MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

SUMMER – 2022 EXAMINATION
MODEL ANSWER

Subject: Network Information Security **Subject Code: 22620**

Important Instructions to examiners:

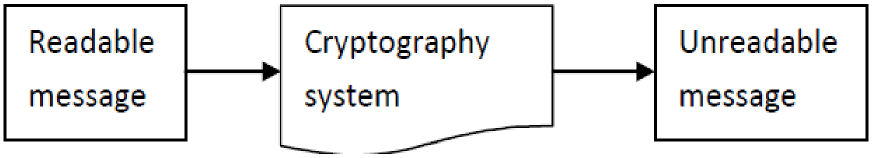
1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling 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.
8) As per the policy decision of Maharashtra State Government, teaching in English/Marathi and Bilingual (English + Marathi) medium is introduced at first year of AICTE diploma Programme from academic year 2021-2022. Hence if the students in first year (first and second semesters) write answers in Marathi or bilingual language (English +Marathi), the Examiner shall consider the same and assess the answer based on matching of concepts with model answer.

Q.No	Sub Q.N.	Answer	Marking Scheme
1.		**Attempt any FIVE of the following:**	**10**
	a)	**Define following terms:** **i) Confidentiality** **ii) Accountability**	**2M**
	Ans	**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. OR 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. **ii) Accountability:** The principle of accountability specifies that every individual who works with an information system should have specific	***1M for each definition***

		responsibilities for information assurance. The tasks for which a individual is responsible are part of the overall information security plan and can be readily measurable by a person who has managerial responsibility for information assurance. One **example** would be a policy statement that all employees must avoid installing outside software on a company-owned information infrastructure. OR The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.	
	b) **Ans.**	**Explain the terms:** **i) Shoulder surfing** **ii) Piggybacking** **i) Shoulder surfing:** It is using direct observation techniques, such as looking over someone's shoulder, to get information. 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. • 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, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. **ii) Piggybacking :** 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. OR 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. OR An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card. 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.	**2M** ***1M for each explanation***

c) **Define term cryptography.** **2M**

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



2M for definition, diagram is optional

d) **Classify following cyber crimes:** **2M**

i) Cyber stalking

ii) Email harassment

Ans. **i) Cyber stalking :** Cyber Stalking means following some ones activity over internet. This can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

OR

Cyber stalking : Cyberstalking/ Harassment refers to the use of the internet and other technologies to harass or stalk another person online, and is potentially a crime in the India under IT act-2000.

This online harassment, which is an extension of cyberbullying and in-person stalking, can take the form of e-mails, text messages, social media posts, and more and is often methodical, deliberate, and persistent.

ii) Email harassment : Email harassment is usually understood to be a form of stalking in which one or more people send consistent, unwanted, and often threatening electronic messages to someone else

OR

Email harassment : Cybercrime against individual

1M for each explanation

e) **Differentiate between viruses & worms (any two)** **2M**

Ans.

S. N	Worms	Virus
1.	The worm is code that replicate itself in order to consume resources to bring it down.	The virus is the program code that attaches itself to application program and when application program run it runs along with it
2.	It exploits a weakness in an application or operating system by replicating itself	It inserts itself into a file or executable program.

1M for each difference, any two can be considered

3	It can use a network to replicate itself to other computer systems without user intervention.	It has to rely on users transferring infected files/programs to other computer systems.
4	Usually not. Worms usually only monopolize the CPU and memory.	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.
5	Worm is faster than virus	Virus is slower than worm.
6	E.g. Code red	E.g. Macro virus, Directory virus, Stealth Virus

f) **Define firewall. Enlist types of firewalls.** **2M**

Ans. **Definition Firewall:** A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

1M for definition 1M for listing any two types

Types of Firewall :

1 .Packet Filter
2. Circuit level Gateway
3. Application Gateway
4. Software
5. Hardware
6. Hybrid
7. Stateful multilayer Inspection Firewall

g) **Define AH & ESP with respect to IP security.** **2M**

1M each, any one point also can be considered

Ans. **Authentication header (AH):**

1. The AH provides support for **data integrity and authentication** of IP packets. The data integrity service ensures that data inside IP packet is not altered during the transit.

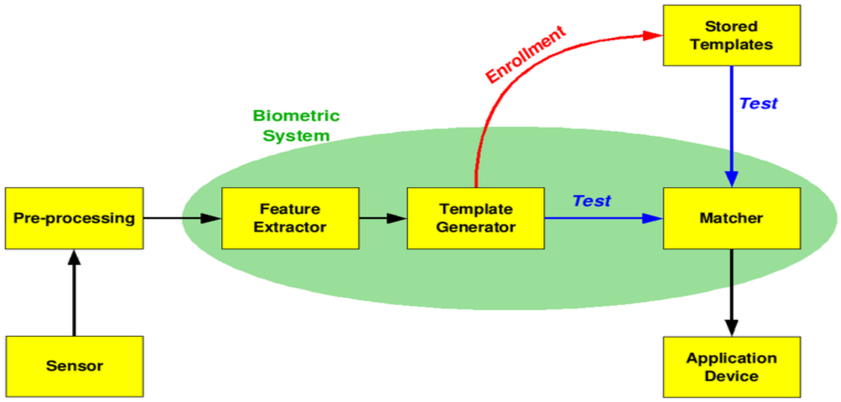
2. The authentication service enables an end user or computer system to authenticate the user or the application at the other end and decides to accept or reject packets accordingly

Encapsulation Header (ESP):

1. Used to provide confidentiality, data origin authentication, data integrity.

2. It is based on symmetric key cryptography technique.

		3. ESP can be used in isolation or it can be combined with AH.	
2.	 **a)** **Ans.**	**Attempt any <u>THREE</u> of the following:** **Define following terms:** **i) Operating System Security** **ii) Hot fix** **iii) Patch** **iv) Service pack** **i) Operating System Security**: The OS must protect itself from security breaches, such as runaway processes (denial of service), memory-access violations, stack overflow violations, the launching of programs with excessive privileges, and many others. **ii)Hot Fix :** 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. **iii) 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. **iv) Service Pack :** *service pack* is a collection of updates and fixes, called patches, for an operating system or a software program. Many of these patches are often released before a larger service pack, but the service pack allows for an easy, single installation. **OR** A service pack (SP) is an update, often combining previously released updates, that helps make Windows more reliable. Service packs can include security and performance improvements and support for new types of hardware.	**12** **4M** ***1M for each definition***
	b) **Ans.**	**Explain the mechanism of fingerprint & voice pattern in Biometrics.**	**4M** ***2M for each explanation , diagram is optional***



Fingerprint registration & verification mechanism

1. During registration, first time an individual uses a biometric system is called an enrollment.

2. During the enrollment, biometric information from an individual is stored.

3. In the verification process, biometric information is detected and compared with the information stored at the time of enrolment.

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

5. The 2nd block performs all the necessary pre-processing.

6. The third block extracts necessary features. This step is an important step as the correct features need to be extracted in the optimal way.

7. If enrollment is being performed the template is simply stored somewhere (on a card or within a database or both).

8. 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.

9. The matching program will analyze the template with the input. This will then be output for any specified use or purpose.

Voice pattern :

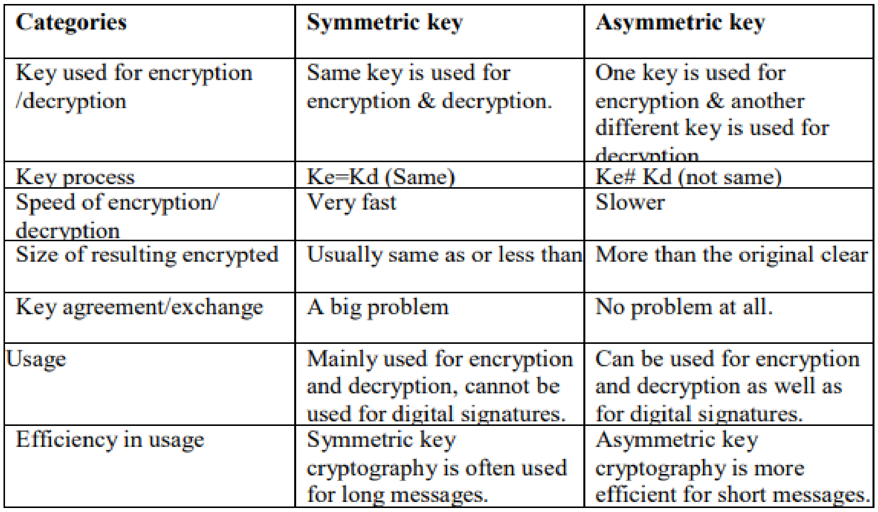
1. Biometric Voice Recognition is the use of the human voice to uniquely identify biological characteristics to authenticate an individual unlike passwords or tokens that require physical input.
2. Voice biometric recognition works by inputting the voice of the individual whose identity has to be stored in the system. This input is kept as a print for authentication. The input print is made with software that can split the voice statement into multiple frequencies
3. A voice biometrics tool collects a user's voice template.

it only checks who is speaking and what is speaking (Who you are and what you speak)

c) **Differentiate between symmetric and asymmetric key cryptography.**

4M
1M for each valid point, any four points can be considered

Ans.



Categories	Symmetric key	Asymmetric key
Key used for encryption /decryption	Same key is used for encryption & decryption.	One key is used for encryption & another different key is used for decryption
Key process	Ke=Kd (Same)	Ke# Kd (not same)
Speed of encryption/ decryption	Very fast	Slower
Size of resulting encrypted	Usually same as or less than	More than the original clear
Key agreement/exchange	A big problem	No problem at all.
Usage	Mainly used for encryption and decryption, cannot be used for digital signatures.	Can be used for encryption and decryption as well as for digital signatures.
Efficiency in usage	Symmetric key cryptography is often used for long messages.	Asymmetric key cryptography is more efficient for short messages.

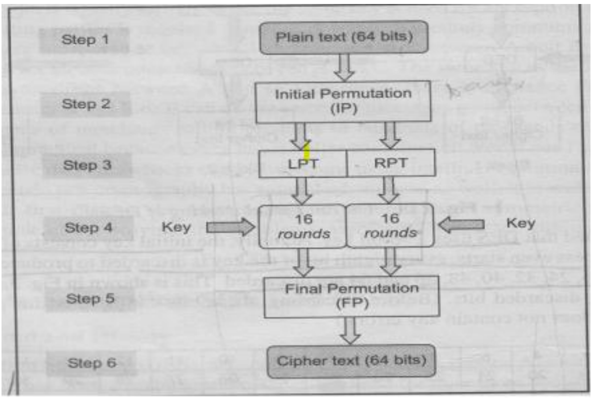
d) **Write & explain DES algorithm**

4M

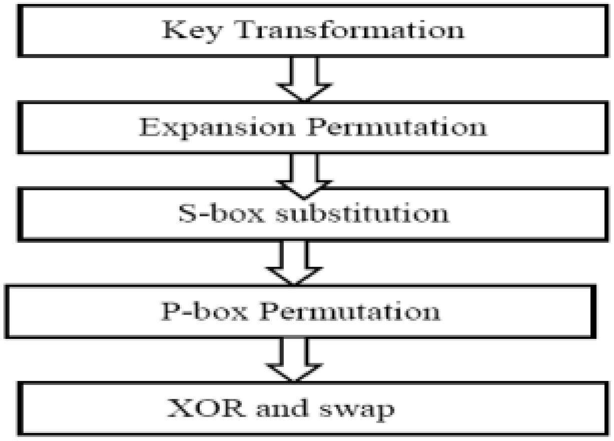
2M for diagram

2M for explanation

Ans.



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 Expansion Permutation Key Transformation

S-box substitution

XOR and swap

P-box Permutation

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 XOR ed with the 48-bit RPT and the resulting output is given to the next step.

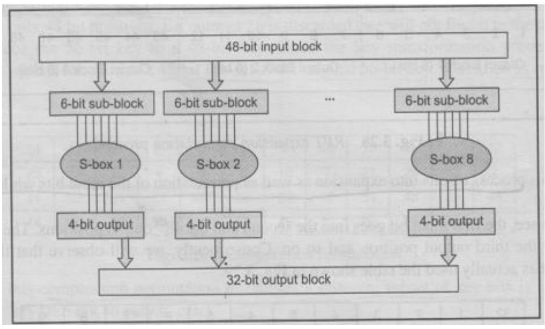
Step 3: S-box substitution: It accepts the 48-bits input from the XOR operation involving the compressed key and expanded RPT and produces 32-bit output using the substitution techniques. Each of the 8 S-boxes has a 6-bit input and a 4-bit output. The output of each S-box then combined to form a 32-bit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

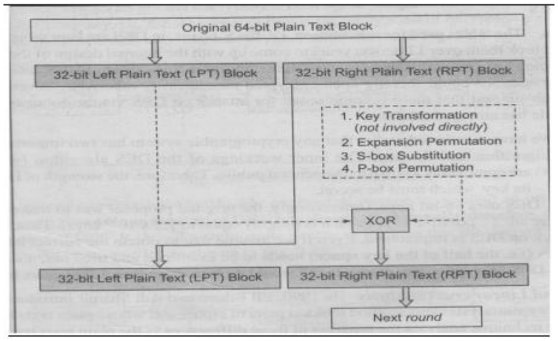
Step 4: P- box permutation: the output of S-box consists of 32-bits. These 32-bits are permuted using P-box. Step

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

<table>
<tr><td></td><td></td><td>

new RPT. The old RPT becomes new LPT, in a process of swapping.




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

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

</td><td></td></tr>
<tr><td>3.</td><td>a)
Ans.</td><td>

Attempt any <u>THREE</u> of the following:

Describe the features of DAC access control policy.

DAC (discretionary access control) policy utilizes user identification procedures to identify and restrict object access .It restricts access to objects based on the identity of subjects and or groups to which they belongs to. The owner of information or any resource is able to change its permissions at his discretion .Data Owners can transfer ownership of information to other users .Data Owners can determine the type of access given to other users (read, write etc.)

Features of DAC policy are as follows :-

Flexible –In DAC policy owner of information or resource can change its permission.

</td><td>12
4M
<i>1M for explanation , 3M for features</i></td></tr>
</table>

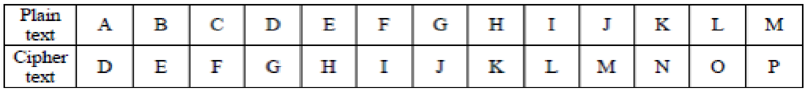
Backup - Discretionary access control allows organizations to backup security policies and data to ensure effective access points.

Usability - Discretionary access control is easy to use. Data Owners can transfer ownership of information to other users easily.

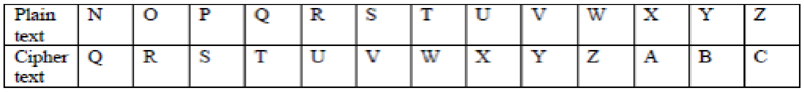
b) **Consider plain text "COMPUTER ENGINEERING" and convert given plain text into cipher text using 'Caesar Cipher' with shift of position three- write down steps in encryption.** **4M**

Ans. Caesar cipher technique is proposed by Julius Caesar. It is one of the simplest and most widely known encryption techniques. It is a type of substitution technique in which each letter in the plain text is replaced by a letter some fixed number of position down the alphabet. The Caesar cipher involves replacing each letter of the alphabet with the letter three places further down the alphabet. For example, with a shift of 3, A would be replaced by D, B would became E, and so on as shown in the table below

2M for explanation 2M for problem solution



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



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

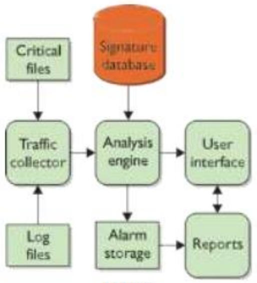
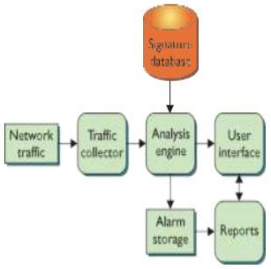
PLAIN TEXT -COMPUTER ENGINEERING
CIPHER TEXT–FRPSXWHU HQJLQHHULQJ

c) **Differentiate between host-based & network based IDS** **4M**

Ans.

S N	Host Based Ids	Network Based Ids
1	Examines activity on an individual system, such as a mail server, web server, or individual PC.	Examines activity on the network itself
2	It is concerned only with an individual system and usually has no visibility into the activity on the network or systems around it	It has visibility only into the traffic crossing the network link it is monitoring and typically has no idea of what is happening on individual systems.

1M for each valid point, any four points can be considered

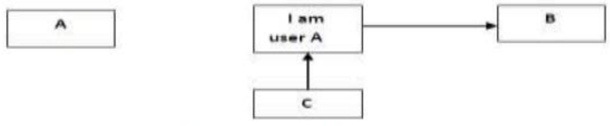
3	HIDS is looking for certain activities that typify hostile actions or misuse, such as the following: • Logins at odd hours • Login authentication failures • Additions of new user accounts • Modification or access of critical system files	NIDSs look for certain activities that typify hostile actions or misuse, such as the following: • 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
4	 Critical files Signature database Traffic collector Analysis engine User interface Log files Alarm storage Reports HIDS	 Signature database Network traffic Traffic collector Analysis engine User interface Alarm storage Reports NIDS
5	It is host dependent	It is host independent
6	It has low false positive rate	It has high false positive rate
7	It senses local attack.	It senses network attack
8	It slow down the host that have IDS client installed	It slow down the network that have IDS client installed

d) **Define access control and explain authentication mechanism for access control.** **4M**

Ans. **Access Control –**

2M for Access control

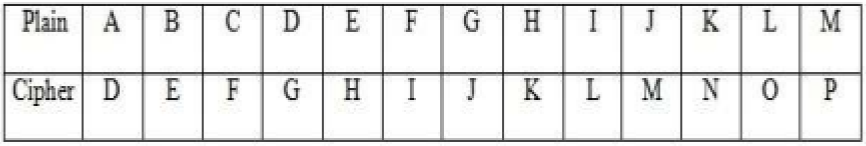
Access is the ability of a subject to interest with an object. Authentication deals with verifying the identity of a subject. It is ability to specify, control and limit the access to the host system or application, which prevents unauthorized use to modify data or

		resources. Access control is to specify, control and limit the access to the host system or application, which prevents unauthorized use to access or modify data or resources. **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 Authentication is the process of determining identity of a user or other entity. It is performed during log on process where user has to submit  Fig. Absence of authentication His / her username and password. There are three methods used in it. 1. Something you know - User knows user id and password. 2. Something you have - Valid user has lock and key. 3. Something about you - User's unique identity like fingerprints, DNA etc.	***2M for authentication***
4.	**a)** **Ans.**	**Attempt any <u>THREE</u> of the following:** **Enlist substitution techniques & explain any one.** Substitution Techniques:- In substitution technique letters of plain text are replaced by the other letters or by numbers or by symbols. Substitution techniques are as follows:- a) Caesar cipher b) Modified version of Caesar cipher c) Mono-alphabetic cipher d) Vigener‘s cipher	**12** **4M** ***1M for list, 2M for explanation 1M for example***

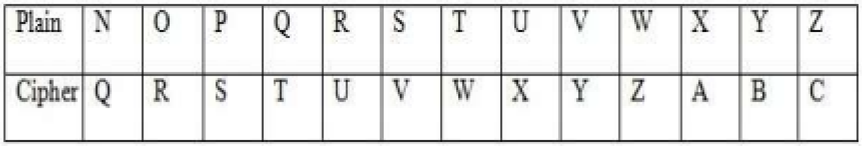
Caesar cipher:

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

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



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



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

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

For S:= (p+k)mod26
= (18 + 3) mod 26
= 21
= V

To allow someone to read the cipher text, you tell them that the key is3

Algorithm to break Caesar cipher:

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

b)
Ans.

Explain DMZ

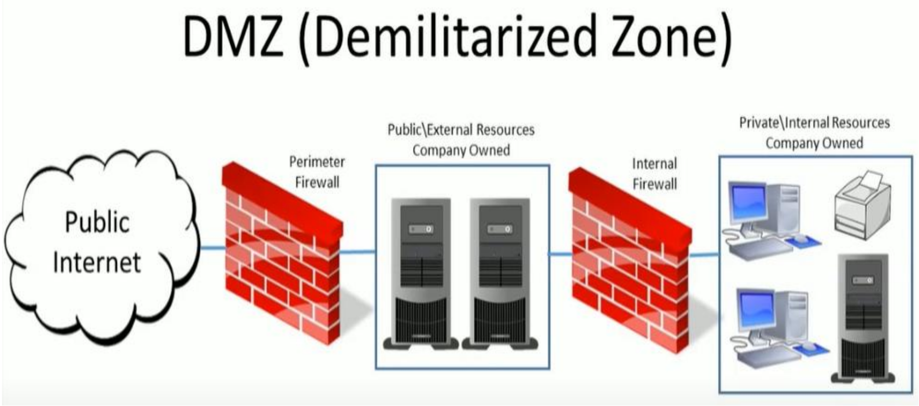
4M
1M for diagram
2M for explanation
1M for

DMZ (Demilitarized Zone):-

- It is a computer host or small network inserted as a "neutral zone" in a company's private network and the outside public network. It avoids outside users from getting direct access to a company's data server. A DMZ is an optional but more secure approach to a firewall. It can effectively acts as a proxy server.

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

example


DMZ (Demilitarized Zone)
Public Internet
Perimeter Firewall
Public\External Resources Company Owned
Internal Firewall
Private\Internal Resources Company Owned

Advantage: The main benefit of a DMZ is to provide an internal network with an additional security layer by restricting access to sensitive data and servers. A DMZ enables website visitors to obtain certain services while providing a buffer between them and the organization's private network.

c) Ans.

Differentiate between firewall & IDS

4M
1M for each correct point Any four points

S. N	Firewall	IDS
1	Firewall is hardware or software that stands between a local network and the Internet and filters traffic that might be harmful based on predetermined rules.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
2	Firewall does not inspect content of permitted traffic	IDS inspects overall network traffic

3	A firewall can block an unauthorized access to network	An IDS can only report an intrusion .It cannot block it.
4	Firewalls Block traffic based on rules the	IDS gives Alerts/alarms on detection of anomaly
5	It filters traffic based on IP address and port numbers	It detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts

d) **Explain Email security in SMTP.** **4M**

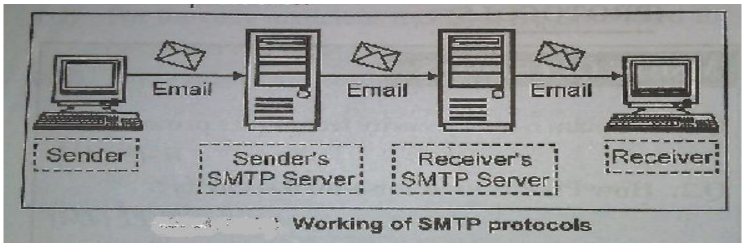
1M for diagram
3M for explanation

Ans. Email Security Email is emerging as one of the most valuable services on the internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver‘s side.

1. SMTP (simple mail transfer protocol)
2. PEM (Privacy Enhance Mail)
3. PGP (Pretty Good Privacy)

SMTP (Simple Mail Transfer Protocol)

Simple Mail Transfer Protocol, a protocol for sending email messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application. SMTP usually is implemented to operate over Internet port 25. An alternative to SMTP that is widely used in Europe is X.400. Many mail servers now support Extended Simple Mail Transfer Protocol (ESMTP), which allows multimedia files to be delivered as e-mail.

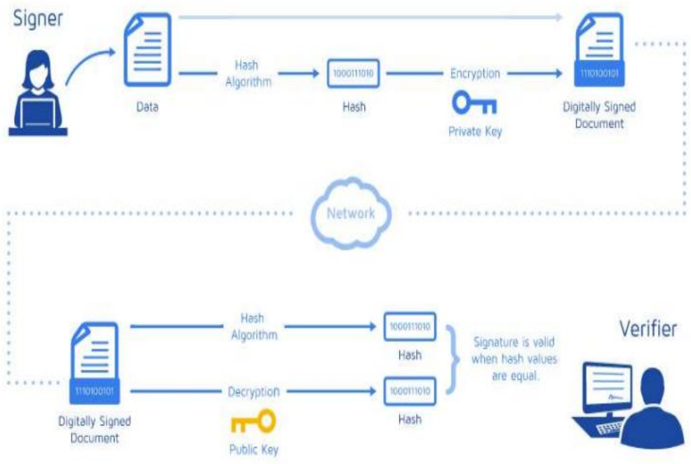


Working of SMTP protocols

		The basic phases of an email communication consists of the following steps :- 1. At sender‘s end an SMTP server takes the message sent by uses computer 2. The SMTP server at the sender‘s end then transfer 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 the other mail protocol such as Post Office Protocol (POP) or IMAP (Internet mail access protocol)	
	e) **Ans.**	**Explain digital signature in Cryptography.** **Digital Signature:** 1. Digital signature is a strong method of authentication in an electronic form. 2. It includes message authentication code (MAC), hash value of a message and digital pen pad devices. It also includes cryptographically based signature protocols. 3. Digital Signature is used for authentication of the message and the sender to verify the integrity of the message. 4. Digital Signature may be in the form of text, symbol, image or audio. 5. In today’s world of electronic transaction, digital signature plays a major role in authentication. For example, one can fill his income tax return online using his digital signature, which avoids the use of paper and makes the process faster. 6. Asymmetric key encryption techniques and public key infrastructure are used in digital signature. 7. Digital signature algorithms are divided into two parts- a. Signing part: It allows the sender to create his digital signature. b. Verification part: It is used by the receiver for verifying the signature after receiving the message. **Generation and Verification of digital signatures:** Working: 1. Message digest is used to generate the signature. The message digest (MD) is calculated from the plaintext or message. 2. The message digest is encrypted using user’s private key. 3. Then, the sender sends this encrypted message digest with the plaintext or message to the receiver.	**4M** ***1Mfor diagram*** ***3M for explanation***

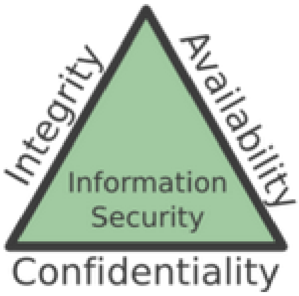
4. The receiver calculates the message digest from the plain text or message he received.

5. Receiver decrypts the encrypted message digest using the sender's public key. If both the MDs are not same then the plaintext or message is modified after signing.



Advantages of Digital Signatures

- Speed: Businesses no longer have to wait for paper documents to be sent by courier. Contracts are easily written, completed, and signed by all concerned parties in a little amount of time no matter how far the parties are geographically.
- Costs: Using postal or courier services for paper documents is much more expensive compared to using digital signatures on electronic documents.
- Security: The use of digital signatures and electronic documents reduces risks of documents being intercepted, read, destroyed, or altered while in transit.
- Authenticity: An electronic document signed with a digital signature can stand up in court just as well as any other signed paper document.
- Non-Repudiation: Signing an electronic document digitally identifies you as the signatory and that cannot be later denied.
- Time-Stamp: By time-stamping your digital signatures, you will clearly know when the document was signed

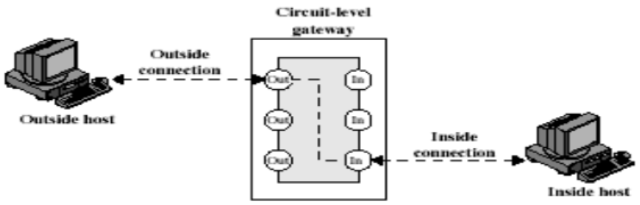
5.	**a)**	**Attempt any <u>TWO</u> of the following** **Define Information. Explain the basic principle of information security.**	**12** **6M**
	Ans.	**Information** is organized or classified data, which has some meaningful values for the receiver. Information is the processed data on which knowledge, decisions and actions are based. For the decision to be meaningful, the processed data must qualify for the following characteristics • **Timely** − Information should be available when required. • **Accuracy** − Information should be accurate. • **Completeness** − Information should be complete. **Basic Principles of information security**  Integrity Availability Information Security Confidentiality Fig CIA Triad of information security 1. Confidentiality: The goal of confidentiality is to ensure that only those individuals who have the authority can view a piece of information, the principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message. 2. Authentication helps to establish proof of identities. Authentication process ensures that the origin of a message is correctly identified. Authentication deals with the desire to ensure that an individual is who they claim to be. 3. Integrity: Integrity is a related concept but deals with the generation and modification of data. Only authorized individuals should ever be able to create or change (or delete) information. When the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.	***2M for definition 1M for diagram 3M for principles explanation***

b) **Define & explain.**
i) Circuit Gateway
ii) Honey Pots
iii) Application Gateway

6M

Ans. i) Circuit level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outer host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed. A typical use of Circuit level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application level or proxy service on inbound connections and circuit level functions for outbound connections.

2M for each definition and explanation

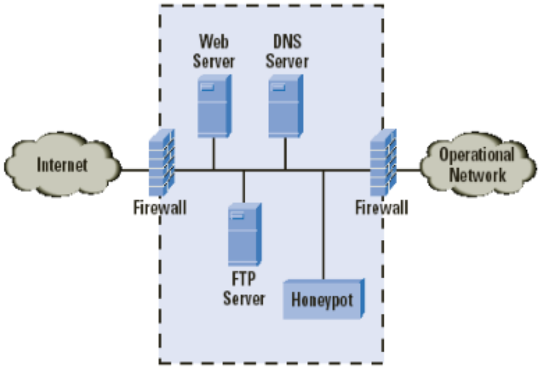


ii) Honey Pots

A relatively recent innovation in intrusion detection technology is the honey pot. Honey pots are decoy systems that are designed to lure a potential attacker away from critical systems. Honey pots are designed to:

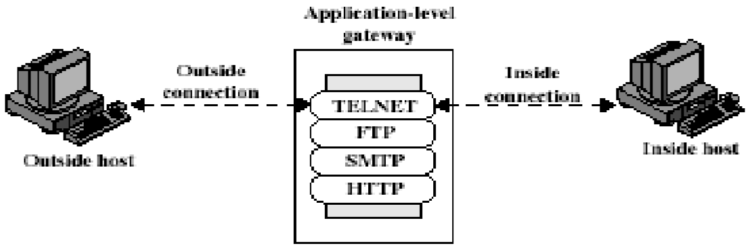
- divert an attacker from accessing critical systems
- collect information about the attacker's activity

It encourages the attacker to stay on the system long enough for administrators to respond. These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn’t access. Thus, any access to the honey pot is suspect.



iii) Application Gateway

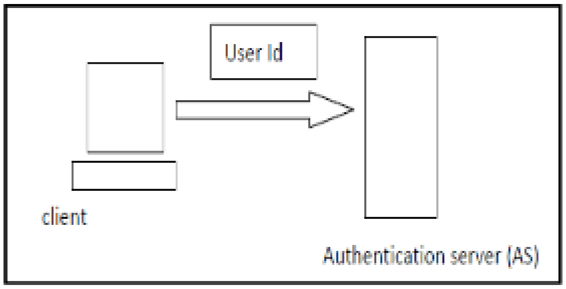
An Application level gateway, also called a proxy server, acts as a relay of application level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
Application level gateways tend to be more secure than packet filters. It is easy to log and audit all incoming traffic at the application level. A prime disadvantage is the additional processing overhead on each connection.



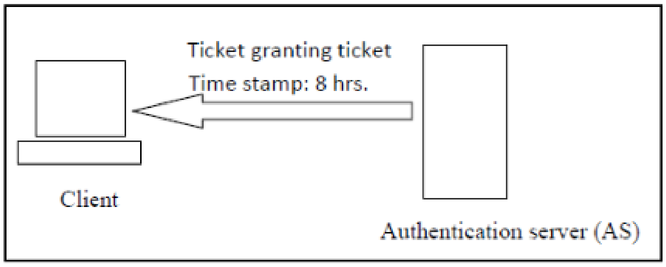
	c) Ans	**Explain the working of Kerberos** Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.	**6M** ***6M for relevant steps***

The entire process takes a total of eight steps, as shown below.

1. The authentication service, or AS, receivers the request by the client and verifies that the Client is indeed the computer it claims to be. This is usually just a simple database lookup of the user's ID.

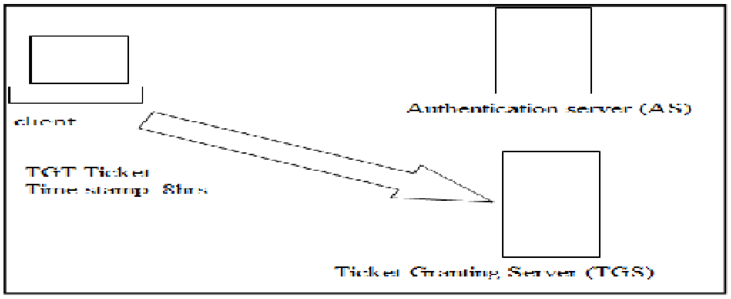


2. Upon verification, a timestamp is crated. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours. The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless. (This is used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

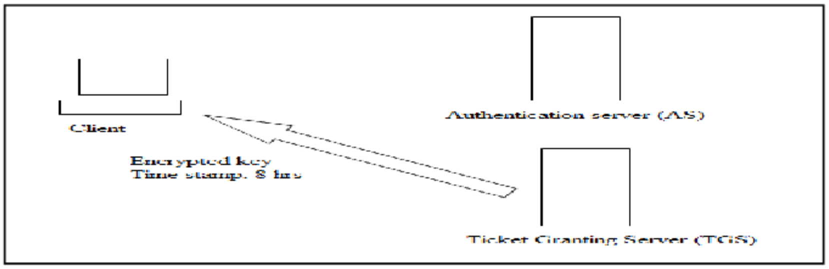


3. The key is sent back to the client in the form of a ticket-granting ticket, or TGT. This is a simple ticket that is issued by the authentication service. It is used for authentication the client for future reference.

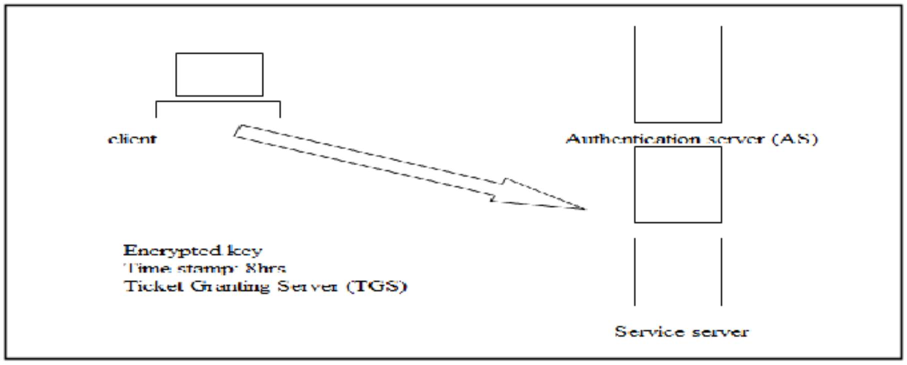
4. The client submits the ticket-granting ticket to the ticket-granting server, or TGS, to get authenticated.



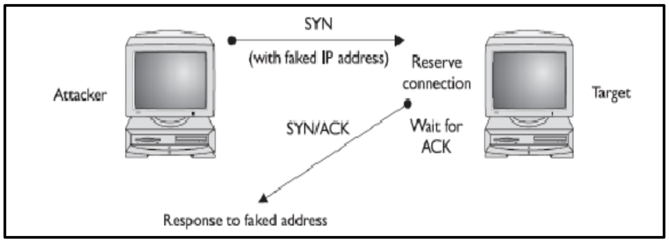
5. The TGS creates an encrypted key with a timestamp, and grants the client a service ticket.



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



7. The service server decrypts the key, and makes sure the timestamp is still valid. If it is, the
service contacts the key distribution center to receive a session that is returned to the client.
8. The client decrypts the ticket. If the keys are still valid,
communication is initiated between client and server.

6.		**Attempt any <u>TWO</u> of the following:**	**12**
	a)	**Explain DOS with neat diagram.**	**6M**
	Ans.	Denial Of Service Attack: Denial of service (DOS) attack scan exploits a known vulnerability in a specific application or operating system, or they may attack features (or weaknesses) in specific protocols or services. In this form of attack, the attacker is attempting to deny authorized users access either to specific information or to the computer system or network itself. The purpose of such an attack can be simply to prevent access to the target system, or the attack can be used in conjunction with other actions in order to gain unauthorized access to a computer or network. SYN flooding is an example of a DOS attack that takes advantage of the way TCP/IP networks were designed to function, and it can be used to illustrate the basic principles of any DOS attack. SYN flooding utilizes the TCP three-way handshake that is used to establish a connection between two systems. In a SYN flooding attack, the attacker sends fake communication requests to the targeted system. Each of these requests will be answered by the target system, which then waits for the third part of the handshake. Since the requests are fake the target will wait for responses that will never come, as shown in Figure.  SYN (with faked IP address) Reserve connection Attacker Target SYN/ACK Wait for ACK Response to faked address The target system will drop these connections after a specific time-out period, but if the attacker sends requests faster than the time-out period eliminates them, the system will quickly be filled with requests. The number of connections a system can support is finite, so when more requests come in than can be processed, the system will soon be reserving all its connections for fake requests. At this point, any further requests are simply dropped (ignored), and legitimate users who want to connect to the target system will not be able to. Use of the system has thus been denied to them.	***2M for diagram*** ***4M for explanation***

b) **Explain Public Key Infrastructure with example.** **6M**

3M Explanation
1M diagram
2M for example

Ans. A **public key infrastructure** (**PKI**) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

PKI is the governing body behind issuing digital certificates. It helps to protect confidential data and gives unique identities to users and systems. Thus, it ensures security in communications.

The public key infrastructure uses a pair of keys: the public key and the private key to achieve security. The public keys are prone to attacks and thus an intact infrastructure is needed to maintain them.

PKI identifies a public key along with its purpose. It usually consists of the following components:

- A digital certificate also called a public key certificate
- Private Key tokens
- Registration authority
- Certification authority
- CMS or Certification management system

Working on a PKI:

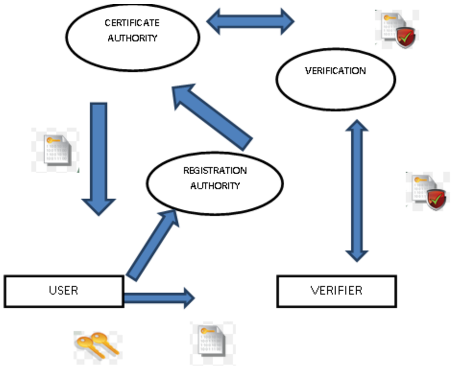
PKI and Encryption: The root of PKI involves the use of cryptography and encryption techniques. Both symmetric and asymmetric encryption uses a public key. There is always a risk of MITM (Man in the middle). This issue is resolved by a PKI using digital certificates. It gives identities to keys in order to make the verification of owners easy and accurate.

Public Key Certificate or Digital Certificate: Digital certificates are issued to people and electronic systems to uniquely identify them in the digital world.

- The Certification Authority (CA) stores the public key of a user along with other information about the client in the digital certificate. The information is signed and a digital signature is also included in the certificate.
- The affirmation for the public key then thus be retrieved by validating the signature using the public key of the Certification Authority.

Certifying Authorities: A CA issues and verifies certificates. This authority makes sure that the information in a certificate is real and correct and it also digitally signs the certificate. A CA or **Certifying Authority performs these basic roles**:

- Generates the key pairs – This key pair generated by the CA can be either independent or in collaboration with the client.
- Issuing of the digital certificates – When the client successfully provides the right details about his identity, the CA issues a certificate to the client. Then CA further signs this certificate digitally so that no changes can be made to the information.
- Publishing of certificates – The CA publishes the certificates so that the users can find them. They can do this by either publishing them in an electronic telephone directory or by sending them out to other people.
- Verification of certificate – CA gives a public key that helps in verifying if the access attempt is authorized or not.
- Revocation – In case of suspicious behavior of a client or loss of trust in them, the CA has the power to revoke the digital certificate.



The most popular usage example of PKI (Public Key Infrastructure) is the HTTPS (Hypertext Transfer Protocol Secure) protocol. HTTPS is a combination of the HTTP (Hypertext Transfer Protocol) and SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols to provide encrypted communication and secure identification of a Web server.

In HTTPS, the Web server's PKI certificate is used by the browser for two purposes:

		Validate the identity of the Web server by verify the CA's digital signature in the certificate. Encrypt a secret key to be securely delivered to the Web server. The secret key will be used to encrypt actual data to be exchanged between the browser and the Web server. Other examples of PKI (Public Key Infrastructure) are: Digital signature - The sender of a digital message uses his/her private key to generate a digital signature attached to the message. The receiver uses the sender's certificate to verify the digital signature to ensure the message was sent by the claimed sender. Encryption of documents - The sender of a digital message uses the receiver's certificate to encrypt the message to protect the confidentiality of the message. Only the receiver who can use his/her private key decrypt the message. Digital identification - User's certificate is stored in a smart card to be used to verify card holder's identities. **(CONSIDER ANY ONE EXAMPLE)**	
	c) **Ans.**	**Explain Policies, configuration & limitations of firewall.** Policies of firewall: All traffic from inside to outside and vice versa must pass through the firewall. To achieve this all access to local network must first be physically blocked and access only via the firewall should be permitted. As per local security policy traffic should be permitted. The firewall itself must be strong enough so as to render attacks on it useless. **Configuration of firewall** There are 3 common firewall configurations. 1. Screened host firewall, single-homed bastion configuration 2. Screened host firewall, dual homed bastion configuration 3. Screened subnet firewall configuration **1. Screened host firewall, single-homed bastion configuration** In this type of configuration a firewall consists of following parts i)A packet filtering router (ii)An application gateway.	**6M** ***1M for policies*** ***1M for listing configuration*** ***2M for configuration, any one can be explained*** ***2M for limitation, any two points***

The main purpose of this type is as follows:•Packet filter is used to ensure that incoming data is allowed only if it is destined for application gateway, by verifying the destination address field of incoming IP packet. It also performs the same task on outing data by checking the source address field of outgoing IP packet.

•Application gateway is used to perform authentication and proxy function. Here Internal users are connected to both application gateway as well as to packet filters therefore if packet filter is successfully attacked then the whole Internal Network is opened to the attacker

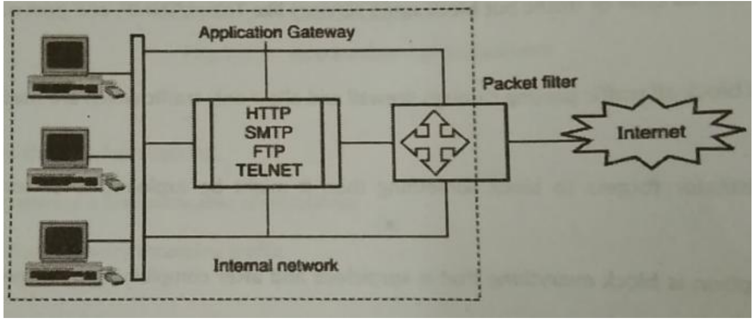


Fig single homed bastion configuration

2. Screened host firewall, dual homed bastion configuration

To overcome the disadvantage of a screened host firewall, single homed bastion configuration, another configuration is available known as screened host firewall, Dual homed bastion. n this, direct connections between internal hosts and packet filter are avoided. As it provide connection between packet filter and application gateway, which has separate connection with the internal hosts. Now if the packet filter is successfully attacked. Only application gateway is visible to attacker. It will provide security to internal hosts.

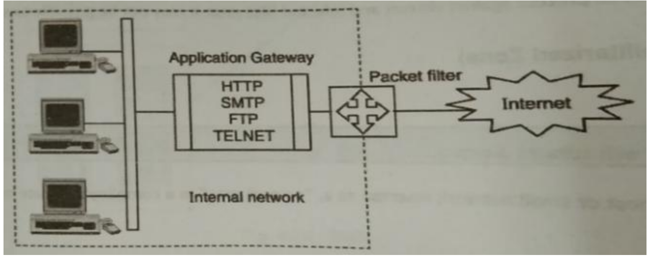


Fig dual homed bastion configuration

3. Screened subnet firewall configuration

It provides the highest security among all firewall configurations. It is improved version over all the available scheme of firewall configuration. It uses two packet filters, one between the internet and application gateway and another between the application gateway and the internal network. Thus this configuration achieves 3 levels of security for an attacker to break into.

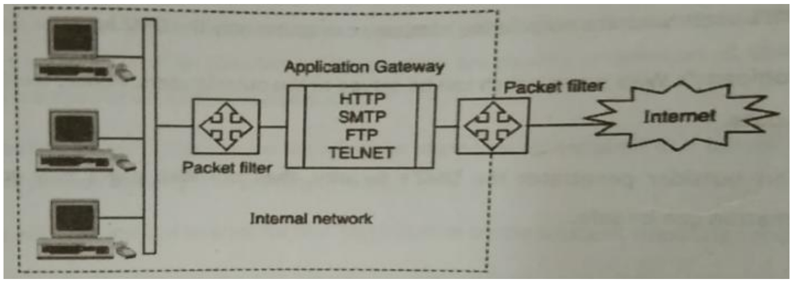


Fig Screened subnet firewall configuration

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