]**

Ans.: **(i) SMTP** – is used for email communications. The email software at the sender's end gives the email message to the local SMTP server. This SMTP server actually transfers the email message to the SMTP receiver. Its main job to carry the email message between the sender and the receiver. SMTP runs on top of TCP/P.

Email using SMTP protocol diagram



The basic phases of an email communication consists of the following steps:

(1) At the sender's end, an SMTP server takes the message sent by a user's computer.

(2) The SMTP server at the sender's end then transfers the message to the SMTP server of the receiver.

(3) The receiver's computer then pulls the email message from the SMTP server at the receiver's end, using other email protocols such as Post Office Protocol (POP) of Internet Mail Access Protocol (IMAP)

(ii) S/MIME – Secure Multipurpose Internet Mail Extensions (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 and then sends it over the Internet to the recipient, but multimedia files or documents in various arbitrary format cant not be sent using this protocol.
- To cater to these needs the Multipurpose Internet Mail Extensions (MIME) system extends the basic email system by permitting users to send the binary files using the basic email system. And when the basic MIME system is enhanced to provide security features, it is called as Secure Multipurpose Internet Mail Extensions.
- S/MIME provides for digital signatures and encryption of email message.

S/MIME functionalities.

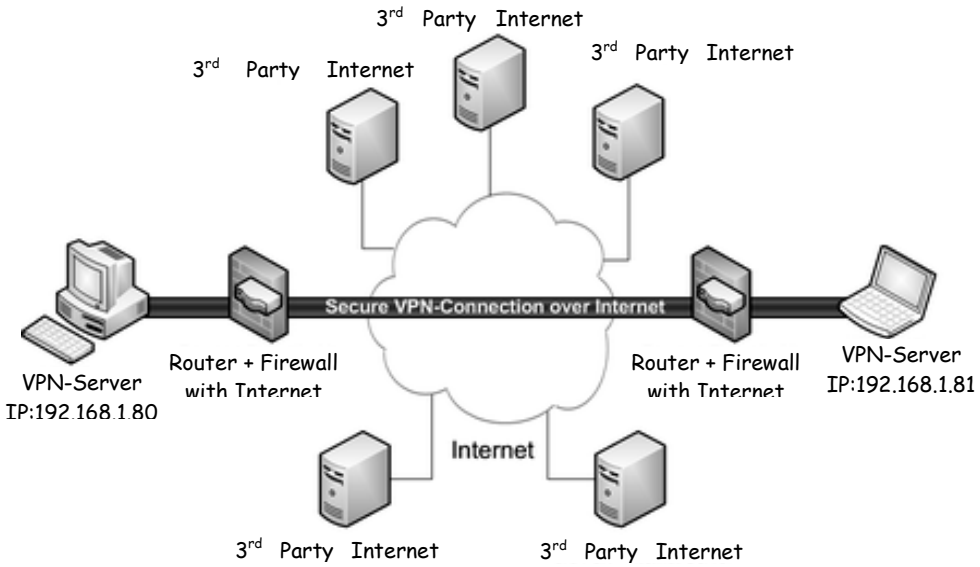
Functionality	Description
Enveloped data	Consists of encrypted content of any type and the encryption key encrypted with the receiver's public key.
Signed data	Consists of a message digest encrypted with the sender's private key. the content and the digital signature are both Base-64 encoded.
Clear-signed data	Similar to Signed data. However only the digital signature is Base 64 encoded.
Signed and enveloped data	Signed only and enveloped-only entities can be combined, so that the enveloped data can be signed, or the Signed/Clear-signed data can be enveloped.

(iii) VPN

- A VPN is a mechanism of employing encryption, authentication and integrity protection so that one we use a public network (internet) as if it is a private network aerated and controlled by us.
- VPN offers high amount of security and yet does not require any special cabling on behalf of the organization that wants to use it.
- Thus a VPN combines the advantages of a public network (cheap and easily available) with those of a private network (secure and reliable)
- A VPN can connect distant networks of an organization or it can be used to allow travelling users to remotely access a private network securely over the internet.

VPN Architecture

- Suppose an organization has two networks, Network 1 and Network 2, which are physically apart from each other, two firewalls can be set up, Firewall 1 and firewall 2. The encryption and decryption are performed by firewalls.
- Network 1 connects to Internet via firewall1 and Network connects to Internet via firewall 2. Two firewalls are virtually connected to each other via the Internet.
- Lets assume Host X on Network 1 to send data packet to Host Y on Network 2.
- Host X creates the packet, inserts its own IP address as the address and the IP address of host Y as the destination address.
- The packet reaches firewall 1. Firewall 1 now adds new headers to the packet. It changes the source IP address of the packet from that of Host X to its own address. It also changes the destination IP address of the packet from that if host Y to the IP address of firewall 2. It also performs encryption and authentication.



- The packet reaches Firewall 2 over the Internet via one or more routers. Firewall 2 discards the outer header and performs the decryption and other cryptographic functions. This yields the original packet. Then the packet is delivered to Y.

(iv) PEM

- PEM is Private Enhanced Mail. It is an email security standard to provide secure electronic mail communication over the internet.
- PEM supports the three main cryptographic functions of encryption, non-repudiation and message integrity.
- The steps in PEM are Canonical Conversion, Digital signature, Encryption and Base-64 Encoding.

(1) Canonical Conversion: 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 the receiving computers, the email message always travels in uniform, independent format.

(2) Digital signature: this process starts by creating a message digest of the email message using MD@ or MD5 algorithm.

Email message
To : anand@abc.com
From:abhay@xyz.net ---→ Message Digest algorithm ---→ 10101
Subject: Our meeting (MD2 or MD5) 01010
10….. Message digest

Message Digest creation of the original message

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

10101
01010 ------→ Encryption with Sender's ------→ Digital signature
10… Private key

(3) Encryption: in this step, the original email and the digital signature are encrypted together with a symmetric key. For this, DES algorithm is used.

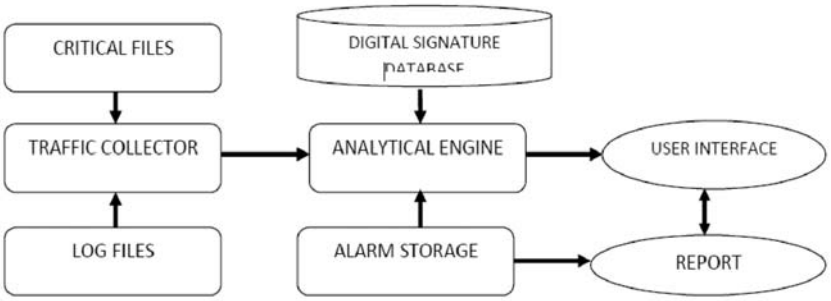
(4) Base-64 Encoding: in this step, the Base-64 encoding process transforms arbitrary binary input into printable character output. In this technique, the binary output is processed in blocks of 3 octets or 24 bits. These 24 bits are considered to be made up of 4 sets, each of 6 bits. Then their decimal equivalent generated is looked up into the 64-encodind mapping table. The character found at the position specified by the decimal number in this table is then mentioned in the output. Finally, the binary equivalent corresponding to 8-bit ASCII of this character is written.

Q.6 (d) What is intrusion detection system ? Explain host based IDS. [4]

Ans.: Intrusion Detection System

- Intrusion Detection System is a system for detecting Network Attacks.
- IDS consists of a set of sensors gathering data, either located on host or on the network. There, data is analyzed, intrusions reported and reactions triggered.

An IDS (Intrusion detection system) is intrusion detection system is process of monitoring the events occurring in computer system or network & analyzing tem for signs of possible incident which are threats of computer security. Intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways.



Host based IDS

Host based IDS resides on a particular computer or server, known as the host, and monitors activity only on that system. HIDS are also known as system integrity verifiers as they monitor the status of the key system files and detect when an intruder creates, modifies or deletes modified files. The HIDs is also capable of monitoring system configuration databases, such as windows registries, in addition to stored configuration files like .ni, .cfg and .dat files. Most HIDs work on the principle of configuration or change management which means they can record the sizes, locations and other attributes of the system files. The HIDs then triggers an alert when one of the following changes occurs: file attributes change, new files are created, or existing files are deleted.

Advantages of Host based IDS

- A HIDs can detect local events on host systems and also detect attacks that may elude a network-based IDS.
- A HIDs function on the host system, where encrypted traffic will have been decrypted and is available for processing.
- The use of switched network protocols does not affect a HIDs.
- A HIDs can detect inconsistencies in how applications and systems programs were used by examining the records stored in audit logs. This can enable it to detect some types of attacks, including Trojan Horse Programs.

Disadvantages of Host based IDS

- HIDs pose more management issues since they are configured and managed on each monitored host. This means that it will require more management effort to install, configure, and operate HIDs than a comparably sized NIDs solution.
- HIDs is vulnerable both to direct attacks and do attacks against the host operating system. This results in loss of HIDs functionality.
- It is not optimized to detect multi-host scanning, nor is it able to detect the scanning of non-host network devices, such as routers or switches.
- HIDs is susceptible to some denial-of-service attacks.
- HIDs can use large amounts of disk space to retain the host OS audit logs; and to function properly, it may require disk capacity to be added to the system.

Q.6 (e) What is SSL/TLS? [4]

Ans.: Transport Layer Security (TLS) and Secure Sockets Layer (SSL), both referred to as "SSL" are cryptographic protocols that provide communications security over a network. The Transport Layer security (TLS) protocol provides communications privacy over internet. The protocol allows client-server applications to communicate in a way that is designed to prevent eavesdropping, tampering or message forgery. The primary goal of the TLS protocol is to provide privacy in data integrity between two communicating applications.

The protocol is composed of two layers:

(i) TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption.

(ii) The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.

❑ ❑ ❑ ❑ ❑