



WINTER– 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.	Answer	Marking Scheme
1	A	Attempt any THREE :	12 M
	a	Define computer security. Explain the need of computer security.	4 M
	Ans	<p>Computer Security: Computer Security is the protection of computing systems and the data that they store or access.</p> <p>Need of computer Security:</p> <ol style="list-style-type: none"> 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. <p style="text-align: center;">OR</p> <p>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: Here, the user of a computer A send a message to user of computer</p>	<p>Definition :1 mark, Need: Any three points:1 mark each OR CIA Model Explanation : 3 marks</p>

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.

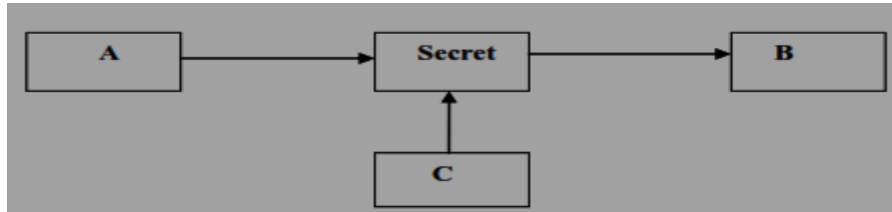


Fig. Loss of confidentiality

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.

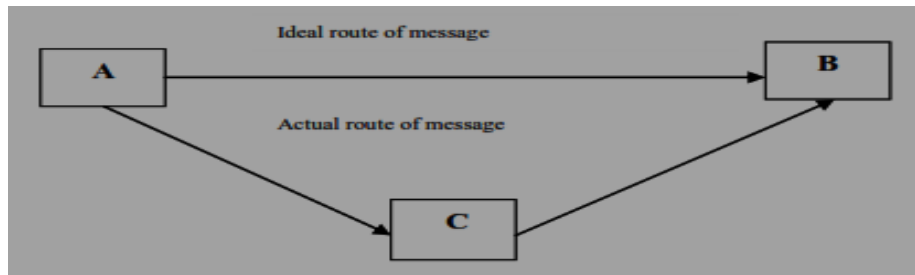


Fig. Loss of Integrity

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 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.

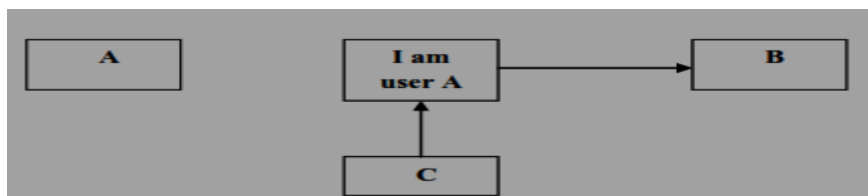


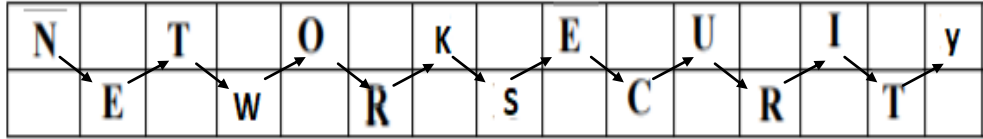
Fig. absence of authentication

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



b	Describe piggy backing & shoulder surfing.	4 M
Ans	<p>Piggy backing:</p> <ul style="list-style-type: none">• 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, 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. <p>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.</p> <ul style="list-style-type: none">• 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	Piggybacking: 2 marks, Shoulder surfing: 2 marks (Relevant answer covering given points)

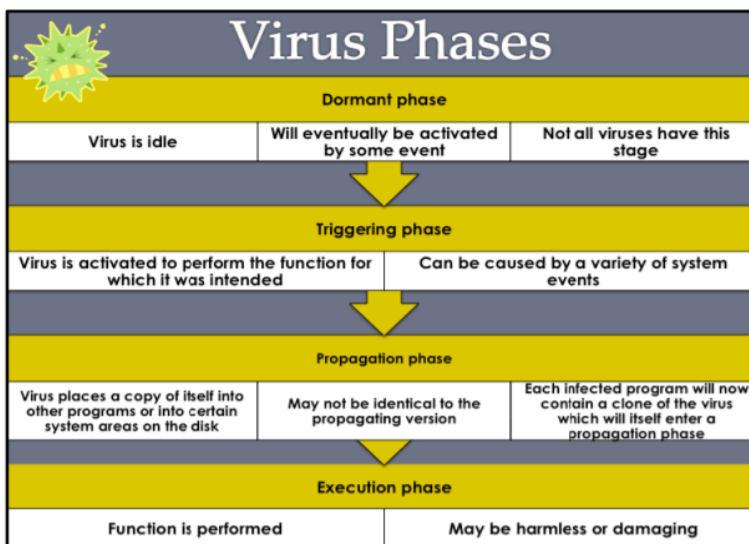


	someone's shoulder, to get information.	
c	Consider plain text “Network Security”, encrypt it with help of Rail Fence technique, also write the algorithm.	4 M
Ans	<p>Rail Fence Technique: It is one of the easiest transposition techniques to create cipher text. When plain text message is codified using any suitable scheme, the resulting message is called Cipher text or Cipher.</p> <p>Steps are: Plain text = NETWORK SECURITY</p> <p>Step 1: Write down Plain text as sequence of diagonal. Read Plain text written in Step 1 as sequence of rows. As,</p>  <p>Then concatenate these two sequences of text as one to create following Cipher Text: NTOKEUIYEWRSCT</p> <p>Steps for rail-fence cipher are as follow:</p> <ol style="list-style-type: none"> 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 NETWORK SECURITY if we perform rail-fence cipher operation on this text it will be coded as NTOKEUIYEWRSCT. 4. It involves writing plain text in a diagonal sequence and then reading it row by row to produce cipher text. 	2 marks for Step marks for cipher text, 2 marks for algorithm
d	State any four limitations of fire wall.	4 M
Ans	<p>Firewalls weakness / limitations</p> <ol style="list-style-type: none"> 1. Firewalls cannot protect against what has been authorized 2. It cannot stop social engineering attacks or an unauthorized user intentionally using their access for unwanted purposes 3. Firewalls cannot fix poor administrative practices or poorly designed security policies 4. It cannot stop attacks if the traffic does not pass through them 5. They are only as effective as the rules they are configured to enforce. 6. firewall can't protect you against malicious insiders 7. A firewall can't protect you against connections that don't go through it. 8. A firewall can't protect against completely new threats. 9. A firewall can't fully protect against viruses. 10. A firewall can't set itself up correctly. 11. Firewalls don't deal with the real problem. 	1 Mark each (for any 4 points)
B	Attempt any ONE :	6 M



a	What is dumpster diving? State preventative measures to avoid Dumpster diving.	6 M
Ans	Dumpster diving: <ol style="list-style-type: none">1. It is the process of going through a target's trash in order to find little bits of information System attackers need certain amount of information before launching their attack.2. One common place to find this information, if the attacker is in the vicinity of target is to go through the target's thrash in order to find little bits of information that could be useful.3. The process of going through target's thrash is known as "dumpster diving".4. The search is carried out in waste paper, electronic waste such as old HDD, floppy and CD media recycle and trash bins on the systems etc.5. If the attacker is lucky, the target has poor security process they may succeed in finding user ID's and passwords.6. If the password is changed and old password is discarded, lucky dumpster driver may get valuable clue. Prevention Mechanism: <ul style="list-style-type: none">• To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company should establish disposal policy.• Shred personal documents and credit card offers before throwing them away, and wipe hard drives clean before you get rid of computers or smartphones.	Concept 2 marks, Prevention mechanism 4 mark
b	How formatted partition can be recovered?	6 M
Ans	Formatted partition recovery: <ul style="list-style-type: none">• Formatting refers to dividing the disk in accordance with certain principles, allowing computer to store and search files.• Formatting disk is to eliminate all files on disk.• There are various formatted partition recovery tool available.• Although every tool will have different GUI & method of recovery.• These tools usually operate as per following process steps: Step1: If you cannot boot the computer, please use data recovery bootable disk. Step 2: Select the file types you want to recover & volume where the formatted hard drive is. The tool will automatically scan the selected volume. Step 3: Then the founded data will be displayed on the screen & you can get a preview of it. Then select the file or directory that you want to recover & save them to a healthy drive.	Explanation : 2 marks, Steps: 4 marks
2	Attempt any TWO :	16 M
a	Define the term virus. Describe the different phases of virus with suitable example.	8 M
Ans	A virus is a program that can "infect" other programs by modifying them and inserting a copy of itself into the program. This copy can then go to infect other programs. Just like its biological counterpart, a computer virus carries in its instructional code the recipe for making perfect copies of itself. A virus attaches	Definition of Virus: 2 mark ,Listing

itself to another program and then executes secretly when the host program is run. During its lifetime a typical virus goes through the following stages:



- **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 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.

phases of Virus:
2mark,
Explanation of Phases: 4 marks

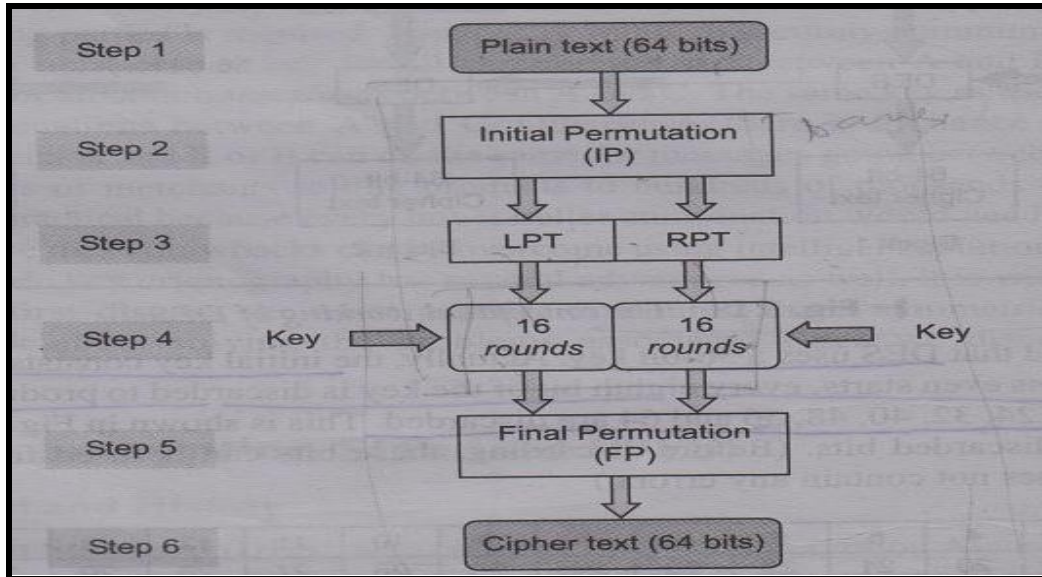
Diagram is Optional.

b What is DES algorithm? Explain each step in detail with the help of diagram.

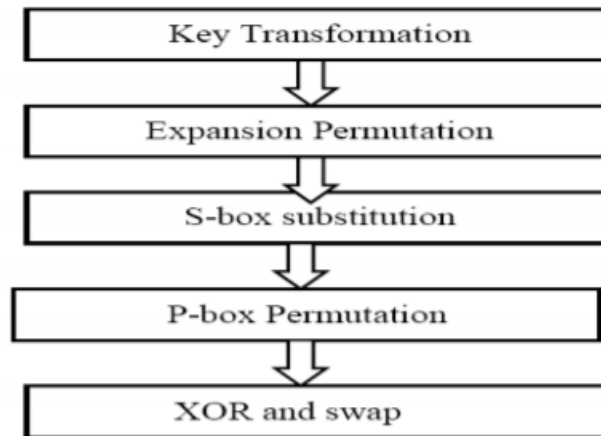
8 M

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:

Definition: 1 mark ;
Diagram: 1m;
process Diagram: 1 mark, for each step: 1marks



Initial Permutation (IP): It happens only once. It replaces the first bit of the original plain text block with the 58th bit of the original plain text block, the second bit with the 50th bit of original plain text block and so on. The resulting 64-bits permuted text block is divided into two half blocks. Each half block consists of 32 bits. The left block called as LPT and right block called as RPT. 16 rounds are performed on these two blocks. Details of one round in DES

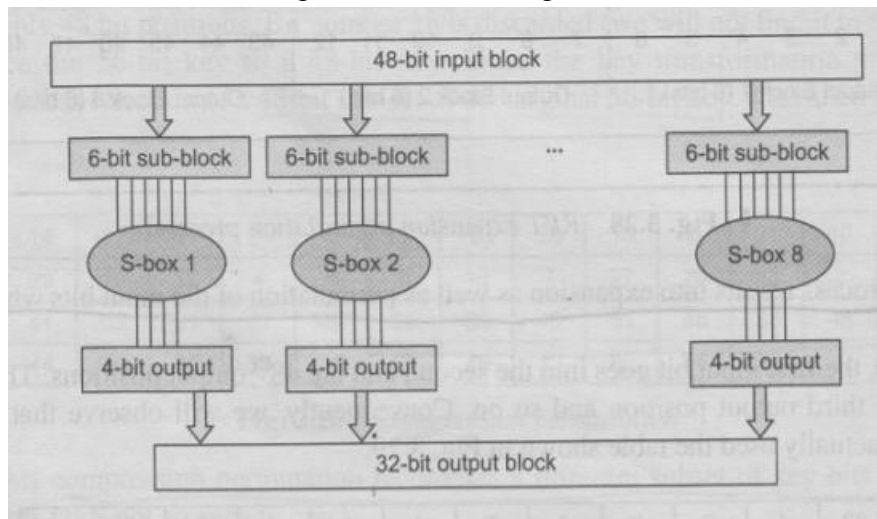


Step 1 : Key Transformation: The initial key is transformed into a 56-bit key by discarding every 8th bit of initial key. Thus ,for each round , a 56 bit key is available, from this 56-bit key, a different 48-bit sub key is generated during each round using a process called as key transformation Expansion Permutation Key Transformation S-box substitution XOR and swap P-box Permutation

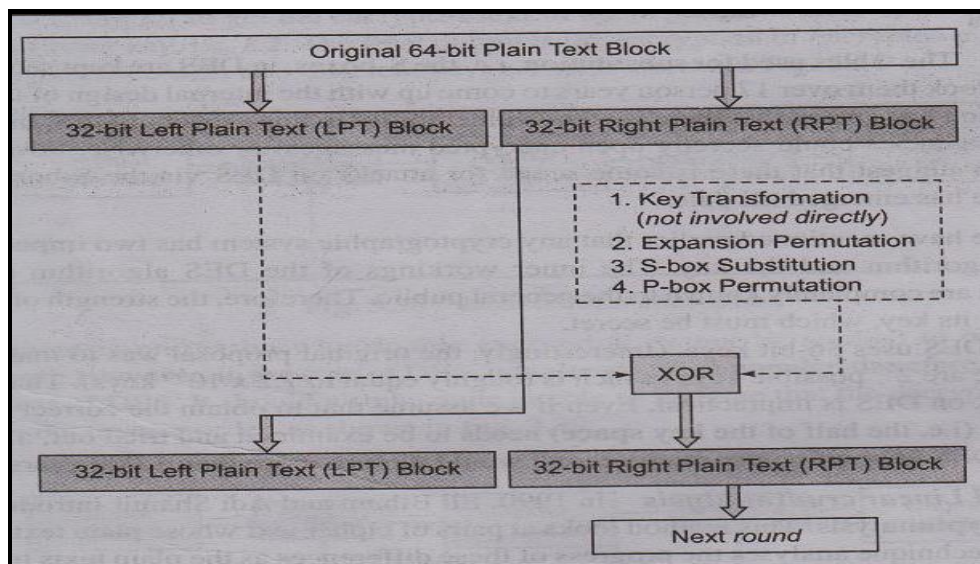
Step 2: Expansion Permutation: During Expansion permutation the RPT is

expanded from 32 bits to 48 bits. The 32-bit RPT is divided into 8 blocks, with each block consisting of 4-bits. Each 4-bits block of the previous step is then expanded to a corresponding 6-bit block, per 4-bit block, 2 more bits are added. They are the repeated 1st and 4th bits of the 4-bit block. The 2nd and 3rd bits are written as they were in the input. The 48 bit key is XORed with the 48-bit RPT and the resulting output is given to the next step.

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



Step 4: P- box Permutation: The output of S-box consists of 32-bits. These 32-bits are permuted using P-box. **Step 5: XOR and Swap:** The LPT of the initial 64-bits plain text block is XORed with the output produced by P box-permutation. It produces new RPT. The old RPT becomes new LPT, in a process of swapping.

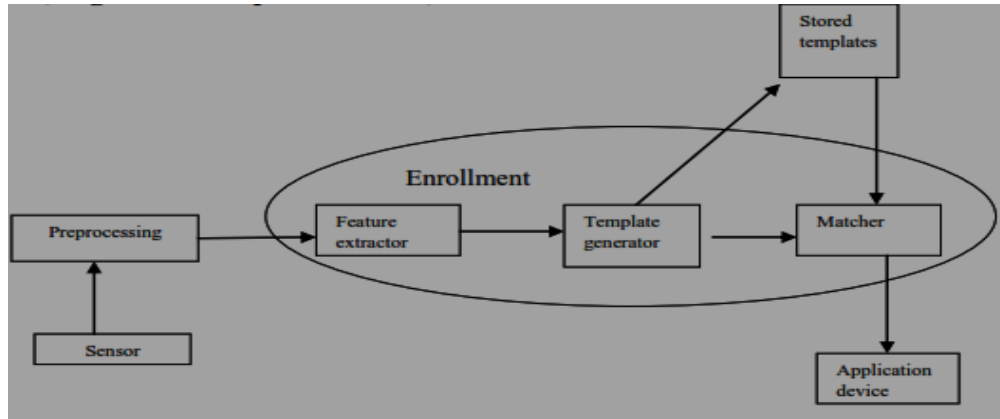




		<p>Final Permutation: At the end of 16 rounds, the final permutation is performed. This is simple transposition. For e.g., the 40th input bit takes the position of 1st output bit and so on.</p>	
	c	<p>Describe the components of NIDS with neat diagram. State its advantages & disadvantages.</p>	8 M
Ans	<p>Network-based Intrusion Detection Systems:</p> <div style="text-align: center;"> <pre> graph LR NT[NETWORK TRAFFIC] --> TC[TRAFFIC COLLECTOR] TC --> AE[ANALYTICAL ENGINE] DS[(DIGITAL SIGNATURE DB)] --> AE AS[ALARM STORAGE] --> AE AE --> UI[USER INTERFACE] AS --> R[REPORT] UI <--> R </pre> </div> <ol style="list-style-type: none"> 1. Traffic collection: 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: 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. <p>Advantages of Network-based Intrusion Detection Systems</p> <ul style="list-style-type: none"> • The deployment of network-based IDSs is usually easy with minimal effort. • Network-based IDSs can be made very secure and is often invisible to most attackers. • They can monitor a heterogeneous set of hosts and operating systems simultaneously, due to the fact that standard network protocols (e.g. TCP, UDP and IP) are supported and used by most major operating systems. <p>Disadvantages of Network-based Intrusion Detection Systems</p> <ul style="list-style-type: none"> • Network-based IDSs cannot analyse encrypted information. This problem is increasing as more organizations and attackers use virtual private networks, which normally utilize encrypted information. • The processing load in a large or busy network may cause significant difficulties to the analysis engine part of the IDS. This condition (high 		<p>Diagram: 2 marks, IDS components :2 marks, Advantades: 2 marks, Disadvantages:2 marks</p>



		<p>processing load) can seriously limit an IDS's ability to detect attacks when the network load is above a specific amount of network traffic. Although some vendors have adopted hardware-based solutions for IDSs, to increase the speed of their processing capability (and the cost of implementation), the limitation still remains.</p> <ul style="list-style-type: none"> The need to analyse packets as fast as possible, force developers to detect fewer attacks. Thus, the detection effectiveness is often compromised for the sake of cost effectiveness. 																			
3		Attempt any FOUR :	16 M																		
	a	Differentiate between virus and worm.	4 M																		
	Ans	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Virus</th> <th style="text-align: center;">Worm</th> </tr> </thead> <tbody> <tr> <td>The virus is the program code that attaches itself to application program and when application program run it runs along with it.</td> <td>The worm is code that replicate itself in order to consume resources to bring it down.</td> </tr> <tr> <td>It inserts itself into a file or executable program.</td> <td>It exploits a weakness in an application or operating system by replicating itself.</td> </tr> <tr> <td>It has to rely on users transferring infected files/programs to other computer systems.</td> <td>It can use a network to replicate itself to other computer systems without user intervention.</td> </tr> <tr> <td>Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.</td> <td>Usually not. Worms usually only monopolize the CPU and memory.</td> </tr> <tr> <td>Virus may need a trigger for execution.</td> <td>Worm does not need any trigger.</td> </tr> <tr> <td>Virus is slower than worm.</td> <td>Worm is faster than virus</td> </tr> <tr> <td>Damage is mostly caused to local machine.</td> <td>It harms the network and consumes network bandwidth.</td> </tr> <tr> <td>E.g. Macro virus, Directory virus, Stealth Virus</td> <td>E.g. Code red</td> </tr> </tbody> </table>	Virus	Worm	The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.	It inserts itself into a file or executable program.	It exploits a weakness in an application or operating system by replicating itself.	It has to rely on users transferring infected files/programs to other computer systems.	It can use a network to replicate itself to other computer systems without user intervention.	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	Usually not. Worms usually only monopolize the CPU and memory.	Virus may need a trigger for execution.	Worm does not need any trigger.	Virus is slower than worm.	Worm is faster than virus	Damage is mostly caused to local machine.	It harms the network and consumes network bandwidth.	E.g. Macro virus, Directory virus, Stealth Virus	E.g. Code red	1 Mark each for any 4 points
Virus	Worm																				
The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.																				
It inserts itself into a file or executable program.	It exploits a weakness in an application or operating system by replicating itself.																				
It has to rely on users transferring infected files/programs to other computer systems.	It can use a network to replicate itself to other computer systems without user intervention.																				
Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	Usually not. Worms usually only monopolize the CPU and memory.																				
Virus may need a trigger for execution.	Worm does not need any trigger.																				
Virus is slower than worm.	Worm is faster than virus																				
Damage is mostly caused to local machine.	It harms the network and consumes network bandwidth.																				
E.g. Macro virus, Directory virus, Stealth Virus	E.g. Code red																				
	b	Enlist types of Biometrics. Explain any one Biometrics type in detail.	4 M																		
	Ans	<p>Biometric refers study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural characteristics.</p> <p>Different types of Biometrics (any two 1 Mark)</p> <ol style="list-style-type: none"> 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 	1 mark-Listing; 1.5 marks-diagram; 1.5 marks-explanation																		



Fingerprint registration & verification process

1. During registration, first time an individual uses a biometric system is called an enrolment.
2. During the enrolment, 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 enrolment is being performed the template is simply stored somewhere (on a card or within a database or both).if a matching phase is being performed the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm. The matching program will analyse the template with the input. This will then be output for any specified use or purpose.

c	Define the following terms: i) Cryptography ii) Cryptanalysis iii) Cryptology iv) Steganography	4 M
---	--	-----

Ans	<p>i) Cryptography- Cryptography is the art or science comprising the principles and methods of transforming an intelligible message into one that is unintelligible.</p> <div style="text-align: center;"> </div> <p>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.</p>	1 Mark each for relevant definitions
-----	--	--------------------------------------



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.



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.

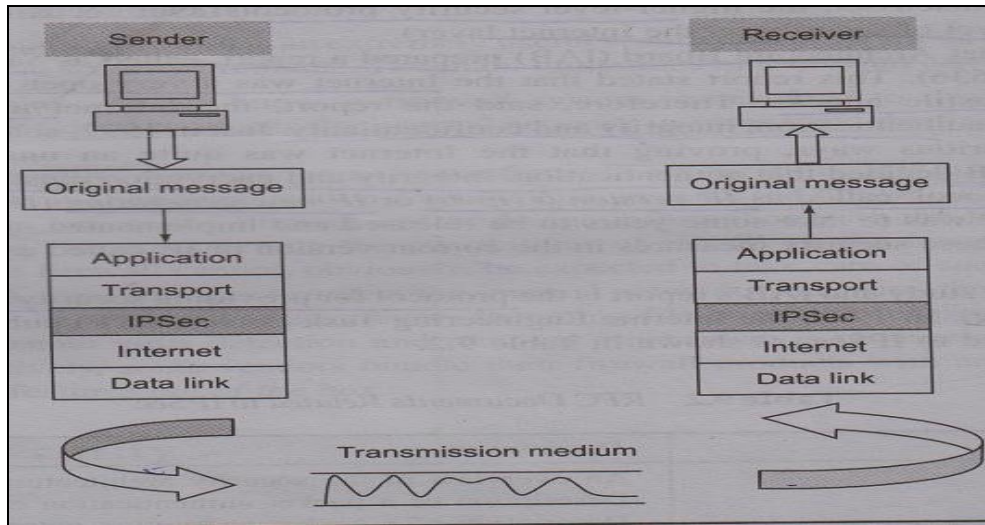
d Explain IPSec security with help of diagram.

4 M

Ans

IPsec architecture: IPsec is to encrypt and seal the transport and application layer data during transmission. Also offers integrity protection for the Internet layer. IPsec layer sits in between the transport and the Internet layers of conventional TCP/IP protocol stack.

2 Marks-
Diagram; 2
Marks-
explanation



IPsec actually consists of two main protocols

- a) Authentication Header (AH):
- b) Encapsulating Security Payload (ESP):

a) Authentication Header (AH): The AH provides support for data integrity and authentication of IP packets. The data integrity service ensures that data inside IP packet is not altered during the transit. The authentication service enables an end user or computer system to authenticate the user or the application at the other end and decides to accept or reject packets accordingly. This also prevents IP spoofing attacks. AH is based on MAC protocol, which means that the two communicating parties must share a secret key in order to

use AH.

b) Encapsulating Security Payload (ESP): ESP is a member of the IPsec protocol suite. In IPsec it provides origin authenticity, integrity and confidentiality protection of packets. ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure.

Modes of operation: Both AH and ESP works in two modes:

- 1. Tunnel mode:** In tunnel mode, IPsec protects the entire IP datagram. It takes an IP datagram, adds the IPsec header and trailer and encrypts the whole thing. It then adds new IP header to this encrypted datagram.
- 2. Transport mode:** Transport mode does not hide the actual source and destination addresses. They are visible in plain text, while in transit. In the transport mode, IPsec takes the transport layer payload, adds IPsec header and trailer, encrypted datagram.

e	What is Secure Electronic Transaction? Enlist and describe any four components of SET.	4 M
----------	---	-----

Ans	<p>Secure electronic Transaction is an open encryption and security specification that is designed for protecting credit card transactions on the Internet. It is a set of security protocols and formats that enable the users to employ the existing credit card payment infrastructure on the internet in a secure manner.(1 mark)</p> <div style="text-align: center;"> </div> <p>Components of SET (1 mark)</p> <ol style="list-style-type: none"> 1) Cardholder 2) Merchant 3) Issuer 4) Acquirer 5) Payment gateway 6) Certification Authority(CA) 	<p>1 Mark- What is SET; 1 Mark- enlisting any 4 components ; 2 Marks- Explanation of any four components</p>
------------	---	--



		<p>Describe any four (1/2 mark for any 4 component)</p> <ol style="list-style-type: none">1) Cardholder: A cardholder is an authorized holder of a payment card such as MasterCard or Visa that has been issued by an Issuer.2) Merchant: Merchant is a person or an organization that wants to sell goods or services to cardholders.3) Issuer: The issuer is a financial institution that provides a payment card to a cardholder.4) Acquirer: this is a financial institution that has a relationship with merchants for processing payment card authorizations and payments. Also provides an assurance that a particular cardholder account is active and that the purchase amount does not exceed the credit limits. It provides electronic fund transfer to the merchant account.5) Payment Gateway: It processes the payment messages on behalf of the merchant. It connects to the acquirer's system using a dedicated network line.6) Certification Authority (CA): This is an authority that is trusted to provide public key certificates to cardholders, merchant, and Payment Gateway.	
4	A	Attempt any THREE :	12 M
	a	Explain active attack and passive attack with suitable example.	4 M
	Ans	<p>Active Attack:</p> <ol style="list-style-type: none">1. In an active attack, the attacker tries to bypass or break into secured systems.2. This can be done through stealth, viruses, worms, or Trojan horses.3. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information.4. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave.5. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.6. Active attacks can be divided into four categories:<ol style="list-style-type: none">a. Masquerade A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.b. Replay In replay attack, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. • Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.c. Modification of messages Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning "Allow Ajay to read confidential accounts" is modified to mean "Allow Vijay to read	1 Mark-active attack explanation; 1 Mark-active attack example; 1 Mark-passive attack explanation; 1 Mark-passive attack example



confidential accounts.

d. Denial of Service(DoS)

Denial of service (DOS) attack scan exploits a known vulnerability in a specific application or operating system, or they may attack features (or weaknesses) in specific protocols or services. In this form of attack, the attacker is attempting to deny authorized users access either to specific information or to the computer system or network itself.

Passive Attack:

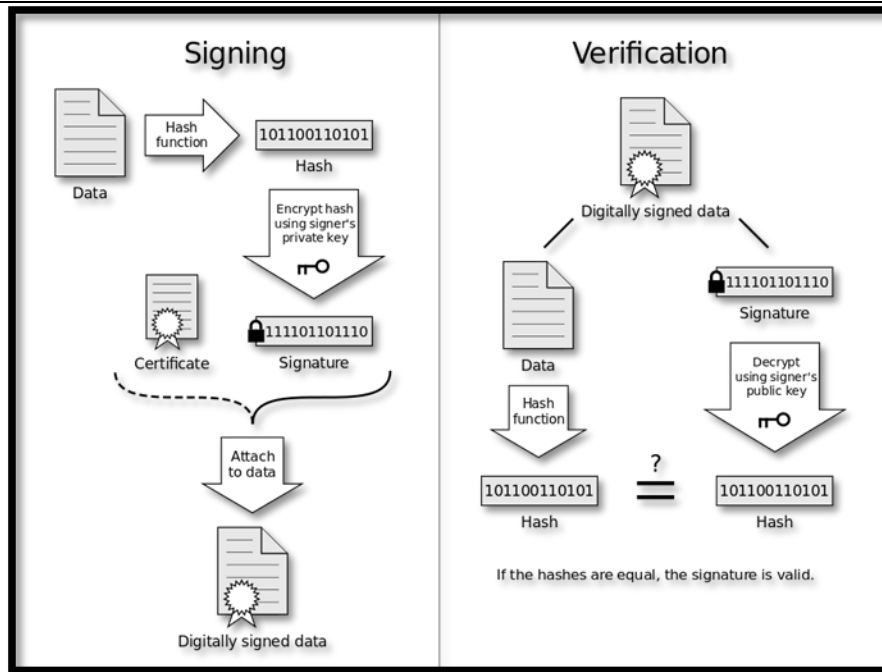
1. A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks.
2. Passive attacks include
 - a. traffic analysis,
 - b. release of message contents
 - c. monitoring of unprotected communications,
 - d. decrypting weakly encrypted traffic,
 - e. Capturing authentication information such as passwords.
3. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
4. The goal of the opponent is to obtain information that is being transmitted.
5. The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
6. A second type of passive attack, traffic analysis.
7. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.
8. Passive attacks are very difficult to detect because they do not involve any alteration of the data.
9. Typically, the message traffic is not sent and received in an apparently normal fashion and the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
10. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.



	b	State any four drawbacks of Retina scan Biometrics.	4 M
	Ans	<ol style="list-style-type: none">1. Very intrusive.2. It has the stigma of consumer's thinking it is potentially harmful to the eye.3. Comparisons of template records can take upwards of 10 seconds, depending on the size of the database.4. Very expensive.5. eye disease may pose problem6. not friendly, may cause discomfort to the user7. It is obscured by eyelashes, lenses and reflections, which create a problem, more often than not.8. Iris is partially blocked by eyelids which are difficult to control by individuals due to frequent blinking.	1 Mark each for any 4 relevant points
	c	What is cyber-crime? Describe hacking and cracking related to cybercrime.	4 M
	Ans	<p>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</p> <ol style="list-style-type: none">1. Hacking2. Cracking3. Theft4. Malicious software5. Child soliciting and abuse <p>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 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:</p> <ol style="list-style-type: none">1. White hat2. Black hat3. Grey hat4. Elite hacker5. Script hacker <p>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</p>	1 Mark- What is cybercrime; 1.5 Marks- Hacking; 1.5 Marks- Cracking



	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	Describe any TWO terms : Application Patches ii) Hotfix iii) Upgrades	4 M
Ans	i) Application patches: As O.S continues to grow and introduce new functions, the potential for problems with the code grows as well. It is almost impossible for an operating system vendor to test its product on every possible platform under every possible platform under every possible circumstance, so functionality and security issues do arise after an O.S has been released. Application patches are likely to come in three varieties: hot fixes, patches and upgrades. Application patches are supplied from the vendor who sells the application. Application patches can be provided in many different forms like can be downloaded directly from the vendor's web site or FTP site or by CD. Application patches are probably come in three varieties: hot fixes, patches and upgrades. i) 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. iii) Upgrades: The term upgrade has a positive implication-you are moving up to a better, more functional and more secure application. The most vendors will release upgrades for fixes rather than any new or enhanced functionality.	2 Marks each for any two terms
B	Attempt any ONE :	6 M
a	Describe Digital Signature mechanism with neat diagram.	6 M
Ans	A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.	3 Marks- Diagram; 3 Marks- Explanation



- A digital signature scheme typically consists of three algorithms
- A *key generation* algorithm that selects a *private key* uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
- A *signing* algorithm that, given a message and a private key, produces a signature.
- A *signature verifying* algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Digital Signature

1. A digital signature performs the same function as its physical counterpart, the sender “marks” the message so that the recipients can verify that the message really came from the sender.
2. The process of digitally signing a message starts with the creation of a unique identify for the message. The unique identifier can be created using a mathematical technique called Hashing.
3. A hash function uses a mathematical algorithm to convert the message into a short fixed-length of bits, often referred to as a “hash value” or “message digest” that uniquely represents the message used to create it.
4. The hash value is specific to the contents of the message. Thus any change to the message contents will change the hash value that would be generated by the hash function.
5. Next, the hash value is encrypted using the sender’s private key. Finally, the message is sent along with the encrypted hash value.
6. On receiving the message and the encrypted hash value, the recipient can only decrypt the hash value using the sender’s public key.
7. This confirms that the message came from the sender and no one else, as long as the sender’s private key remains secure. The message can be

	rehashed and compared with the decrypted hash value-if the values do not match, then the message has been altered since it was same.	
b	List types of firewall. Explain packet filter with diagram.	6 M
Ans	<p>List of types of firewall:</p> <ul style="list-style-type: none"> • Packet filter as a firewall • Hardware Firewall • Software Firewall • Circuit level gateway firewall • Application level gateway firewall • Proxy server as a firewall <p><u>Packet Filtering Firewall</u></p> <ul style="list-style-type: none"> • A firewall works as a barrier, or a shield, between your PC and cyber space. • When you are connected to the Internet, you are constantly sending and receiving information in small units called packets. • The firewall filters these packets to see if they meet certain criteria set by a series of rules, and thereafter blocks or allows the data. • This way, hackers cannot get inside and steal information such as bank account numbers and passwords from you. <div style="text-align: center;"> <p>The diagram shows an oval labeled 'Internal(private) network' on the left, connected by a line to a blue square with a white cross labeled 'firewall'. Another line connects the firewall to a jagged orange starburst labeled 'internet' on the right. A dashed line encloses the internal network and the firewall.</p> </div> <p align="center">Packet filter</p> <div style="text-align: center;"> <p>The diagram shows a blue square with a white cross labeled 'firewall' in the center. To its left are four blue rectangles labeled 'Outgoing packets'. To its right are three blue rectangles labeled 'Incoming packets'. A box below the firewall contains the text: 'Receive each packet. Apply rules. If no rules, apply default'. A line connects this box to the firewall.</p> </div>	<p>Listing of types of firewall: 2 mark, Explanation of packet filter as a firewall: 2 marks ,diagram of packet filter as a firewall: 2 mark</p>



		<p>Working:-</p> <ol style="list-style-type: none">1. 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.2. A packet filter performs the following functions.<ol style="list-style-type: none">a. Receive each packet as it arrives.b. 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.c. If there is no match with any rule, take the default action. It can be discard all packets or accept all packets.3. Advantages: simplicity, transparency to the users, high speed4. Disadvantages: difficult to set up packet filtering rules, lack of authentication.	
5		Attempt any TWO :	16 M
	a	Describe the following terms: <ol style="list-style-type: none">i) Intrudersii) Insidersiii) Sniffingiv) Spoofing	8 M
	Ans	<p>i) Intruders:</p> <ul style="list-style-type: none">• 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.• 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 <p>ii) Insiders:</p> <ul style="list-style-type: none">• More dangerous than outsiders As they have the access and knowledge to	2 M for each term correct explanation



	<p>cause</p> <ul style="list-style-type: none"> • 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 <p>iii) Sniffing:</p> <ul style="list-style-type: none"> • This is software or hardware that is used to observe traffic as it passes through a network on shared broadcast media. • It can be used to view all traffic or target specific protocol, service, or string of characters like logins. • Some network sniffers are not just designed to observe the all traffic but also modify the traffic. • Network administrators use sniffers for monitoring traffic. • They can also use for network bandwidth analysis and to troubleshoot certain Problems such as duplicate MAC addresses. <p>iv) Spoofing:</p> <ul style="list-style-type: none"> • Spoofing is nothing more than making data look like it has come from a different source. • This is possible in TCP/ IP because of the friendly assumption behind the protocol. When the protocols were developed, it was assumed that individuals who had access to the network layer would be privileged users who could be trusted. • When a packet is sent from one system to another, it includes not only the destination IP address ant port but the source IP address as well which is one of the forms of Spoofing. • Example of spoofing email spoofing, URL spoofing, IP address spoofing. 	
b	<p>What is access control? Describe following access control:</p> <p>i) DAC</p> <p>ii) MAC</p> <p>iii) RBAC</p>	8 M
Ans	<p>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.</p> <p>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</p> <p>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</p>	Access control Definition: 2M ,Each access control description: 2M

	<p>that access.</p> <p>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.</p>	
<p>c</p>	<p>Explain the Kerberos with help of suitable diagram.</p>	<p>8 M</p>
<p>Ans</p>	<p>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.</p> <div data-bbox="272 625 1307 1239" data-label="Diagram"> </div> <p>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.</p> <p>The entire process takes a total of eight steps, as shown below.</p> <ol style="list-style-type: none"> 1. The authentication service, or AS, receives 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 created. 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 	<p>Diagram: 2M, Kerberos Description in detail: 6M</p> <p>Any one answer given below can be considered</p> <p>2 marks diagrams</p> <p>4 marks Explanation of correct steps.</p>

- TGS, to get authenticated.
5. The TGS creates an encrypted key with a timestamp, and grants the client a service ticket.
 6. The client decrypts the ticket, tells the TGS it has done so, and then sends its own encrypted key to the service.
 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.

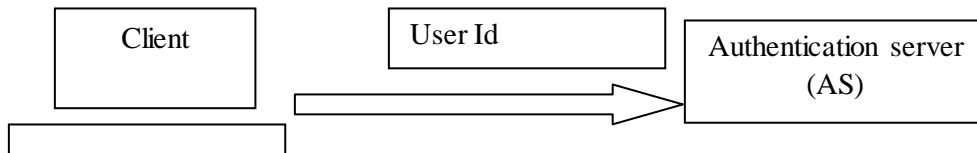
OR

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.

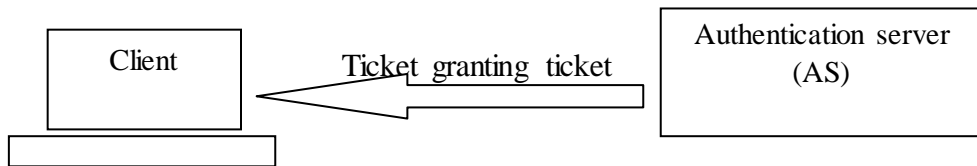
When working with the encryption key, the details are actually sent to a **key distribution center** (KDC), instead of sending the details directly between each computer.

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

1. The authentication service, or AS, receives 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.

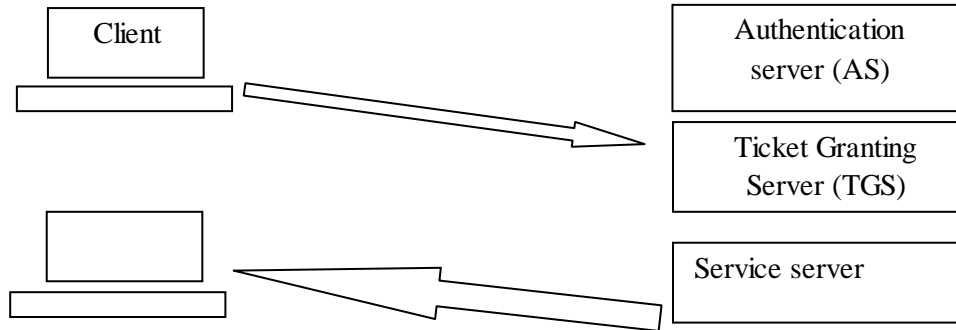


2. Upon verification, a timestamp is created. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours. The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless. (This is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



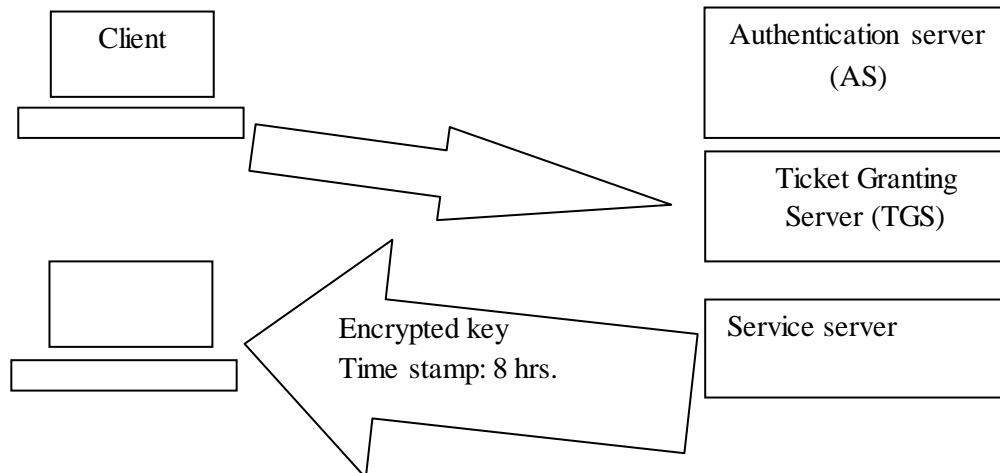
Time stamp: 8 hrs.

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.

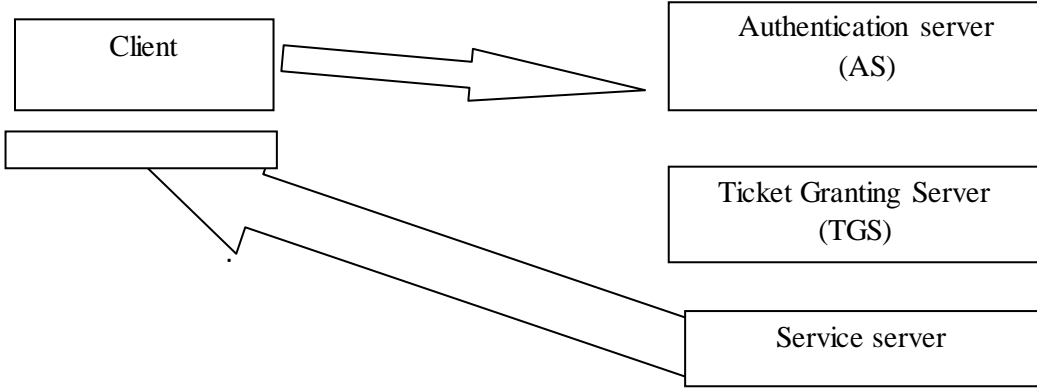


TGT Ticket Time stamp: 8 hrs.

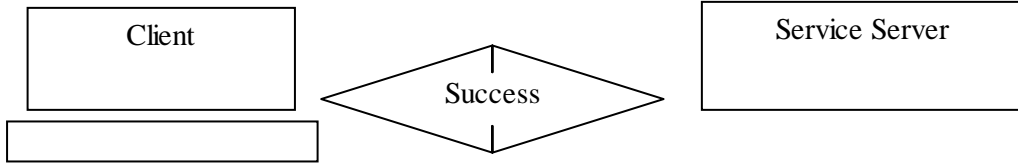
5. The TGS creates an encrypted key with a timestamp, and grants the client a service ticket.



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



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.

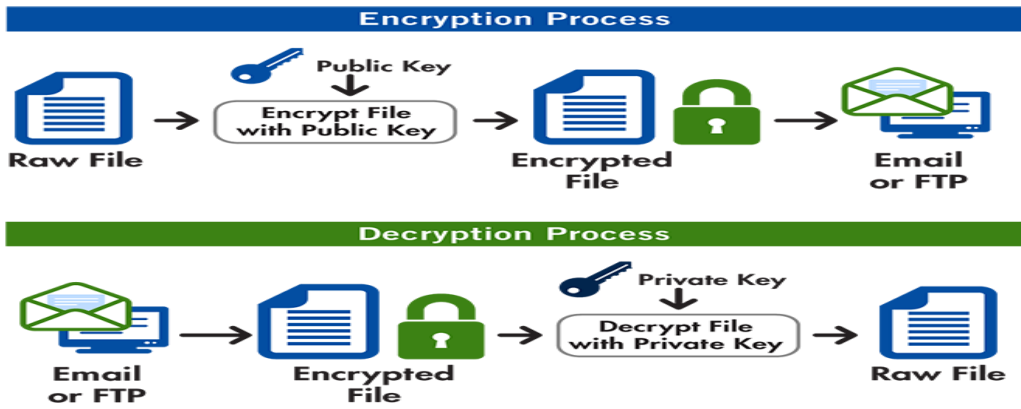


8. The client decrypts the ticket. If the keys are still valid, communication is initiated between client and server.

6	Attempt any FOUR :	16 M
a	Explain Man-In-Middle attack with help of diagram.	4 M
Ans	<p>Man-In-Middle attack</p> <p>A man in the middle attack occurs when attackers are able to place themselves in the middle of two other hosts that are communicating in order to view or modify the traffic. This is done by making sure that all communication going to or from the target host is routed through the attacker's host. Then the attacker is able to observe all traffic before transmitting it and can actually modify or block traffic. To the target host, communication is occurring normally, since all expected replies are received.</p>	<p>Diagram: 2M, Description: 2M</p>
b	State any four advantages of Biometrics.	4M



Ans	<p><u>Identification accuracy</u> Since every individual on the planet possesses unique physiological features that can't be easily swapped, shared, or stolen, biometric identification has the potential to accurately identify someone without a shadow of a doubt nearly 100% of the time. Occasionally, the ability to accurately identify someone can be affected by environmental, age, or skin integrity issues, but with a multimodal biometric identification system you can eliminate those factors. Multiple biometric attributes can identify someone with 100% certainty every time you scan them.</p> <p><u>Difficult to forge</u> Biometric attributes are almost impossible to forge or duplicate. Even if you manage to forge a biometric attribute such as a fingerprint, modern biometric devices with liveness detection have the capability to identify a fake from the original.</p> <p><u>Establishes accountability</u> Implementation of a biometric identification solution creates a concrete activity audit trail to help establish accountability. Each and every action or transaction will be recorded and clearly documented by the individual associated with it which reduces the possibility of system misuse and fraud.</p> <p><u>Adds convenience</u> Biometric technology makes individual identification convenient without the need to carry around ID cards or remember complicated passwords. Due to the fact that passwords can be forgotten or easily guessed and the fact that ID cards can be damaged, swapped, or shared, biometrics are more convenient because individual physiological attributes are always with you.</p> <p><u>Biometrics reduces administrative costs</u> Modern biometric identification management systems are comprised of hardware and software that are simple to install and easy to use. This reduces the need for intense training and ongoing management costs.</p> <p><u>Scalable</u> As your business develops and grows, it's important to have systems in place that can scale with the growth of your business. Biometric security systems are flexible and easily scalable. Whether you want to secure more areas of your facility or just add more data for additional employees, biometric security systems will grow alongside your business for ease and security.</p> <p><u>Profitable</u> The return on investment (ROI) on a biometric security system is very high. For one, it's much more effective at avoiding fraud than most security systems, protecting your business from potentially catastrophic breaches.</p>	Any 4 advantages 4M, any other suitable advantage also carries mark
c	What is PGP? How PGP is used for email security?	4 M
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.	PGP Definition: 2M, Steps in PGP for email security: 2M



There are five steps as shown below:

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.

d	Describe the following terms w.r.t cyber laws: i) IT Act, 2000 ii) IT Act, 2008	4 M
Ans	<p>(i) IT act 2000</p> <p>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.</p> <p>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 is important to understand what the various perspectives of the IT Act 2000 are and what it offers.</p> <p>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.</p>	Each IT Act Description: 2M



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 advise 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.

OR

IT act 2000

According to Indian cyber laws, Information technology is the important law and it had passed in Indian parliament in year 2000. This act is helpful to encourage business by use of internet. Due to misuse of internet and increase of cybercrime, the Govt. of India made an act for safeguarding the internet users.

The main objectives of this act are as follows.

1. To provide legal recognition to the transaction that can be done by electronic way or by using internet.
2. To provide legal recognition to digital signature used in transaction.
3. To provide facilities like filling of document online relating to admission or registration.
4. To provide facility to any company that they can store their data in electronic storage.
5. To provide legal recognition for bankers and other companies to keep accounts in electronic form.



(i) 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 of the transaction i.e. Electronic Data Interchange (EDI) and other electronic communications. This Act also gives facilities for electronic filing 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.

e

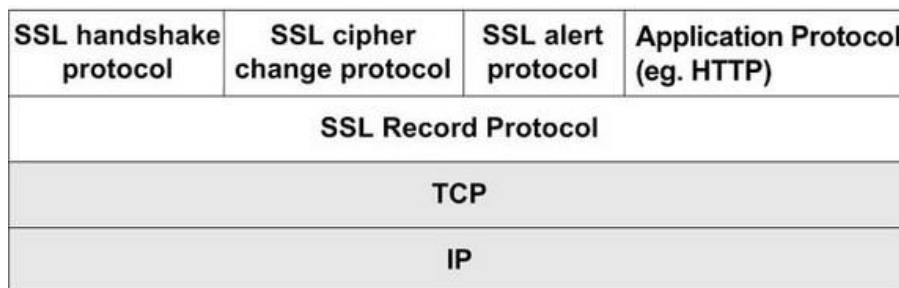
Explain architecture of secure sockets layer (SSL) with help of diagram.

4 M

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

Diagram:
2M,
Explanation
: 2M



	<p>segments above the transport layer, which is a network connection component above the program layer.</p> <p>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.</p> <p>The objectives of SSL are:</p> <ul style="list-style-type: none">• 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. <p>SSL is the predecessor of Transport Layer Security (TLS), which is a cryptographic protocol for secure Internet data transmission.</p>	
--	---	--