WINTER– 19 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.	Answer	Marking Scheme
1.		**Attempt any Three of the following:**	12M
	a	**Define Virus. Describe different phases of virus.**	4M
	Ans	Virus is a program which attaches itself to another program and causes damage to the computer system or the network. It is loaded onto your computer without your knowledge and runs against your wishes. Types of viruses: • Parasitic Viruses • Memory resident viruses • Non-resident viruses • Boot sector Viruses • Overwriting viruses • Stealth Virus • Macro Viruses **Different phases of viruses are:** • **Dormant phase:** The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage. • **Propagation phase:** The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propagating version; viruses often morph to evade detection. Each	2M for definition, 2M for explanation of types

infected program will now contain a clone of the virus, which will itself enter a propagation phase.

- **Triggering phase:** The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.
- **Execution phase:** The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

b **Describe components of good password.** **4M**

Ans

Components of good password are:

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

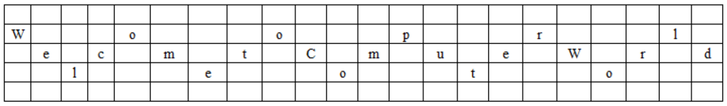
4M for correct explanation

c **Consider plain text "Welcome to Computer World", encrypt with help of Rail fence technique, and also write the algorithm.** **4M**

Ans

Plain text "Welcome to Computer World"

Assuming number of rails as 3



W				o				o				p				r				l	
	e		c		m		t		C		m		u		e		W		r		d
		l				e				o				t				o			

Cipher text is: Wooprl ecmtCmueWrd leoto

Algorithm for rail-fence cipher is as follow:

1. Write down the plain text message as a sequence of diagonals.
2. Read the plain text written in step 1, row wise.
3. Let's see example of rail-fence cipher. Suppose plain text is Welcome to Compute World, if we perform rail-fence cipher operation on this text it will be coded as Wooprl ecmtCmueWrd leoto.
4. It involves writing plain text in a diagonal sequence and then reading it row by row to produce cipher text.

2M for problem solving, 2M for algorithm

d **List and explain any four techniques used by firewall to control access and enforce security policy.**

	Ans	**Techniques used by firewall are:** 1) Service control 2) Direction control 3) User control 4) Behavior control **1) Service control:** This control determines the types of internet services that can be accessed, inbound or outbound. Firewall may filter traffic on the basis of IP address, protocol or TCP port number. It may provide proxy software that receives and interprets each service request before passing it on. It may host the server software itself such as a web or mail service. **For Example:** Incoming HTTP Requests – Rejected unless they are directed to an official web server host. **2) Direction control:** This control regulates the direction in which particular service request may be initiated and allowed to flow through firewall. **3) User control:** A User control manages or authorizes admission to a service according to which entity is trying to access that specified service .This feature is applied to users inside the firewall perimeter (Internal Users). It may also be applied to incoming traffic from external users. But it requires some form of secure authentication technology. **4) Behavior control:** Controls how particular services are used. For example: The firewall may filter email to eliminate spam or it may enable external access to only a portion of the information on a Local web server. Filtering of email spam attacks – may require examination of Sender's email address in message headers and message contents.	2M for listing, 2M for explanation
1.	**(B)**	**Attempt any ONE of the following:**	**6M**
	a	**Explain spoofing attack with example. State different ways of spoofing.**	
	Ans	• Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. • Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server. • Spoofing can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. • Spoofing is often the way a bad actor gains access in order to execute a larger cyber-attack such as an advanced persistent threat or a man-in-the-middle attack. **For example:** By using corporate logos, or other specific graphics, criminals can disguise emails to make it look like they've come from a trusted source.	2M for explanation of spoofing attack, 4M for stating types

		Different ways of spoofing are: **Email Spoofing:** Email spoofing occurs when an attacker uses an email message to trick a recipient into thinking it came from a known and/or trusted source. These emails may include links to malicious websites or attachments infected with malware, or they may use social engineering to convince the recipient to freely disclose sensitive information. **Caller ID Spoofing:** With caller ID spoofing, attackers can make it appear as if their phone calls are coming from a specific number either one that is known and/or trusted to the recipient, or one that indicates a specific geographic location. Attackers can then use social engineering often posing as someone from a bank or customer support to convince their targets to, over the phone, provide sensitive information such as passwords, account information, social security numbers, and more. **Website Spoofing:** Website spoofing refers to when a website is designed to mimic an existing site known and/or trusted by the user. Attackers use these sites to gain login and other personal information from users. **IP Spoofing:** Attackers may use IP (Internet Protocol) spoofing to disguise a computer IP address, thereby hiding the identity of the sender or impersonating another computer system. One purpose of IP address spoofing is to gain access to a networks that authenticate users based on IP addresses. **ARP Spoofing:** Address Resolution Protocol (ARP) is a protocol that resolves IP addresses to Media Access Control (MAC) addresses for transmitting data. ARP spoofing is used to link an attacker's MAC to a legitimate network IP address so the attacker can receive data meant for the owner associated with that IP address. ARP spoofing is commonly used to steal or modify data but can also be used in denial-of-service and man-in-the-middle attacks or in session hijacking. **DNS Server Spoofing:** DNS (Domain Name System) servers resolve URLs and email addresses to corresponding IP addresses. DNS spoofing allows attackers to divert traffic to a different IP address, leading victims to sites that spread malware.	
	b	**Explain in brief IT Act 2000 and IT Act 2008.**	
	Ans	**IT Act 2000:** In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it	3M for IT Act 2000, 3M for IT Act 2008

is important to understand what the various perspectives of the IT Act 2000 are and what it offers. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means.

The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. Some highlights of the Act are listed below: The Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

The Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference and details the legal recognition of Digital Signatures. The Act gives a scheme for Regulation of Certifying Authorities.

The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital signature Certificates. The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act.

The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

IT Act 2008:

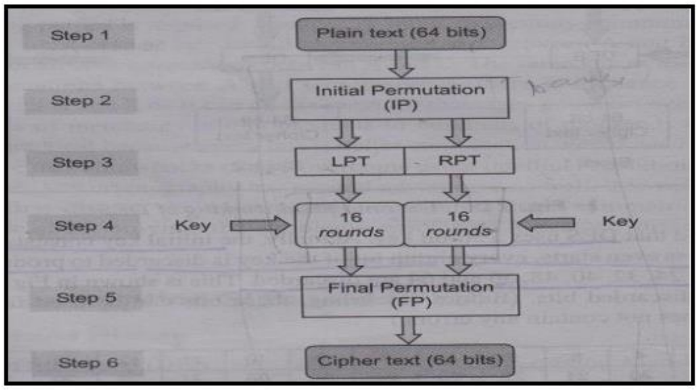
IT acts 2008: It is the Information Technology Amendment Act, 2008.the act was developed for IT industries, control e-commerce, to provide e-governance facility and to stop cybercrime attacks.

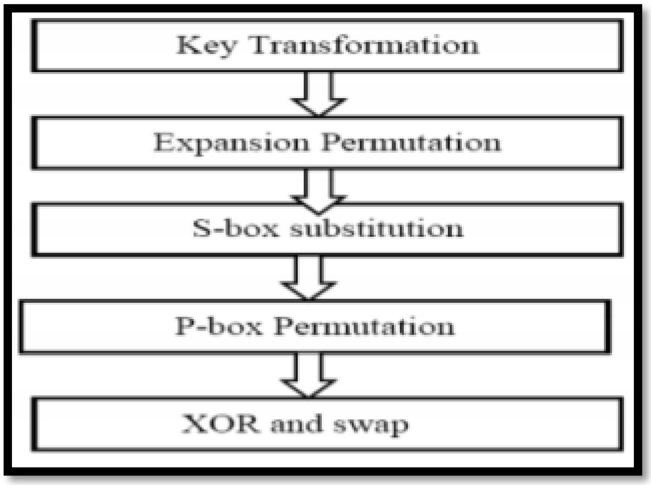
Following are the characteristics of IT ACT 2008: This act provides legal recognition or the transaction i.e. Electronic Data Interchange (EDI) and other electronic communications. This Act also gives facilities for electronic filling of information with the Government agencies. It is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

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 cyber terrorism. •Authorizing an Inspector to investigate cyber offences.	
2.		**Attempt any Two of the following:**	**16M**
	a	**List different types of attack. Describe any two in brief.**	**8M**
	Ans	**Types of attacks are:** 1. Passive attacks 2. Active attacks 3. Denial of service attacks 4. Backdoor attacks 5. Trapdoor attacks 6. Man-in-the middle attacks **Passive Attacks:** A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. **Active Attacks:** An Active attack attempts to alter system resources or effect their operations. Active attack involves some modification of the data stream or creation of false statement. **Denial of service Attacks:** A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected. **Backdoor Attacks:** It is secret entry point into program that allows user to gain access without going through the usual security access procedures. It is used legitimately in debugging and testing. It also refers to the entry and placement of a program or utility into a network that creates a backdoor entry for attackers. This may allow a certain user ID to log on without password a program or gain of administrative services. It becomes threat when programmers use them to gain unauthorized access. There are several backdoor programs and tools used by hackers in terms of automated tools. **Trapdoor Attacks:** A trap door is an entrance in a system which circumvents the normal safety measures. It is secret entry point into a program that allows someone who is aware of gaining access using procedure other that security procedure. It might be hidden program which makes the protection system ineffective. This entry can be deliberately in traduced by the developer to maintain system in case of disaster management. Trapdoor programs can be installed through malware using internet.	2M for listing, 6M for explanation

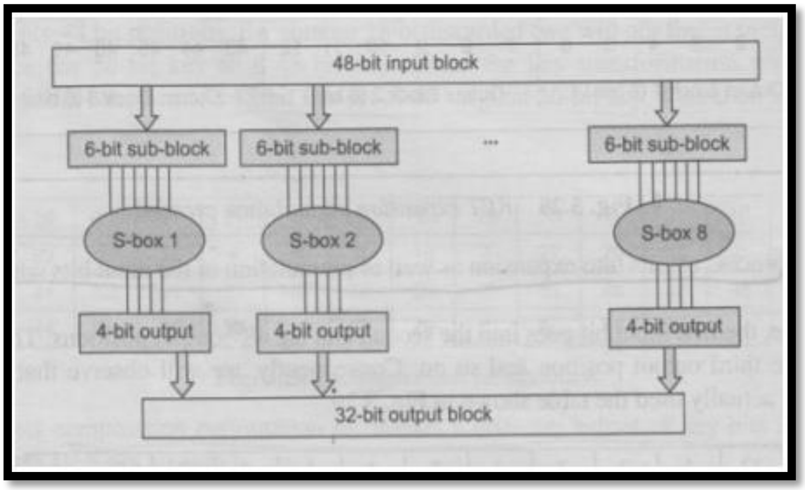
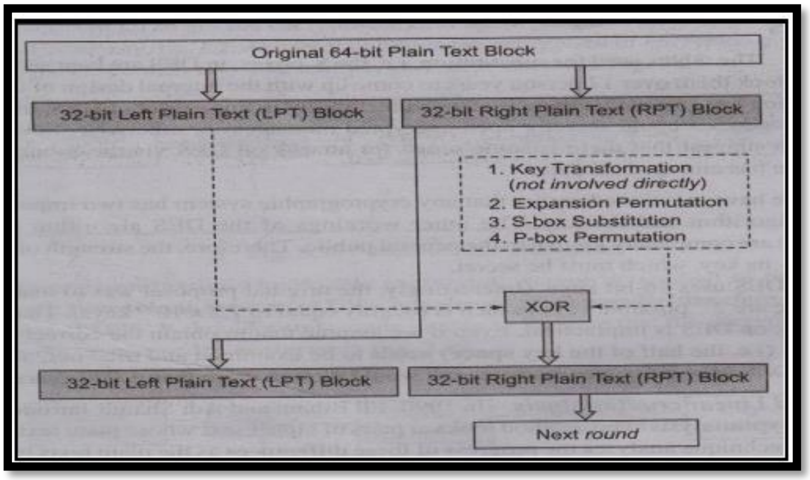
		Man in Middle Attacks: A man-in-the-middle attack is a type of cyber-attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late.	
	b	**Explain DES algorithm? Explain each step in detail with help of diagram.**	
	Ans	The Data Encryption Standard is generally used in the ECB, CBC, or the CFB mode. DES is a block cipher. It encrypts data in blocks of size 64 bits each. That is, 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text .DES is based on the two fundamental attributes of cryptography: substitution and transposition. The process diagram as follows:  Step 1 Plain text (64 bits) Step 2 Initial Permutation (IP) Step 3 LPT RPT Step 4 Key 16 rounds 16 rounds Key Step 5 Final Permutation (FP) Step 6 Cipher text (64 bits) **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.	2M for explanation of DES, 4M for steps, 2M for diagram

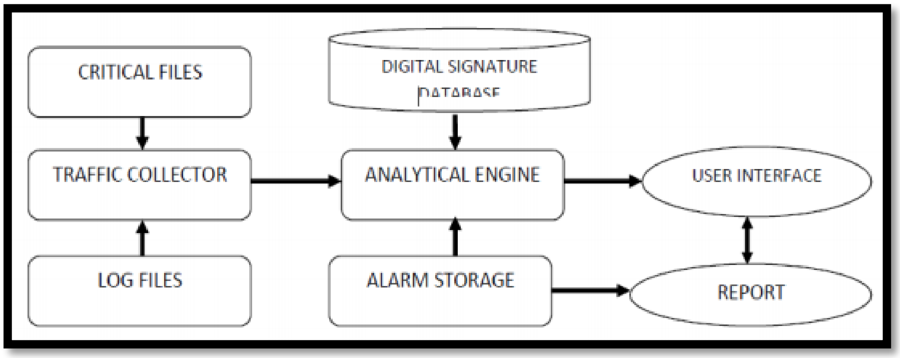


Step 1: Key Transformation: The initial key is transformed into a 56-bit key by discarding every 8th bit of initial key. Thus ,for each round , a 56 bit key is available, from this 56-bit key, a different 48-bit sub key is generated during each round using a process called as key transformation Expansion 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 XORed with the 48-bit RPT and the resulting output is given to the next step.

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

		 48-bit input block 6-bit sub-block 6-bit sub-block ... 6-bit sub-block S-box 1 S-box 2 S-box 8 4-bit output 4-bit output 4-bit output 32-bit output block **Step 4: P- box Permutation:** The output of S-box consists of 32-bits. These 32-bits are permuted using P-box. Step 5: XOR and Swap: The LPT of the initial 64-bits plain text block is XORed with the output produced by P box permutation. It produces new RPT. The old RPT becomes new LPT, in a process of swapping.  Original 64-bit Plain Text Block 32-bit Left Plain Text (LPT) Block 32-bit Right Plain Text (RPT) Block 1. Key Transformation (not involved directly) 2. Expansion Permutation 3. S-box Substitution 4. P-box Permutation XOR 32-bit Left Plain Text (LPT) Block 32-bit Right Plain Text (RPT) Block Next round **Final Permutation:** At the end of 16 rounds, the final permutation is performed. This is simple transposition. For e.g., the 40th input bit takes the position of 1st output bit and so on.	
	c	**Describe IDS and its two types.**	**8M**
	Ans	An Intrusion Detection System (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.	4M for explanation of IDS, 4M for explanation of types



IDS have following logical components:

1. Traffic collection: It collects activity as events from IDS to examine. On Host-based IDS, this can be log files, Audit logs or traffic coming to or leaving a system. On network based IDS, this is typically a mechanism for copying traffic of network link.

2. Analysis Engine: It examines collected network traffic & compares it to known patterns of suspicious or malicious activity stored in digital signature. The analysis engine act like a brain of IDS.

3. Signature database: A collection of patterns & definitions‟ of known suspicious or malicious activity.

4. User Interface & Reporting: Interfaces with human element, providing alerts when suitable & giving the user a means to interact with & operate the IDS.

IDS are mainly divided into two categories, depending on monitoring activity:

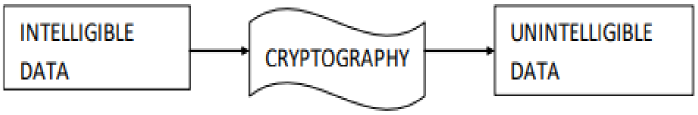
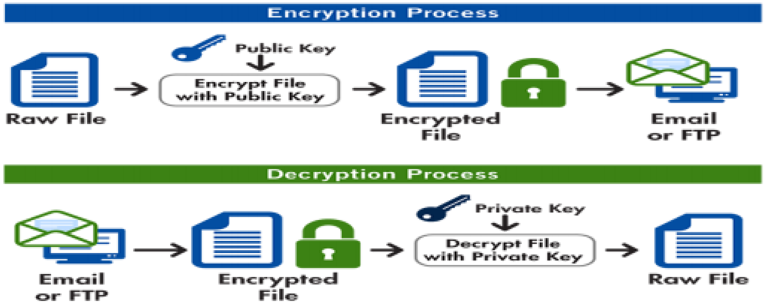
1) Host-based IDS: Host based IDS looks for certain activities in the log files are:

1. Logins at odd hours
2. Login authentication failure
3. Adding new user account
4. Modification or access of critical systems files.
5. Modification or removal of binary files
6. Starting or stopping processes
7. Privilege escalation
8. Use of certain program

2) Network based IDS: Network based IDS looks for certain activities like:

1. Denial of service attacks.
2. Port scans or sweeps
3. Malicious contents in the data payload of packet(s)
4. Vulnerability of scanning
5. Trojans, Viruses or worms
6. Tunneling
7. Brute force attacks.

<table>
<tr><td><b>3.</b></td><td></td><td><b>Attempt any Three of the following:</b></td><td><b>16M</b></td></tr>
<tr><td></td><td><b>a</b></td><td><b>Compare Intruders and Insiders</b></td><td><b>4M</b></td></tr>
<tr><td></td><td><b>Ans</b></td><td>
<table>
<tr><th>Intruders</th><th>Insiders</th></tr>
<tr><td>Keep trying attacks till success as they have the access and knowledge to cause immediate damage to organization</td><td>Insiders are authorized users who try to access system or network for which he is unauthorized.</td></tr>
<tr><td>Individual or a small group of attackers, they can be more in numbers.</td><td>They can be more in numbers who are directly or indirectly access the organization.</td></tr>
<tr><td>They are hackers or crackers</td><td>Insiders are not hackers.</td></tr>
<tr><td>Intruders are illegal users.</td><td>Insiders are legal users</td></tr>
<tr><td>Less dangerous than insiders</td><td>More dangerous than outsiders As they have the access and knowledge to cause immediate damage to organization</td></tr>
<tr><td>They do not have access to system.</td><td>They may give remote access to the organization.</td></tr>
</table>
</td><td>1M each for one point</td></tr>
<tr><td></td><td><b>b</b></td><td><b>Explain password selection strategies</b></td><td><b>4M</b></td></tr>
<tr><td></td><td><b>Ans</b></td><td><b>There are four basic techniques passwords selection strategies:</b>
<b>a) User education:</b> Tell the importance of hard-to-guess passwords to the users and provide guidelines for selecting strong password.
<b>b) Computer generated password:</b> Computer generated passwords are random in nature so difficult for user to remember it and may note down somewhere.
<b>c) Reactive password checking:</b> 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.
<b>d) Proactive password checking:</b> 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.</td><td>4Meach for any 4 points OR Answer with Relevant Contents</td></tr>
<tr><td></td><td><b>c</b></td><td><b>Define the following terms:</b>
<b>i)Cryptography</b>
<b>ii)Cryptanalysis</b>
<b>iii)Cryptology</b>
<b>iv)Steganography</b></td><td><b>4M</b></td></tr>
</table>

	Ans	i) **Cryptography:** Cryptography is the art or science comprising the principles and methods of transforming an intelligible message into one that is unintelligible.  ii) **Cryptanalysis:** Cryptanalysis is the art or science comprising the principles and methods of transforming an unintelligible message back into an intelligible message without the knowledge of key. UNINTELLIGIBLE DATA CRYPTANALYSIS INTELLIGIBLE DATA iii) **Cryptology:** Cryptology is the art or science comprising the principles and methods of transforming an intelligible message into one that is unintelligible and unintelligible message back to intelligible one. CRYPTOGRAPHY + CRYPTANALYSIS = CRYPTOLOGY iv) **Steganography:** Steganography is the art and science of writing hidden message in such a way that no one apart from sender and intended recipient suspects the existence of the message.	1 M each for relevant definitions
	d	**Explain the role of PGP in Email security.**	**4M**
	Ans	PGP is Pretty Good Privacy. It is a popular program used to encrypt and decrypt email over the internet. It becomes a standard for email security. It is used to send encrypted code (digital signature) that lets the receiver verify the sender's identity and takes care that the route of message should not change. PGP can be used to encrypt files being stored so that they are in unreadable form and not readable by users or intruders It is available in Low cost and Freeware version. It is most widely used privacy ensuring program used by individuals as well as many corporations.  Encryption Process Public Key Raw File Encrypt File with Public Key Encrypted File Email or FTP Decryption Process Private Key Email or FTP Encrypted File Decrypt File with Private Key Raw File **There are five steps as shown below:**	PGP Definition: 2M, Steps in PGP for email security: 2M

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.

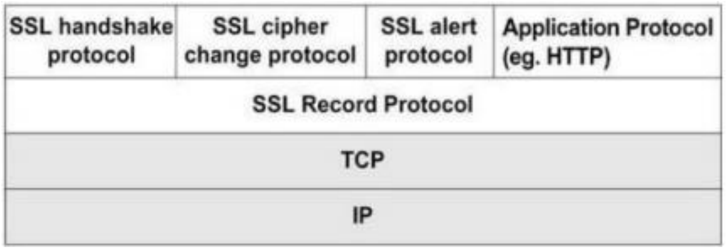
3. Encryption: The compressed output of step 2 (i.e. the compressed form of the original email and the digital signature together) are encrypted with a symmetric key.

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.

e **Describe SSL protocol.**

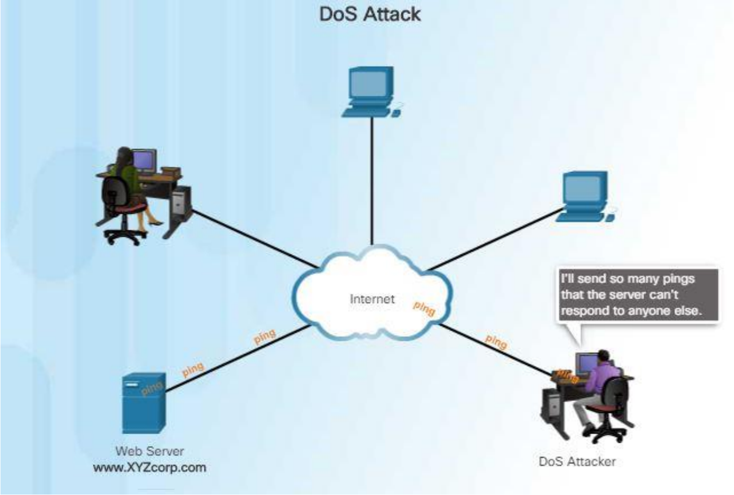
Ans **Definition -Secure Sockets Layer (SSL)** Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network. Developed by Netscape, SSL technology creates a secure link between a Web server and browser to ensure private and integral data transmission. SSL uses Transport Control Protocol (TCP) for communication. Architecture of secure socket layer (SSL)



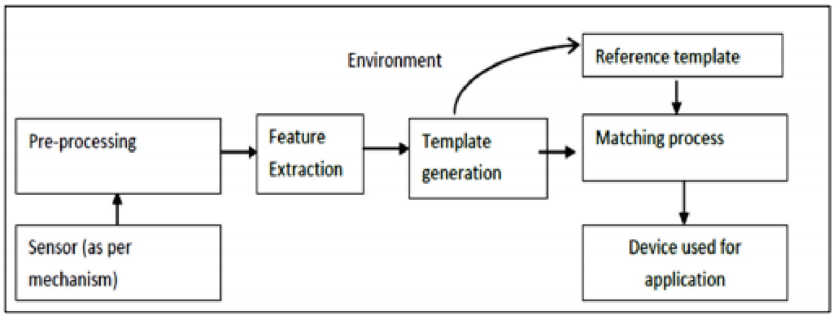
Working:

In SSL, the word socket refers to the mechanism of transferring data between a client and server over a network. When using SSL for secure Internet transactions, a Web server needs an SSL certificate to establish a secure SSL connection.

SSL encrypts network connection segments above the transport layer, which is a network connection component above the program layer.

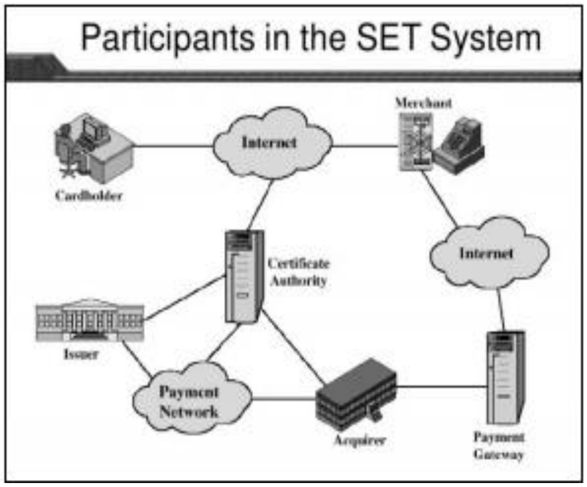
		SSL follows an asymmetric cryptographic mechanism, in which a Web browser creates a public key and a private (secret) key. The public key is placed in a data file known as a certificate signing request (CSR). The private key is issued to the recipient only. **The objectives of SSL are:** • **Data integrity:** Data is protected from tampering. • **Data privacy:** Data privacy is ensured through a series of protocols, including the SSL Record Protocol, SSL Handshake Protocol, SSL Change Cipher Spec Protocol and SSL Alert Protocol. • **Client-server authentication:** The SSL protocol uses standard cryptographic techniques to authenticate the client and server. SSL is the predecessor of Transport Layer Security (TLS), which is a cryptographic protocol for secure Internet data transmission	
4.	**(A)**	**Attempt any Three of the following:**	**12M**
	a	**Explain DOS attack with neat labelled diagram.**	**4M**
	Ans	A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy  DoS Attack Internet ping ping ping ping ping ping I'll send so many pings that the server can't respond to anyone else. Web Server www.XYZcorp.com DoS Attacker	2M explanation 2 M diagram

	b	**Enlist types of Biometric. Explain any one type in detail.**	4M
	Ans	Biometric refers study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral characteristics. Different types of Biometrics (any two 1 Mark) 1. Finger print recognition 2. Hand print recognition 3. Retina/iris scan technique 4. Face recognition 5. Voice patterns recognition 6. Signature and writing patterns recognition 7. Keystroke dynamics: **Fingerprint registration & verification process:** 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.	1 M Listing; 1.5 M diagram; 1.5 M explanation

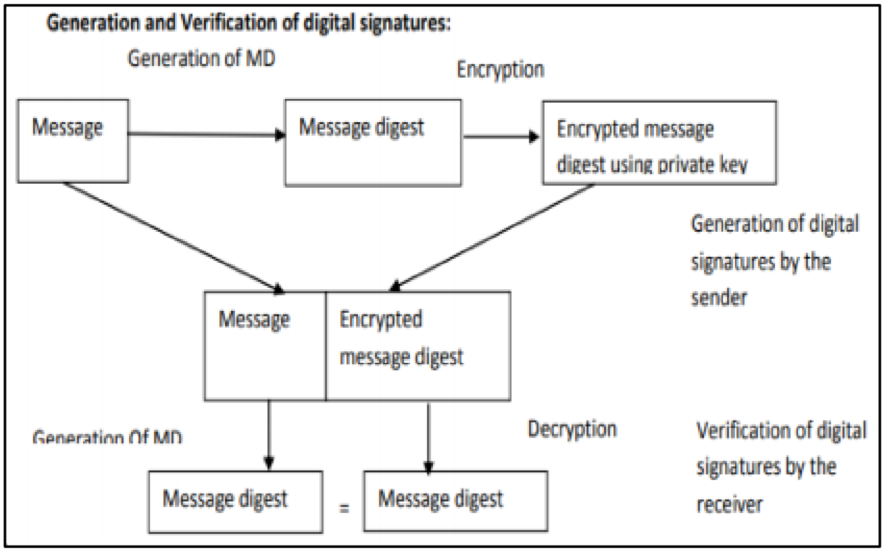
		 Environment Reference template Pre-processing Feature Extraction Template generation Matching process Sensor (as per mechanism) Device used for application	
	c	**Describe cybercrime? Describe hacking & cracking related to cybercrime.**	**4M**

	Ans	**Cybercrime :**
		Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.
		Types of Cybercrimes are
		1. Hacking
		2. Cracking
		3. Theft
		4. Malicious software
		5. Child soliciting and abuse Hacking:
		Hacking is one of the most well-known types of computer crime. A hacker is someone who find out and exploits the weaknesses of s computer systems or networks. Hacking refers to unauthorized access of another's computer systems. These intrusions are often conducted in order to launch malicious programs known as viruses, worms, and Trojan horses that can shut down hacking an entire computer network. Hacking is also carried out as a way to talk credit card numbers, intent passwords, and other personal information. By
			1 M What is cybercrime;
			1.5 M Hacking;
			1.5 M Cracking

		accessing commercial database, hackers are able to steal these types of items from millions of internet users all at once. There are different types of hackers: 1. White hat 2. Black hat 3. Grey hat 4. Elite hacker 5. Script hacker **Cracking**: In the cyber world, a cracker is someone who breaks into a computer system or network without authorization and with the intention of doing damage. Crackers are used to describe a malicious hacker. Crackers get into all kinds of mischief like he may destroy files, steal personal information like credit card numbers or client data, infect the system with a virus, or undertake many others things that cause harm. Cracking can be done for profit, maliciously, for some harm to organization or to individuals. Cracking activity is harmful, costly and unethical.	
	d	**List & explain the key participants in Secure Electronic Transaction (SET).**	**4M**
	Ans	**For secure electronic transaction SET participant are there.** **1) Cardholders-** cardholder is an authorized holder of payment card like Master card, visa that has been issued by an issuer. **2) Merchant-** A merchant is a person or organization that has goods or services to sell to cardholder **3) Issuer-** This is financial institution like bank. **4) Acquirer-** This is a financial institution that establishes account with merchant & process payment card authorization & payment. **5) Payment Gateway-** This is a function operated by acquire. The payment gateway process between SET & existing bankcard payment networks .For authorization & payment function. **7) The merchant** exchanges SET messages with payment gateway over internet. **8) Certificate Authority-** This is an entity that is trusted to issue public key for cardholder, merchant & payment gateways.	1 M listing any 4 components ; 2 M Explanation of any four components

		 Participants in the SET System Merchant Internet Cardholder Certificate Authority Internet Issuer Payment Network Acquirer Payment Gateway	
4	(B)	**Attempt any ONE of the following:**	6M
	a	**Describe digital signature mechanism with neat diagram.**	
	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: 4M, Explanation: 4M

Generation and Verification of digital signature:


Generation and Verification of digital signatures:
Generation of MD
Encryption
Message
Message digest
Encrypted message digest using private key
Generation of digital signatures by the sender
Message
Encrypted message digest
Generation Of MD
Decryption
Verification of digital signatures by the receiver
Message digest
=
Message digest

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.

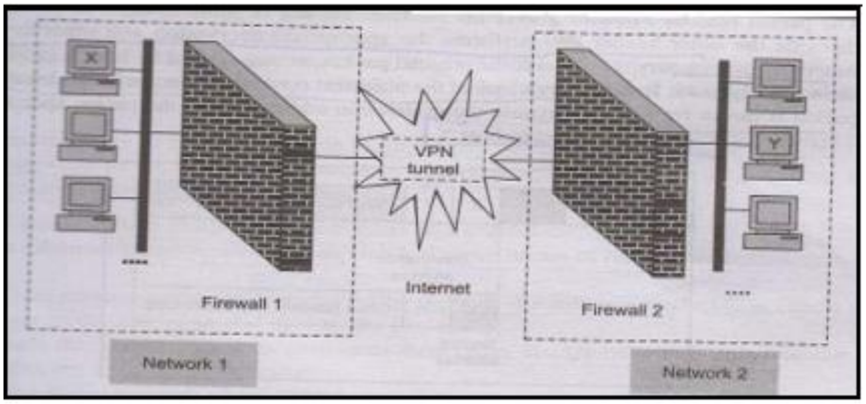
3. Then, the sender sends this encrypted message digest with the plaintext or message to the receiver.

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.

	b	**Explain VPN with diagram.**	
	Ans	A Virtual Private Network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization’s network. With a VPN,all network traffic (data,voice,and videos) goes through virtual tunnel between the host device(client) and the VPN provider server’s and is encrypted.VPN technology uses a combination of features such as encryption, tunneling protocols, data encapsulation, and certified connections to provide you with a secure connection to private networks and to protect your identity.	Explanation-2M Diagram2M OR Answer with Relevant Contents

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.



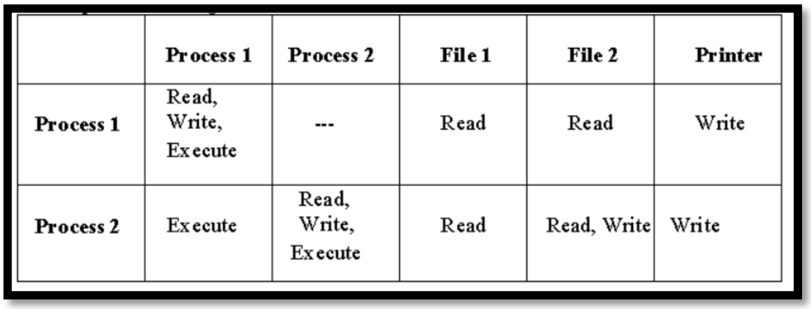
5. **Attempt any Three of the following:** **12M**

a **Describe access control, availability, authentication, authorization related to physical security.**

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

2 M each for 4 criteria

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

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.

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.

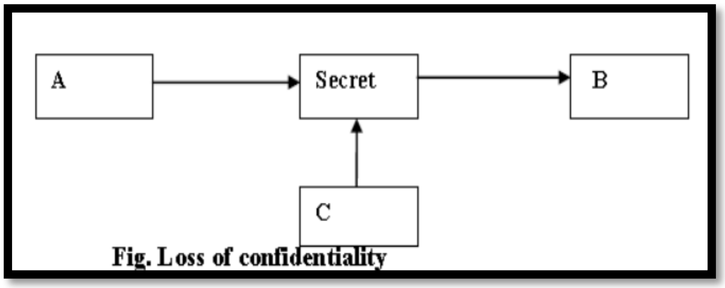


Fig. Loss of confidentiality

Authorization

Authorization is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data and application features. Authorization is normally preceded by authentication for user identity verification. System administrators (SA) are typically assigned permission levels covering all system and user resources. During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.

b **Explain DAC and MAC with principles and policies.**

Ans **DAC: -** In Discretionary access control (DAC), each system object (file or data object) has an owner, and each initial object owner is the subject that causes its creation. Thus, an object's access policy is determined by its owner.

4 M- DAC explanation; 4 M- MAC explanation

A typical example of DAC is Unix file mode, which defines the read, write and execute permissions in each of the three bits for each user, group and others.

DAC attributes include:

- User may transfer object ownership to another user(s).
- User may determine the access type of other users.
- After several attempts, authorization failures restrict user access.
- Unauthorized users are blind to object characteristics, such as file size, file name and directory path.
- Object access is determined during access control list (ACL) authorization and based on user identification and/or group membership.

MAC: -Mandatory Access Control (MAC) is is a set of security policies constrained according to system classification, configuration and authentication. MAC policy management and settings are established in one secure network and limited to system administrators.MAC defines and ensures a centralized enforcement of confidential security policy parameters.

For best practices, MAC policy decisions are based on network configuration. In contrast, certain operating systems (OS) enable limited Discretionary Access Control (DAC).

MAC advantages and disadvantages depend on organizational requirements, as follows:

- MAC provides tighter security because only a system administrator may access or alter controls.
- MAC policies reduce security errors.
- MAC enforced operating systems (OS) delineate and label incoming application data, which creates a specialized external application access control policy.

c **Explain the Kerberos with the help of suitable diagram.**

Ans **Kerberos** is a network authentication protocol.

- It is designed to provide strong authentication for client/server applications by using secret-key cryptography.
- Kerberos was created by MIT as a solution for network security problems and it is freely available from MIT, under copyright permission.

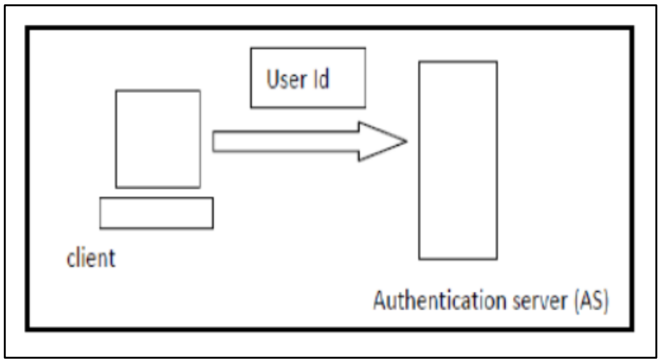
4 M- Kerberos explanation;
4 M- Kerberos Diagram

How Kerberos does works?

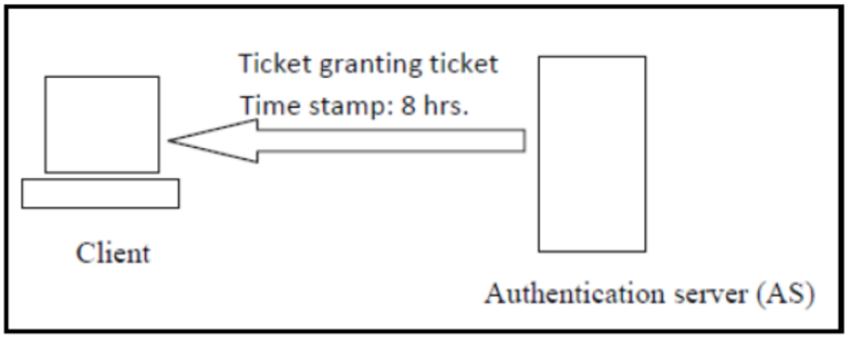
- Kerberos operates by encrypting data with a symmetric key.
- A symmetric key is a type of authentication where both the client and server agree to use a
- Single encryption/decryption key for sending and receiving data.
- When working with the encryption key, the details are actually sent to a key distribution center (KDC), instead of sending the details directly between each computer.

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.

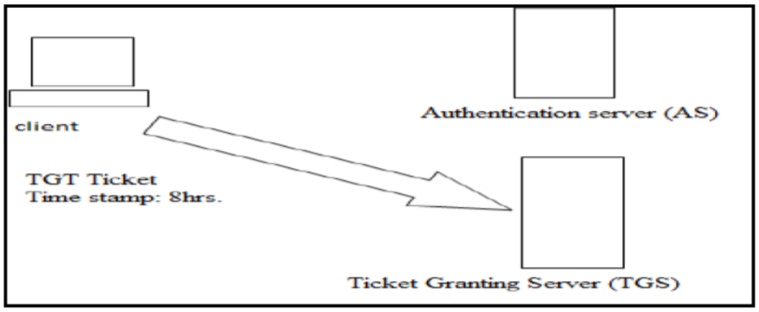


2. Upon verification, a timestamp is crated. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours. The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless. (This is used 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)

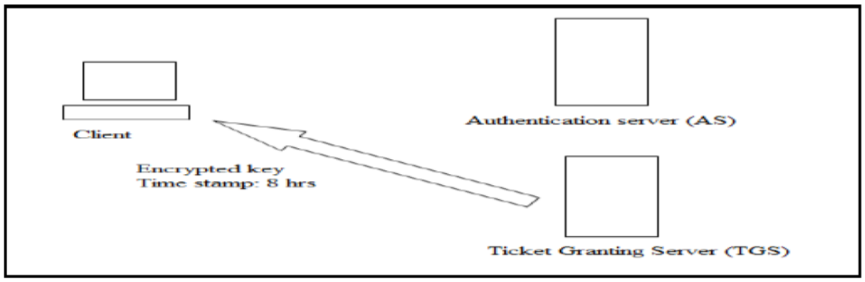


3. The key is sent back to the client in the form of a ticket-granting ticket, or TGT. This is a simple ticket that is issued by the authentication service. It is used for authentication the client for future reference.

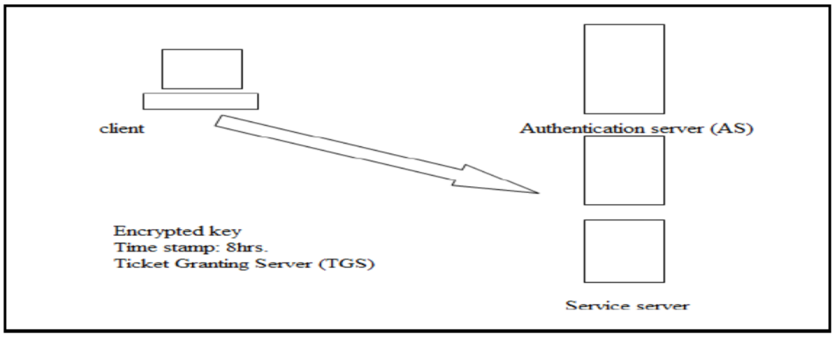
4. The client submits the ticket-granting ticket to the ticket-granting server, or TGS, to get authenticated.



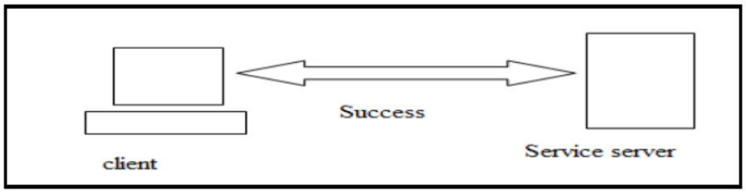
5. The TGS creates an encrypted key with a timestamp, and grants the client a service ticket



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



7. The service 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 Three of the following:**	**16M**
	a	**Explain different models of access control.**	**4M**
	Ans	**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. **Discretionary Access control (DAC):** Restricting access to objects based on the identity of subjects and or groups to which they belong 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. 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 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	1 M- explanation of access control; 1 M- each for explanation of DAC, MAC and RBAC
	b	**Describe piggybacking and shoulder surfing.**	**4M**
	Ans	• **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.	2 M each for piggybacking and shoulder surfing explanation

		• 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, 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. • **Shoulder Surfing:** • 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. • 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	**Describe the working principle of firewall.**	**4M**
	Ans	**Working:** Firewalls enforce the establishment security policies. Variety of mechanism includes: **Network Address Translation (NAT)** **Basic Packet Filtering** **Stateful Packet Filtering** **Access Control Lists (ACLs)** **Application Layer Proxies.** • One of the most basic security function provided by a firewall is Network Address Translation (NAT).	4 M:- any relevant explanation for working of firewall

		• This service allows you to mask significant amounts of information from outside of the network. • This allows an outside entity to communicate with an entity inside the firewall without truly knowing its address. • Basic Packet Filtering, the most common firewall technique, looking at packets, their protocols and destinations and checking that information against the security policy. • Telnet and FTP connections may be prohibited from being established to a mail or database server, but they may be allowed for the respective service servers. • This is a fairly simple method of filtering based on information in each packet header, like IP addresses and TCP/UDP ports. This will not detect and catch all undesired packet but it is fast and efficient.	
	d	**List and explain different types of hackers.**	**4M**
	Ans	**There are different types of hackers:** 1. White hat 2. Black hat 3. Grey hat 4. Elite hacker 5. Script kiddie hacker **1) Black Hat Hacker** • Black-hat Hackers are also known as an Unethical Hacker or a Security Cracker. • These people hack the system illegally to steal money or to achieve their own illegal goals. • They find banks or other companies with weak security and steal money or credit card information. • They can also modify or destroy the data as well. Black hat hacking is illegal. **2) White Hat Hacker** • White hat Hackers are also known as Ethical Hackers or a Penetration Tester. White hat hackers are the good guys of the hacker world. • These people use the same technique used by the black hat hackers. • They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. • They focus on security and protecting IT system. White hat hacking is legal. **3) Gray Hat Hacker**	1 M- listing ; 3 M for explaining any 3 types of hacker

		• Gray hat Hackers Are Hybrid between Black Hat Hackers and White hat hackers. • They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system. • In most cases, they tell the administrator of that system. • But they are also illegal because they test the security of the system that they do not have permission to test. • Grey hat hacking is sometimes acted legally and sometimes not. **4) Elite Hacker** • Elite hackers avoid deliberately destroying information or otherwise damaging the computer systems they have exploited. **5) Script Kiddie** • A script kiddie, or “skiddie,” is someone who lacks programming knowledge and uses existing software to launch an attack. • Often a script kiddie will use these programs without even knowing how they work or what they do. • For example, imagine a child gets their first computer. The child watches a movie about hacking and then downloads a copy of Kali Linux. They begin playing with the various programs while searching for online tutorials. At first, they may be perceived as nothing more than an internet troll or noob, due to their lack of experience and quickness to brag and boast. Sometimes they will even resort to cyberstalking or bullying. However, this may simply be a cover for other more nefarious activity.	
	e	**Explain four threats to web security.**	**4M**
	Ans	The main types of threats to web systems are listed below: **Physical:** • Physical threats include loss or damage to equipment through fire, smoke, water & other fire suppressants, dust, theft and physical impact. • Physical impact may be due to collision or the result of malicious or accidental damage by people. • Power loss will affect the ability for servers and network equipment to operate depending upon the type of back-up power available and how robust it is.	Explanations -4M for any 4 threat OR Answer with Relevant Contents

		Malfunction: • Both equipment and software malfunction threats can impact upon the operations of a website or web application. • Malfunction of software is usually due to poor development practices where security has not been built into the software development life cycle. 1) **Malware:** • Malware, or malicious software, comes in many guises. • Web servers are popular targets to aid distribution of such code and sites which have vulnerabilities that allow this are popular targets. 2) **Spoofing:** • Spoofing where a computer assumes the identity of another and masquerading where a user pretends to be another, usually with higher privileges, can be used to attack web systems to poison data deny service or damage systems. 3) **Scanning:** • Scanning of web systems are usually part of network or application fingerprinting prior to an attack, but also include brute force and dictionary attacks on username, passwords and encryption keys. 4) **Eavesdropping:** • Monitoring of data (on the network, or on user's screens) may be used to uncover passwords or other sensitive data.	