SUMMER– 18 EXAMINATION

Subject Name: Computer Security **Model Answer** **Subject Code:** 17514

Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills.
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

Q. No.	Sub Q. N.	Answers	Marking Scheme
1.	**(A)**	**Attempt any THREE:**	**12 Marks**
	(a)	**What is Computer Security & its need?**	**4M**
	Ans:	Computer Security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. **Need of computer Security:** 1. For prevention of data theft such as bank account numbers, credit card information, passwords, work related documents or sheets, etc. 2. To make data remain safe and confidential. 3. To provide confidentiality which ensures that only those individuals should ever be able to view data they are not entitled to. 4. To provide integrity which ensures that only authorized individuals should ever be able change or modify information. 5. To provide availability which ensure that the data or system itself is available for use when authorized user wants it. 6. To provide authentication which deals with the desire to ensure that an authorized individual. **7.** To provide non-repudiation which deals with the ability to verify that message has been sent and received by an authorized user.	**(Definition :1 mark, Need: Any three points:1 mark each or CIA Model Explanation: 3 marks)**

OR

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

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

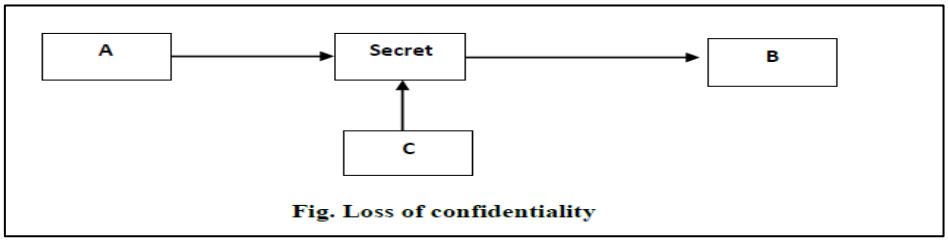


Fig. Loss of confidentiality

Here, the user of a computer A send a message to user of computer B. another user C gets access to this message, which is not desired and therefore, defeats the purpose of Confidentiality.

This type of attack is also called as **interception.**

2. 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**.

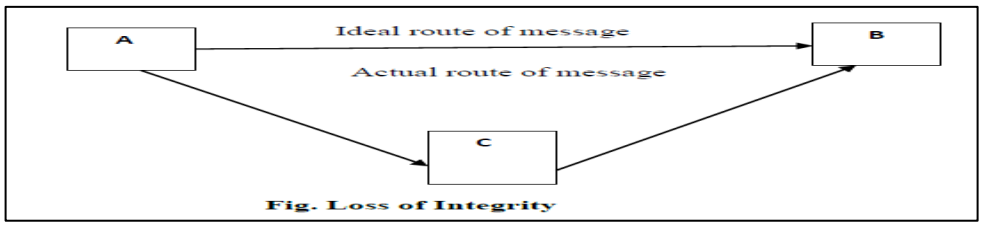


Fig. Loss of Integrity

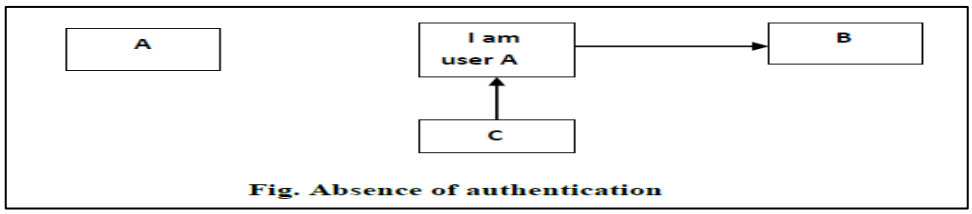


Fig. Absence of authentication

3. 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.**

4. **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.

	(b)	**Explain criteria for password selection.**	**4M**
	Ans:	**There are four basic techniques passwords selection strategies:** **a) User education:** Tell the importance of hard-to-guess passwords to the users and provide guidelines for selecting strong password. **b) Computer generated password:** Computer generated passwords are random in nature so difficult for user to remember it and may note down somewhere. **c) Reactive password checking:** the system periodically runs its own password cracker program to find out guessable passwords. If the system finds any such password, the system cancels it and notifies the user. **d) Proactive password checking:** It is a most promising approach to improve password security. In this scheme, a user is allowed to select his own password, if password is allowable then allow or reject it.	**(Any 4 Criteria: 1mark each)**
	(c)	**Explain one time pad. technique.**	**4M**
	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	**(Explanation: 2 marks, Example: 2 marks)**

Steps for One time pad :

1. The key should be as long as the message
2. Key and plain text calculated modulo 26
3. 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”

Fig: One Time Pad

```
     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
```

OR

Assume :

PLAIN TEXT	M	A	H	A	R	A	S	H	T	R	A

And

ONE-TIME-PAD	V	I	R	A	T	K	O	H	A	L	I

Then using following values:

PLAIN TEXT	A	B	C	D	E	F	G	H	I	J	K	L	M
VALUES	0	1	2	3	4	5	6	7	8	9	10	11	12

PLAIN TEXT	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
VALUES	13	14	15	16	17	18	19	20	21	22	23	24	25

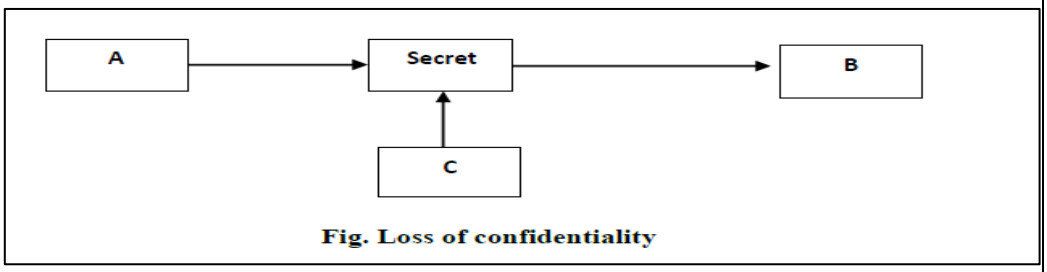
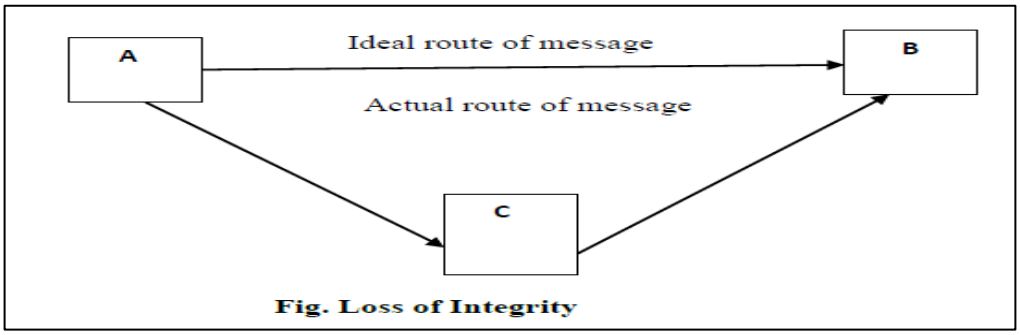
PLAIN TEXT	M	A	H	A	R	A	S	H	T	R	A
VALUES	12	0	7	1	16	0	18	7	19	17	0
ONE-TIME-PAD	V	I	R	A	T	K	O	H	A	L	I
VALUES	21	8	17	0	19	10	14	7	0	11	7
INITIAL TOTAL	33	8	24	1	35	10	32	14	19	28	7
SUBTRACT 26 IF 11TH ROW IS >25	26	0	0	0	26	0	26	0	0	26	0
	7	8	24	1	9	10	6	14	19	2	7
CIPHER-TEXT	H	I	Y	B	J	K	G	O	T	C	H

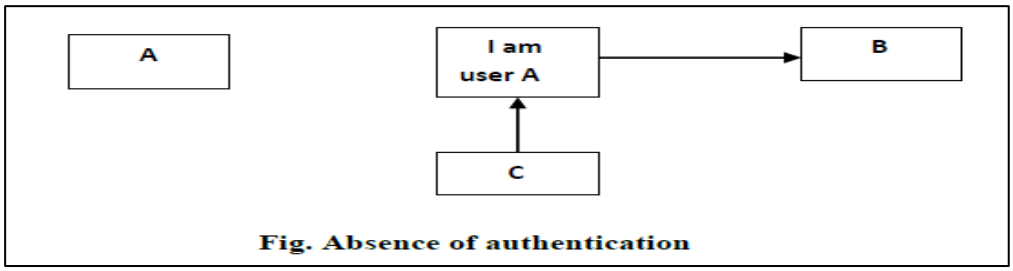
	(d)	**Define Counter Measure in computer system & threats types at least four for computers.**	**4M**
	Ans:	**Counter measure:** Countermeasure is a defensive technology method used to prevent an exploit from successfully occurring once a threat has been detected. Service patches and access control lists are also considered to be types of countermeasures **Threats Types:** Following are threats to security. 1. Virus & worms 2. Intruders 3. Insiders 4. Criminal organization 5. Terrorists 6. Information warfare 7. Avenues of attack 8. 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. 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:** 1. Extremely patient as time consuming More dangerous than outsiders 2. Outsiders Insiders 3. Keep trying attacks till success As they have the access and knowledge to cause immediate damage to organization 4. Individual or a small group of attackers They can be more in numbers who are	**(Definition of counter measure: 1 mark, Any Four threats types: 3 marks)**

5. Next level of this group is script writers, i.e. Elite hackers are of three types: Masquerader, Misfeasor, Clandestine user is misuse of access given by insiders directly or indirectly access the organization.
6. They may give remote access to the Organization
7. Intruders are authorized or unauthorized users who are trying access the system or network.
8. They are hackers or crackers
9. Intruders are illegal users.
10. Less dangerous than insiders They have to study or to gain knowledge about the security system
11. They do not have access to system.
12. Many security mechanisms are used to protect system from Intruders.

Insiders:

- More dangerous than outsiders As they 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.

	(B)	**Attempt any ONE:**	**6 Marks**
	(a)	**Explain Security Basics in detail.**	**6M**
	Ans:	**1. Confidentiality:** The principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message. Example of compromising the Confidentiality of a message is shown in fig:  **Fig. Loss of confidentiality** Here, the user of a computer A send a message to user of computer B. another user C gets access to this message, which is not desired and therefore, defeats the purpose of Confidentiality. This type of attack is also called as **interception.** **2. 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** **3. 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	**(Any three Security Basics points Explanation: 2 marks Each)**

		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** **4**. **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.	
	(b)	**Explain following terms of Intellectual property:** **(i) Copyright, (ii) Patent, (iii) Trademark.**	**6M**
	Ans:	**(i) Copyright** Copyright is a form of IPR concerned with protecting works of human intellect. The domain of copyright is literary and artistic works, might that be writings, musicals and works of fine arts, such as paintings and sculptures, as well as technology-based works such as computer programs and electronic databases. **(ii) Patent** Patent is an exclusive right granted by law to an inventor or assignee to prevent others from commercially benefiting from his/her patented invention without permission, for a limited period of time in exchange for detailed public disclosure of patented invention. **(iii) Trademark** A trademark is a sign that individualizes the goods or services of a given enterprise and distinguishes them from those of competitors. To fall under law protection, a trademark must be distinctive, and not deceptive, illegal or immoral.	**(Copyright : 2 marks, Patent: 2 marks, Trademark : 2 marks)**

2.		Attempt any TWO:	16 Marks
	(a)	Explain risk & threat analysis w.r.t. (i) Assets, (ii) Threats, (iii) Vulnerabilities	8M
	Ans:	**Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: **1.** The adverse impacts that would arise if the circumstance or event occurs; and **2.** The likelihood of occurrence. **(i) Assets** Asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware, software and confidential information. **(ii) Threats** The term "threat" refers to the source and means of a particular type of attack. It is a set of things which has potential to loss or harm to computer system &network. A threat assessment is performed to determine the best approaches to securing a system against a particular threat, or class of threat. Penetration testing exercises are substantially focused on assessing threat profiles, to help one develop effective countermeasures against the types of attacks represented by a given threat. Where risk assessments focus more on analysing the potential and tendency of one's resources to fall prey to various attacks, threat assessments focus more on analysing the attacker's resources. Analysing threats can help one develop specific security policies to implement in line with policy priorities and understand the specific implementation needs for securing one's resources. **(iii) Vulnerabilities** It is a weakness in computer system & network. The term "vulnerability" refers to the security flaws in a system that allows an attack to be successful. Vulnerability testing should be performed on an on-going basis by the parties responsible for resolving such vulnerabilities, and helps to provide data used to identify unexpected dangers to security that need to be addressed. Such vulnerabilities are not particular to technology — they can also apply to social factors such as individual authentication and authorization policies. Testing for vulnerabilities is useful for maintaining on-going security, allowing the people responsible for the security of one's resources to respond effectively to new dangers as they arise. It is also invaluable for policy and technology development, and as part of a technology selection process;	**(Risk: 2 marks, Assets: 2 marks, Threats: 2 marks, Vulnerabilities:2 marks)**

selecting the right technology early on can ensure significant savings in time, money, and other business costs further down the line.

(b) Describe Access control policies in detail. **8M**

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

(Explanation of access control: 2 marks; Any three Access Control Policies: 2 marks Each)

It can be represented using **Access Control matrix or List**:

	Process 1	Process 2	File 1	File 2	Printer
Process 1	Read, Write, Execute	---	Read	Read	Write
Process 2	Execute	Read, Write, Execute	Read	Read, Write	Write

Various access controls are:

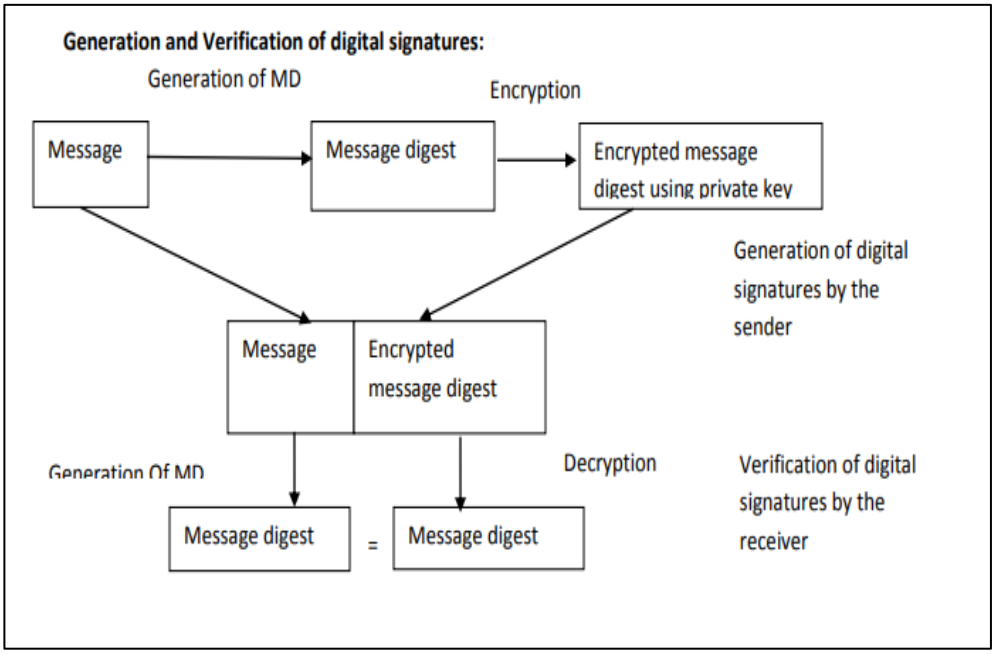
- **Discretionary Access control (DAC)**: Restricting access to objects based on the identity of subjects and or groups to which they belongs to, it is conditional, basically used by military to control access on system. UNIX based System is common method to permit user for read/write and execute

- **Mandatory Access control (MAC):** It is used in environments where different levels of security are classified. It is much more restrictive. It is sensitivity based restriction, formal authorization subject to sensitivity. In MAC the owner or User cannot determine whether access is granted to or not. i.e. Operating system rights. Security mechanism controls access to all objects and individual cannot change that access.

- **Role Based Access Control (RBAC):** Each user can be assigned specific access permission for objects associated with computer or network. Set of roles

		are defined. Role in-turn assigns access permissions which are necessary to perform role. • Different User will be granted different permissions to do specific duties as per their classification.	
	(c)	**Describe digital signature mechanism with neat diagram.**	**8M**
	Ans:	**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.	**(Any suitable Diagram: 4 marks, Explanation: 4 mark)**

Generation and Verification of digital signature:



Procedure:

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.
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.

3.		**Attempt any FOUR:**	**16 Marks**
	(a)	**Describe proxy server.**	**4M**
	Ans:	Proxy server is an intermediary server between client and the internet. Proxy servers offers the • following basic functionalities: • Firewall and network data filtering.	**(Diagram: 2marks, Explanation: 2 marks)**

- Network connection sharing
- Data caching

Purpose of Proxy Servers

Following are the reasons to use proxy servers:

- Monitoring and Filtering
- Improving performance
- Translation
- Accessing services anonymously
- Security

1. Monitoring and Filtering
   - Proxy servers allow us to do several kind of filtering such as:
   - Content Filtering

2. Filtering encrypted data
   - Bypass filters
   - Logging and eavesdropping
   - Improving performance
   - It fastens the service by process of retrieving content from the cache which was saved when previous request was made by the client.

3. Translation
   - It helps to customize the source site for local users by excluding source content or substituting
   - Source content with original local content. In this the traffic from the global users is routed to the
   - Source website through Translation proxy.

4. Accessing services anonymously
   - In this the destination server receives the request from the anonymzing proxy server and thus does not receive information about the end user.

5. Security
   - Since the proxy server hides the identity of the user hence it protects from spam and the hacker attacks.

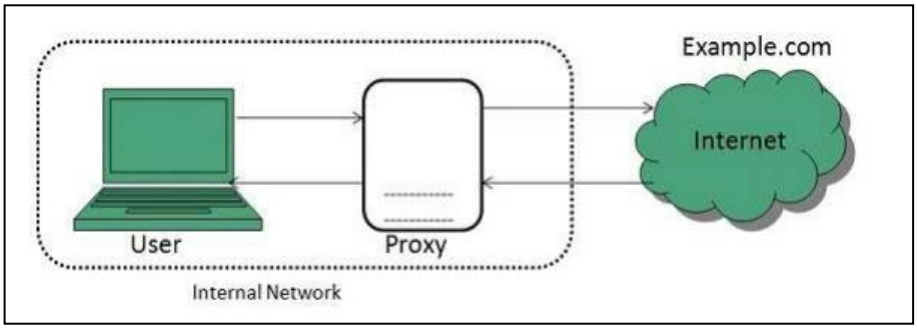


Fig. Proxy Server

	(b)	**Describe in brief :** **(i) Piggy backing** **(ii) Shoulder Surfing**	**4M**
	Ans:	**(i) Piggy backing:** • 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 a legally and ethically controversial practice, with laws that vary by jurisdiction around the world. While completely outlawed or regulated in some places, it is permitted in others. The process of sending data along with the acknowledgment is called piggybacking. Piggybacking is distinct from war driving, which involves only the logging or mapping of the existence of access points. • 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: 2 marks, Shoulder surfing: 2 marks)**

		• Piggybacking, in a wireless communications context, is the unauthorized access of a wireless LAN. Piggybacking is sometimes referred to as "Wi-Fi squatting." • The usual purpose of piggybacking is simply to gain free network access rather than any malicious intent, but it can slow down data transfer for legitimate users of the network. **(ii) Shoulder Surfing:** • Shoulder surfingis 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. • To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. • 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.	
	(c)	**Decipher a message :** **"TSACT SGCEB HISRM SELNV ISEEE AVITP" using a Rail fence using 10 Columns & 3 rails & retrieve original massage.**	**4M**
	Ans:	1. The number of columns in rail fence cipher remains equal to the length of plain-text message. 2. Hence, rail matrix can be constructed accordingly. Once we've got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively). 3. Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.	**(Decryption Algorithm: 2 marks, Original Message: 2 marks)**

T	S	A	C	T	S	G	C	E	B
H	I	S	R	M	S	E	L	N	V
I	S	E	E	E	A	V	I	T	P

Original Message:- THIS IS A SECRET MESSAGE VCLIENT BVP

	(d)	**Describe VPN (Virtual private network) in brief & define DMZ.**	**4M**
	Ans:	**VPN(Virtual Private Network) :** A VPN or Virtual Private Network is a network connection that enables you to create a secure connection over the public Internet to private networks at a remote location. With a VPN, all network traffic (data, voice, and video) goes through a secure virtual tunnel between the host device (client) and the VPN provider's servers, and is encrypted. VPN technology uses a combination of features such as encryption, tunnelling protocols, data encapsulation, and certified connections to provide you with a secure connection to private networks and to protect your identity. VPN connections technically give you all the benefits of a Local Area Network (LAN), which is similar to that found in many offices but without requiring a hard-wired connection. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.	**(Explanation of VPN: 3 marks, Definition of DMZ: 1 mark)**

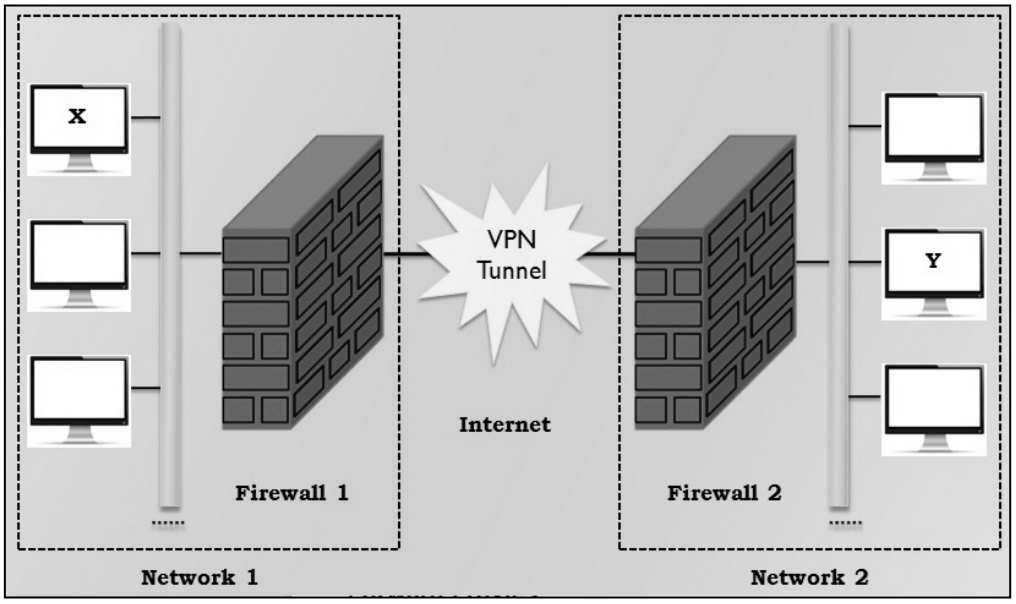


Fig: Virtual Private Network (VPN)

		DMZ: It is a computer host or a small network inserted as a neutral zone between company's private network and outside public network. It prevents direct Access to a server that has company data. 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.	
	(e)	**Write the steps to create active directory in windows server OS.**	**4M**
	Ans:	Steps to create active directory in windows server OS: **1.** Start Server Manager. **2.** Select **Roles** in the left pane, and then click on **Add Roles** in the center console. **3.** Depending on whether you checked off to skip the **Before You Begin** page while installing another service, you will now see warning pages telling you to make sure you have strong security, static IP, and latest patches before adding roles to your server. If you get this page, then just click **Next**. **4.** In the **Select Server Roles** window we are going to place a check next to **Active Directory Domain Services** and click **Next**. **5.** The information page on Active Directory Domain Services will give the following warnings, which after reading, you should click **Next**: • Install a minimum of two Domain Controllers to provide redundancy against server outage (which would prevent users from logging in with only one) • AD DS requires DNS which if not installed you will be prompted for • After installing AD DS you must run dcpromo.exe to upgrade to a fully functional domain controller • Installing AD DS will also install DFS Namespaces, DFS Replication, and Filer Replication services which are required by Directory Service **6.** The **Confirm Installation Selections** screen will show you some information messages and warn that the server may need to be restarted after installation. Review the information and then click **Next**. **7.** The **Installation Results** screen will hopefully show **Installation Succeeded**, and an additional warning about running dcpromo.exe (I think they really want us to run dcpromo). After you review the, click **Close**.	**(Correct steps: 4 marks)**

		8. After the Installation Wizard closes you will see that server manager is showing that **Active Directory Domain Services** is still not running. This is because we have not run dcpromo yet. **9.** Click on the **Start** button, type **dcpromo.exe** in the search box and either hit **Enter** or click on the search result. **10.** The **Active Directory Domain Services Installation Wizard** will now start.	
4.	**a)**	**Attempt any THREE:**	**12 Marks**
	(i)	**What are the techniques for transforming plain text to cipher text? Explain any one in detail.**	**4M**
	Ans:	Transforming plain text to cipher text is the science of encrypting information scheme is based on algorithms. **1. Substitution technique** a) Caesar cipher b) Modified version of Caesar cipher c) Mono-alphabetic cipher d) Vigener's cipher **2. Transposition technique** a) Rail fence b) Route cipher c) Columnar cipher **3.Steganography** **4. Hashing** **5. Symmetric and asymmetric cryptography** **6. DES (dat**a encryption standard) **1. Caesar cipher:** It is proposed by Julius Caesar. In cryptography Caesar cipher also known as Caesar's cipher/code, shift cipher/code. It is one of the simplest and most widely known encryption techniques. It is a type of substitution technique in which each letter in the plain text is replaced by a letter some fixed number of position down the alphabet. For example, with a shift of 3, A would be replaced by D, B would became E, and so on as shown in the table below.	**(Enlisting of Techniques: 2 marks, Explanation of any one technique: 2 marks)**

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

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

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

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

2. 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: 1. The message is written out in rows of a fixed length. 2. Read out again column by column according to given order or in random order. 3. According to order write cipher text.

Example

The key for the columnar transposition cipher is a keyword e.g. ORANGE. The row length that is used is the same as the length of the keyword.

To encrypt a below plaintext COMPUTER PROGRAMMING

O	R	A	N	G	E
C	O	M	P	U	T
E	R	P	R	O	G
R	A	M	M	I	N
G	L	E	X	X	M

In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes

decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.

5	6	1	4	3	2
O	R	A	N	G	E
C	O	M	P	U	T
E	R	P	R	O	G
R	A	M	M	I	N
G	L	E	X	X	M

The Encrypted text or Cipher text is: MPMET GNMUO IXPRM XCERG ORAL (Written in blocks of Five)

3. **Rail Fence Technique:** It is one of the easiest transposition techniques to create cipher text. When plain text message is codified using any suitable scheme, the resulting message is called Cipher text or Cipher.

Steps are:

Plain text = **COMPUTER SECURITY**

1. Write down Plain text as sequence of diagonal.

Read Plain text written in Step 1 as sequence of rows.

As ,

CMUESCRT,

Followed with

OPTREUIY

Then concatenate these two sequences of text as one to create following

Cipher text: CMUESCRTOPTREUIY

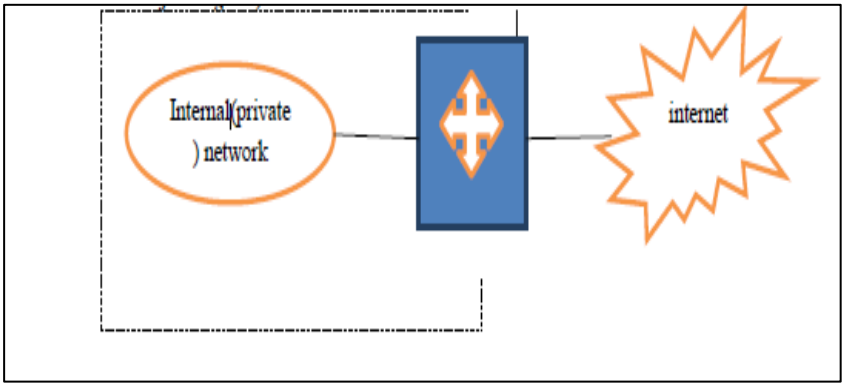
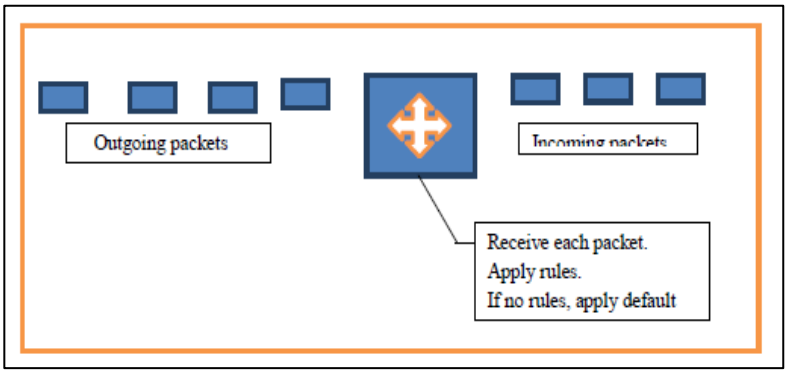
Following details will be OPTIONAL.

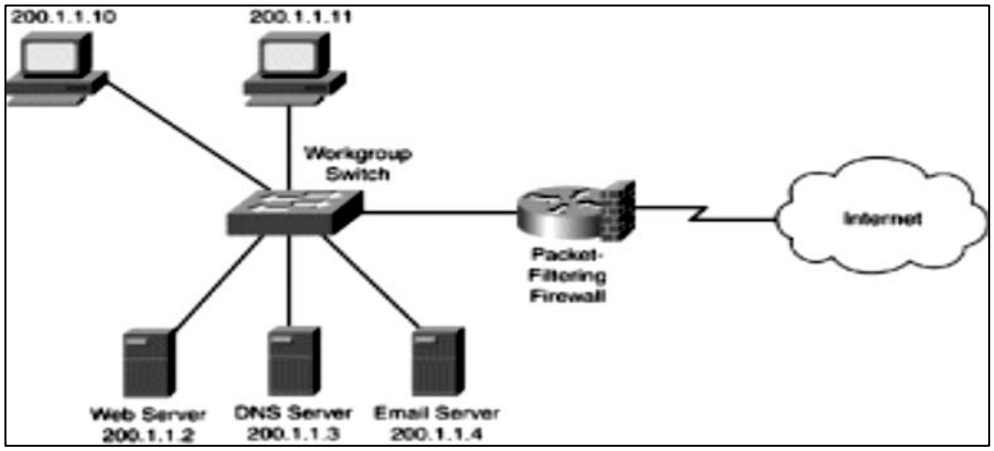
Some other examples of rail fence techniques

1. The rail-fence cipher is inscribed by zigzag pattern and extracted by rows.

			N						M						R						G			
		I		F				E		E				A		R				N		N		
	E				O		C				N		S				I		I				O	
R						R						T						V						W

Ciphertext NMRGI FEEAR NNEOC NSIIO RRTVW

	(ii)	**Describe packet filter router firewall with neat diagram.**	**4M**
	Ans:	  **Packet** A packet filtering router firewall applies a set of rules to each packet and based on outcome, decides to either forward or discard the packet. Such a firewall implementation involves a router, which is configured to filter packets going in either direction i.e. from the local network to the outside world and vice versa. A packet filter performs the following functions. 1. Receive each packet as it arrives. 2. Pass the packet through a set of rules, based on the contents of the IP and transport header fields of the packet. If there is a match with one of the set rule, decides whether to accept or discard the packet based on that rule. 3. If there is no match with any rule, take the default action. It can be discard all packets or accept all packets. **Advantage:**	**(Diagram: 2 marks, Explanation : 2 marks)**

		The Biggest Advantage of Packet Filtering Firewalls is Cost and Lower Resource Usage and best suited for Smaller Networks. **Disadvantage:** Packet Filtering Firewalls can work only on the Network Layer and these Firewalls do not support Complex rule based models. And it‘s also Vulnerable to Spoofing in some Cases.  **Fig: Packet Filtering Firewall**	
	(iii)	**Explain IT Act, 2008 laws.**	**4M**
	Ans:	IT acts 2008: It is the Information Technology Amendment Act, 2008.the act was developed for IT industries, control e-commerce, to provide e-governance facility and to stop cybercrime attacks. Following are the characteristics of IT ACT 2008: This act provides legal recognition or the transaction i.e. Electronic Data Interchange (EDI) and other electronic communications. This Act also gives facilities for electronic filling of information with the Government agencies. It is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records. **Characteristics of IT Act 2008:** **Different Fraudulent situations:** • Tampering with any computer source code use for a computer, computer programmer computer system or computer network. • Hacking with computer system • Sending offensive or false information through computer or a communicative device. • Receiving or retaining stolen computer resource or communication device.	**(Correct Explanation: 4 marks)**

		• Capturing transmitting or publishing the image of a private area of any person without consent. • Punishment for Cyber terrorism. • Publishing transmitting information which is obscene in electronic form. • Publishing and transmission of containing sexually explicit act or conduct. • Penalty for mis-representation.: imprisonment for a term which may extend to two yearsor with fine up to Rs. 1 lakh or with both. • Penalty for breach of confidentiality and privacy • Punishment for disclosure of information in breach of contract. • Punishment for publishing digital signature certificate false in certain particulars. • Publication for fraudulent purpose. **Features of I.T. Amendment Act 2008:** • Focusing on data privacy • Focusing on information security. • Defining cyber café. • Making digital signature technology neutral. • Defining reasonable security practices to be followed by corporate. • Redefining the role of intermediaries. • Recognizing the role of Indian computer Emergency Response Team. • Inclusion of some additional cybercrimes like child pornography and cyberterrorism. • Authorizing an Inspector to investigate cyber offences.	
	(iv)	**Describe process of application Hardening.**	**4M**
	Ans:	Application Hardening: It is to secure an application against local &Internet-based attacks. In this the functions or components are removed which are not needed, Restrict the access where you can and make sure the application is kept up to date with patches. It includes: **1. Application Patches**- Application patches are supplied from the vendor who sells the application. They are probably come in three varieties: hot fixes, patches & up-grades. **2. 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. **3. 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.	**(Process Explanation: 4 marks)**

		4. **Upgrades:** Upgrades are another popular method of patching application & they are likely to be received with a more positive role than patches. 5. **Web servers:** Web servers are the most common Internet server-side application in use. These are mainly designed to provide content & functionality to remote users through a standard web browser. 6. **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.	
	(B)	**Attempt any ONE :**	**6 Marks**
	(i)	**Explain Malware.**	**6M**
	Ans:	Malware is a software program which is developed to destroy a computer system.These programs runs in victim's computer without any information to the victim, i.e.victim do not know that someone hacked his system. **Types of Malware:** 1. Rootkits 2. Trojan 3. Worm 4. Adware 5. Backdoor 6. RAT – Remote Access Trojan 7. Botnet 8. Downloader Malware 9. Information Stealing Malware 10. Keyloggers 11. Launcher malware **1.Rootkits:** Originally, a rootkit was a set of tools installed by a human attacker on a Unix system, allowing the attacker to gain administrator (root) access. Today, the term rootkit is used more generallyfor concealment routines in a malicious program. Once a malicious program is installed on a system, it is essential that it stays concealed, to avoid detection and disinfection. The same is true when a human attacker breaks into a computer directly. Techniques known as rootkits allow this concealment, by modifying the host's operating system so that the malware is hidden from the user. Rootkits can prevent a malicious process from being visible in the system's list of processes, or keep its files from being read. **2.Trojan:** A Trojan or a Trojan horse as malware is a malicious program functioning as a backdoor. Just like the ancient Greek story of the wooden horse with Greek	**(Definition: 1 mark, Listing of types: 1 mark, Explanation of any four types: 1 mark each)**

troops inside which was used to invade the city of Troy, a Trojan in computing tends to appear like a regular application, media or any other file but containing a malicious payload. Trojans are often spread through social engineering where the victim is fooled into executing the file or application with the Trojan. Most Trojans contain backdoors which can be used by the attacker to steal information, spread other malware or use the infected machine's resources in a botnet. Literally anything is possible when infected with a Trojan which was installed or run with elevated privileges. Trojans in computing have been around for a long time, a few old and popular Trojans are: Netbus, SubSeven or Sub7 and Back Orifice.

3.Worm:

A worm is a piece of malware that replicates itself in order to spread and infect other systems. Computer worms use the network, links, P2P networks, e-mail and exploit vulnerabilities to spread themselves. Often more than one way is used to spread the worm. The difference with a virus is that a virus inserts code into other programs where a worm does not and replicates only itself. Worms do not necessarily contain a payload but most worms do. Worms can also be designed to only spread without a payload.

4.Adware:

Adware as malware is malicious software which presents unwanted advertising to the user. This kind of malware often uses pop-up windows which cannot be closed by the user. Adware is often included with free software and browser toolbars. Malware which is also collecting user data, activity and other information for targeted advertising is called spyware.

5.Backdoor:

A backdoor is a piece of malicious code which allows an attacker to connect to the infected target and take control of the target machine. In most cases there is no authentication required to log in the remote machine other than authentication methods required by the malware. A backdoor is often generated by a Trojan which goes unnoticed if the host has no effective detection mechanisms. Backdoors can use a lot of methods to communicate home. Also port 80 is commonly used by malware over the HTTP protocol because this port is open on most machines connected to the internet.

6.RAT – Remote Access Trojan:

A Remote Access Trojan (RAT), or sometimes called a Remote Administration Tool or Remote Access Tool, is software which allows an attacker to take control of the infected host by the use of a backdoor. We'll call it a Remote Access Trojan in this article to emphasize the maliciousness of this kind of RAT. We are talking

about the malicious RAT's and not the ones which are used by system administrators or software vendors for remote support and troubleshooting. Remote Access Trojans are often included with free software and send as attachment by e-mail.

7.Botnet:

A botnet is a network of remote controlled private computers with backdoors which are being controlled by a command and control server. All infected hosts in the botnet are controlled as a group and receive the same instructions from the server which is controlled by the attacker. Botnets are often used to send spam, to perform distributed denial-of-service (DDoS) attacks or malware distribution.

8.Downloader Malware:

Downloader Malware is malicious software which downloads other malicious software. Attackers often infect a machine with downloader malware when they have gained first access to the system. The downloader malware than infects the target machine silently with other malware.

9.Information Stealing Malware:

Information stealing malware is a collection of malware types which are developed to steal information like credit card numbers, bank account details, account details and other personal information. The collected information is usually send to the attacker who often uses it to gain access to your personal account or to put it up for sale on the deep web. Information stealing malware often comes in the form as keyloggers, password (hash) grabbers and sniffers. The stolen information is often send to a command and control server for further processing.

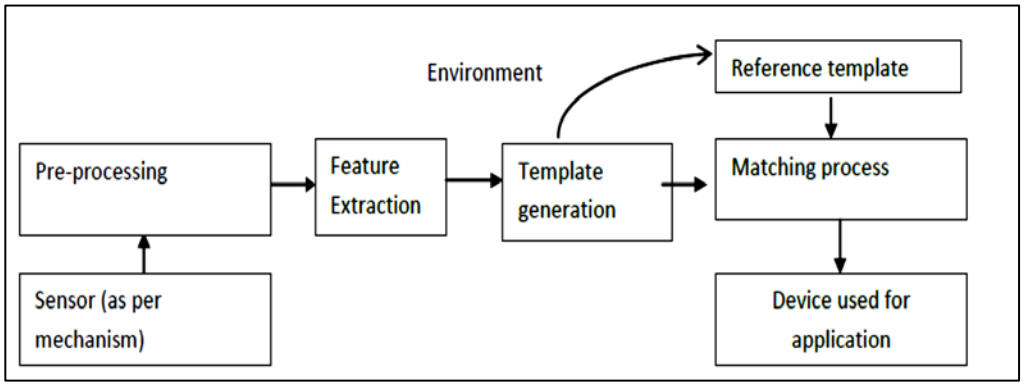
10.Keyloggers:

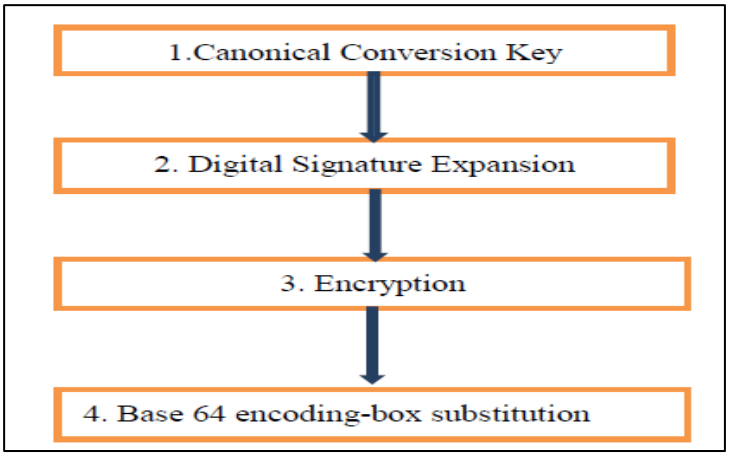
Keylogger malware is a malicious piece of software (or hardware) which records your keystrokes in order to retrieve passwords, conversations and other personal details. The recorded keystrokes are than send to the attacker. A keylogger is a very effective way for attackers to steal passwords because there is no need to crack hashes, decrypt information or to sniff secured connections for passwords.

11.Launcher malware:

A launcher is a piece of malicious software which is used to launch other malware. This piece of malicious software is often combined with downloader malware. The launcher malware often uses stealthy and unconventional methods to launch other malicious code to avoid detection.

	(ii)	**Describe Insiders & Intruders. Who is more dangerous?**	**6M**
	Ans:	**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 They can be more in numbers who are • Next level of this group is script writers, i.e. Elite hackers are of three types: Masquerader, 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 they 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. • 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.	**(Intruders: 2 marks, Insiders: 2marks,Who is dangers Explanation : 2 marks)**

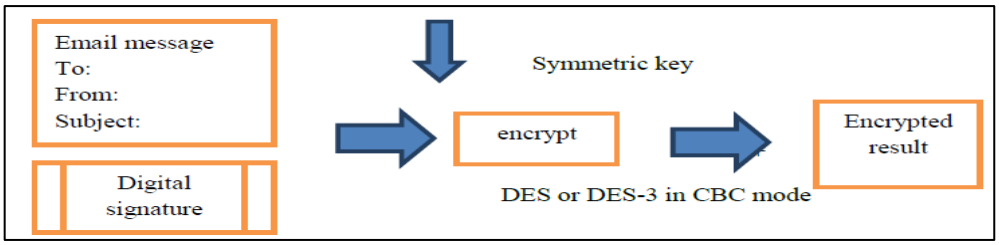
		ii) There is no security mechanism to protect system from Insiders. So they can have all the access to carry out criminal activity like fraud. They have knowledge of the security systems and will be better able to avoid detection.	
5.		**Attempt any TWO :**	**16 Marks**
	(a)	**Explain working of fingerprint mechanism & its limitations.**	**8M**
	Ans:	1. Biometric refers study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral characteristics. 2. Biometric identification is used on the basis of some unique physical attribute of the user that positively identifies the user. Example: finger print recognition, retina and face scan technique, voice synthesis and recognition and so on.  **<u>Fingerprint registration & verification process</u>** 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.	**(Diagram : 3 marks; Explanation : 3 marks; limitation : 2 marks)**

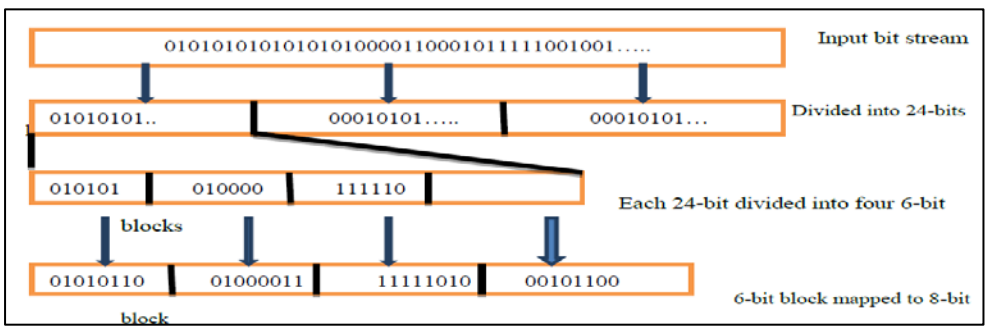
		9. The matching program will analyze the template with the input. This will then be output for any specified use or purpose. **Limitations:-** 1) Using the fingerprint scanner does not take into consideration when a person physically changes 2) The cost of computer hardware and software programs can be expensive 3) Using the fingerprint scanner can lead to false rejections and false acceptance. 4) It can make mistakes with the dryness or dirty of the finger's skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly).	
	(b)	**Describe the working of PEM e-mail security & PGP with reference to e-mail security.**	**8M**
	Ans:	**PEM e-mail security:** PEM supports the 3 main cryptographic functions of encryption, nonrepudiation and message integrity. The steps involved in PEM operation as follows.  **Step 1: canonical conversion**: there is a distinct possibility that the sender and the receiver of an email message use computers that have different architecture and operating systems. PEM transforms each email message into an abstract, canonical representation This means that regardless of the architecture and the operating system of the sending and receiving computers, the email travels in a uniform, independent format.	**(PEM Diagram:2 marks, PEM Explanation: 2 marks; PGP Diagram: 2 marks;, PGP Explanation : 2 marks)**

Step 2: Digital Signature:
-It starts by creating a MD of email message using an algorithm such as MD2 or MD5.
- The MD thus created is then encrypted with sender's private key to form the sender's digital signature.

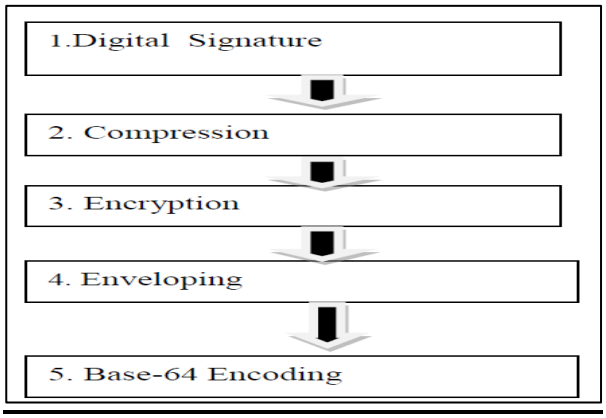
Step 3-encryption:
The original email and the digital signature are encrypted together with a symmetric key.

Step 4: Base- 64 encoding-This process transforms arbitrary binary input into printable character output. The binary input is processed in blocks of 3 octets or 24 bits. These 24 bits are considered to be made up of 4 sets, each of 6 bits. Each such set of 6 bits is mapped into an 8-bit output character in this process.





PGP e-mail security:



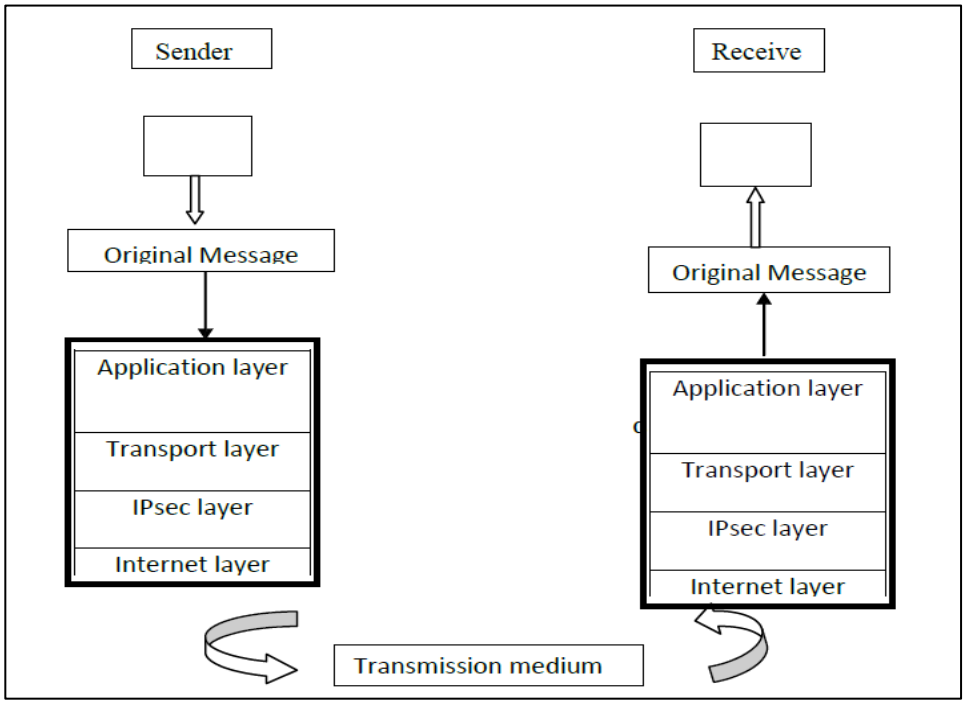
1. **Digital signature:** it consists of the creation a message digest of the email message using SHA-1 algorithm. The resulting MD is then encrypted with the sender‘s private key. The result is the sender‘s digital signature.

2. **Compression:** the input message as well as p digital signature are compressed together to reduce the size of final message that will be transmitted. For this the Lempel-Ziv algorithm is used.

3. **Encryption:** The compressed output of step 2 (i.e. the compressed form of the original email and the digital signature together) are encrypted with a symmetric key.

4. **Digital enveloping:** the symmetric key used for encryption in step 3 is now encrypted with the receiver‘s public key. The output of step 3 and 4 together form a digital envelope.

5. **Base -64 encoding:** this process transforms arbitrary binary input into printable character output. The binary input is processed in blocks of 3 octets (24-bits).these 24 bits are considered to be made up of 4 sets, each of 6 bits. Each such set of 6 bits is mapped into an 8-bit output character in this process.

	(c)	**Give IPSEC configuration. Describe AH & ESP Modes of IPSEC.**	**8M**
	Ans:	**IP sec overview:** 1. It encrypts and seals the transport and application layer data during transmission. It also offers integrity protection for internet layer. 2. 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 all its branches over internet.	**(Diagram: 1 mark, Explanation :1 mark , Explanation of AH and ESP: 3 marks each)**

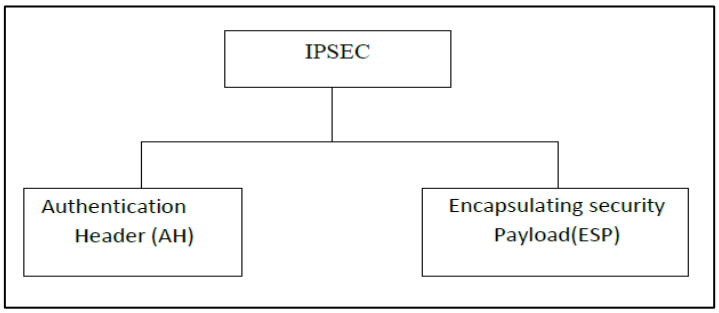
3. **Setup communication with other organization:** Just as IPsec allow connectivity between various branches of an organization, it can also be used to connect the network of different organization together in a secure & inexpensive fashion.

Main advantages of IPsec:

1. IPsec is transparent to end users.
2. There is no need for an user training key, key issuance or revocation.
3. When IPsec is configured to work with firewall it becomes the only entry-exit point for all traffic, making it extra secure.
4. IPsec works at network layer. Hence no changes are needed to upper layers or router, all outgoing & incoming traffic gets protected.
5. IPsec allow travelling staff to have secure access to the corporate network
6. IPsec allows interconnectivity between branches/offices in a very in expensive manner.

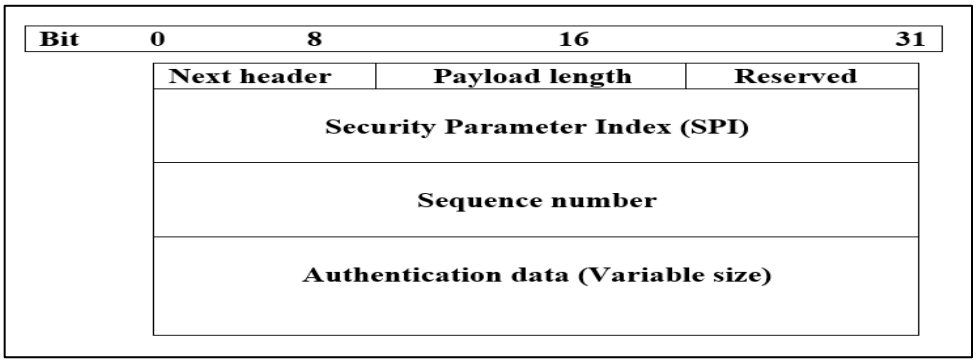
Basic Concept of IPsec Protocol:

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 & 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):

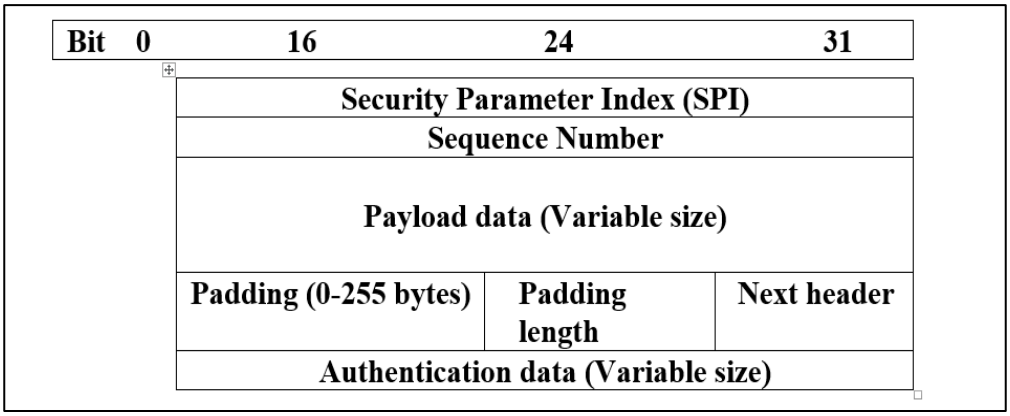
1. Authentication header is an IP Packet (AH) protocol provides authentication, integrity &an optional anti-reply service.
2. The IPsec AH is a header in an IP packet. The AH is simply inserted between IP header & any subsequent packet contents no changes are required to data contents of packet. Security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



Authentication Header (AH) format

Encapsulation Header (ESP):

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.



6.		**Attempt any FOUR :**	**16 Marks**
	(a)	**Describe role of people in security.**	**4M**
		a) Password selection: **1.** User should be able to create their own easy to remember passwords, but should not be easy for someone else to guess or obtain using password cracking utilities.	**(Any 4 point :1 mark each)**

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

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

b) Piggybacking:

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

c) Shoulder surfing:

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

d) Dumpster diving:

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

e) Installing Unauthorized Software/Hardware:

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

f) Access by non-employees:

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

g) Security awareness:

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

h) Individual user responsibilities:

i) Lock the door of office or workspace.

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

iii) Secure storage media which contains sensitive information. iv) Shredding paper containing organizational information before discarding it.(more points can be added).

	(b)	**Explain the concept of Hashing. Give its advantage.**	**4M**
	Ans:	**Hashing** 1. Hashing functions are one of the most commonly used encryption methods. 2. A hash is a special function that performs one-way encryption, meaning that once the algorithm is processed, there is no feasible way to take the cipher text and retrieve the plain text that was used to generate it. 3. The hash code is a function of all bits of the message and provides as error detection capability. A change in any bit or bits results in a change of hash value. 4. A hash value h is generated by a function H of the form h = H(M) where, M is variable length message and H(M) is the fixed length hash value. 5. The hash value is appended to the message at the source at a time when the message is assumed or known to be correct. 6. The receiver authenticates that message by re-computing the hash value. Hash value is not considered to be secret so something is required to protect the hash value. 7. The message plus concatenated Hash code is encrypted using symmetric encryption. Sender and receiver share the same secret key. The message must have come from authorized sender and has not been altered is checked by recomputing and comparing hash code by receiver. **Advantages: (any two)** **1.** It is more efficient to compute a digital signature using a document‘s message digest. **2.** A digest can be made public without revealing the contents of the document from which it derives.	**(Explanation : 3marks, Any two advantages: ½ marks Each)**

		3. It is used for digital authentication must have certain properties that make it secure enough for cryptographic use. **4.** Combining the data message with the secret, and running it through a hash function, a signature is generated in the form of the hash value. The data message is transmitted along with the signature. The recipient combines the received message with the secret, generates a hash value, and checks to make sure it's identical to the signature. The message's authenticity is thus verified.	
	(c)	**Explain Honey Pots.**	**4M**
	Ans:	• Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet. • The honeypot is designed to do the following: 1. Divert the attention of potential attacker. 2. Collect information about the intruder's action. 3. Provide encouragement to the attacker so as to stay for some time, allowing the administrations to detect this and swiftly act on this. • Honeypots are designed for 2 important goals 1. Make them look-like full real-life systems. 2. Do not allow legitimate users to know about or access them. • Different types of honeypots: 1. **Research Honeypot** – A Research Honeypot is used to study about the tactics and techniques of the intruders. It is used as a watch post to see how an attacker is working when compromising a system. 2. **Production Honeypot** – These are primarily used for detection and to protect organizations. The main purpose of a production honeypot is to help mitigate risk in an organization.	**(Explanation: 4 marks)**
	(d)	**Describe data recovery procedures & ethics.**	**4M**
	Ans:	**Deleted file recovery:** • When we delete a file on the disk having FAT32 or NTFS (new technology file system) file system, its content is not erased from the disk but only reference to file data in file allocation Table or master table is marked as deleted. • It means that we might be able to recover deleted files or make it visible for file system again.	**(Data Recover Procedures: 2 marks, Ethics: 2 marks)**

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

- There are various data/file recovery tools available these tools find & recover recoverable deleted files from NTFS & FAT.
- These tools usually operate as per following process steps:

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

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

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

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

Data Recovery Ethics:

It is concerned with security of your data. These are used to think through different situations.

- It is a major part of the society and should be followed in letter and spirit
- There are policies in many organizations that provide guidelines for ethics.
- It is a behavior of the person in relation with the subject.
- There are four primary issues:
  Privacy, Accuracy, Property and Access
- Some standards are :

  Standard of right and wrong behavior

  A gauge of personal integrity

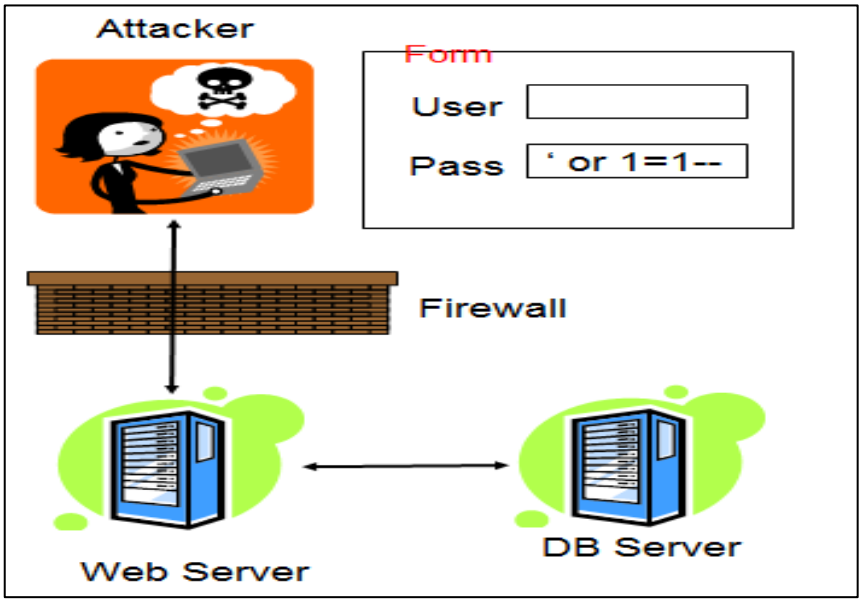
  The basis of trust and cooperation in relationships with others.

	(e)	**Explain how SQL injection can be done on website with example & prevention of it for web security.**	**4M**
	Ans:	• SQL injection is a code injection technique that might destroy your database.	(**How SQL injection can be**

- SQL injection is the placement of malicious code in SQL statements, via web page input.

How SQL injection can be done on website:

1. Attacker submits form with SQL exploit data.
2. Application builds string with exploit data.
3. Application sends SQL query to DB.
4. DB executes query, including exploit, sends data back to application.
5. Application returns data to user.



Unauthorized Access Attempt:
password = **' or 1=1 --**
SQL statement becomes:
select count(*) from users **where** username = 'user' **and** password = '' **or 1=1 --**
Checks if password is empty OR 1=1, which is always true, permitting access.

- **How to prevent SQL injection:**

1. Employ comprehensive data sanitization.

2. Use a web application firewall.

3. Limit database privileges by context.

4. Avoid constructing SQL queries with user input.

done on website:2 marks, How to prevent SQL injection:2 marks)

		5. Eliminate unnecessary database capabilities 6. Regularly apply software patches 7. Suppress error messages. 8. Continuously monitor SQL statements from database-connected applications.	