



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

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)	<b>Attempt any THREE of the following:</b>	<b>12Marks</b>
	(a)	<b>Describe CIA Security model.</b>	<b>4M</b>
	Ans:	<p><b><u>CIA Model for security:</u></b> Confidentiality, Integrity and Authentication i.e. these three concepts are considered as backbone of security. These concepts represent the fundamental principles of security.</p> <p><b>1. <u>Confidentiality:</u></b></p> <ul style="list-style-type: none"> <li>The principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message.</li> <li>Confidentiality gets compromised if an unauthorized person is able to access the contents of a message.</li> <li>Example of compromising the Confidentiality of a message is shown in fig</li> </ul> <div style="text-align: center;"> <pre> graph LR     A[A] --&gt; Secret[Secret]     Secret --&gt; B[B]     C[C] --&gt; Secret </pre> </div> <p><b>Fig. Loss of confidentiality</b></p> <ul style="list-style-type: none"> <li>Here, the user of a computer A send a message to user of computer B. another user C gets access to this message, which is not desired and therefore, defeats the purpose</li> </ul>	<b>(CIA: 2 marks, Explanation of Each Concept with Example:2 marks )</b>

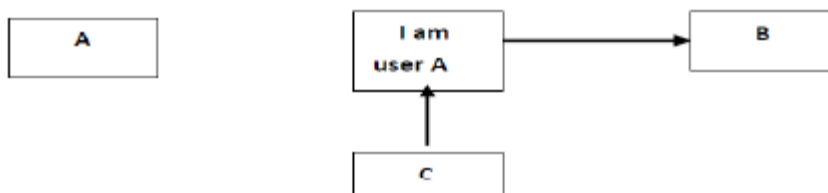


of Confidentiality.

- This type of attack is also called as **Interception**.

**2. Authentication:**

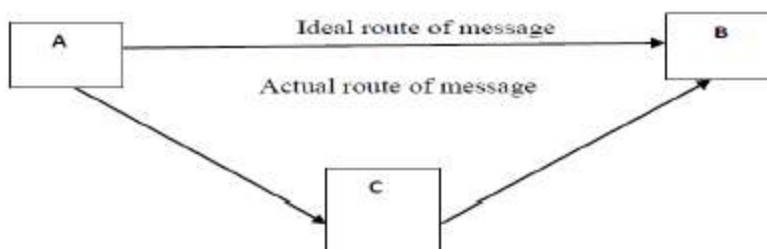
- Authentication helps to establish proof of identities.
- The Authentication process ensures that the origin of a message is correctly identified.
- For example, suppose that user C sends a message over the internet to user B. however, the trouble is that user C had posed as user A when he sent a message 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**

**3. 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**



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514

	(b)	<b>What is shoulder surfing? How it can be prevented?</b>	<b>4M</b>
	Ans:	<ul style="list-style-type: none"><li>• <b>Shoulder surfing</b> is a similar procedure in which attackers position themselves in such a way as-to be-able to observe the authorized user entering the correct access code or data.</li><li>• 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.</li><li>• Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information.</li><li>• 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.</li><li>• Shoulder surfing can also be done long-distance with the idea of binoculars or other vision-enhancing devices.</li><li>• <b><u>To prevent shoulder surfing:</u></b></li></ul> <p>Experts recommend that you shield paper work or your keypad from view by using your body or cupping your hand.</p>	<b>(Explanation: 3 marks, Prevention: 1 mark)</b>
	(c)	<b>Describe symmetric and asymmetric key cryptography.</b>	<b>4M</b>
	Ans:	<p><b><u>Symmetric-Key Cryptography:</u></b></p> <ul style="list-style-type: none"><li>• Symmetric-key cryptography uses a single key for both encryption and decryption.</li><li>• Encryption and decryption algorithm are inverse of each other.</li></ul> <p><b>Example:</b> To create the cipher text from the plain text John uses an encryption algorithm and a key. To create the plain text from cipher text, Bob uses the decryption algorithm and the same key.</p> <p><b><u>Asymmetric-Key cryptography:</u></b></p> <ul style="list-style-type: none"><li>• It is also called public key cryptography.</li><li>• In public key cryptography two keys: a private key and a public key is used.</li><li>• Encryption is done through the public key and decryption through private key.</li><li>• Receiver creates both the keys and is responsible for distributing its public key to the communication community.</li><li>• <b>Example:</b> The sender (say John) uses the public key to encrypt the plain text into cipher text and the receiver (say Bob) uses his private key to decrypt the cipher text.</li></ul>	<b>(Symmetric key: 2 marks, Asymmetric key: 2 marks)</b>



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514

(d)	<b>What is a Virus? Describe various phases of virus.</b>	<b>4M</b>
Ans:	<p>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.</p> <p>During the lifecycle of virus it goes through the following four phases:</p> <ul style="list-style-type: none"><li>• <b>Dormant phase:</b> The virus is idle and activated by some event.</li><li>• <b>Propagation phase:</b> It places an identical copy of itself into other programs or into certain system areas on the disk.</li><li>• <b>Triggering phase:</b> The virus is activated to perform the function for which it was intended.</li><li>• <b>Execution phase:</b> The function of virus is performed</li></ul>	<b>(Definition of Virus: 1 mark, Listing phases of Virus: 1 mark, Explanation of Phases: 2 marks)</b>
(B)	<b>Attempt any ONE of the following:</b>	<b>6Marks</b>
(a)	<b>Describe with the neat diagram model for security.</b>	<b>6M</b>
Ans:	<div><div><div>Sender</div><div>Original Message (Plain Text)</div><div>Encryption</div><div>Cipher Text</div></div><div><div>Receiver</div><div>Original Message (Plain Text)</div><div>Decryption</div><div>Cipher Text</div></div><div><div></div><div></div><div></div><div></div></div></div> <p>OR</p>	<b>( Diagram: 2 marks, Explanation : 4 marks)</b>

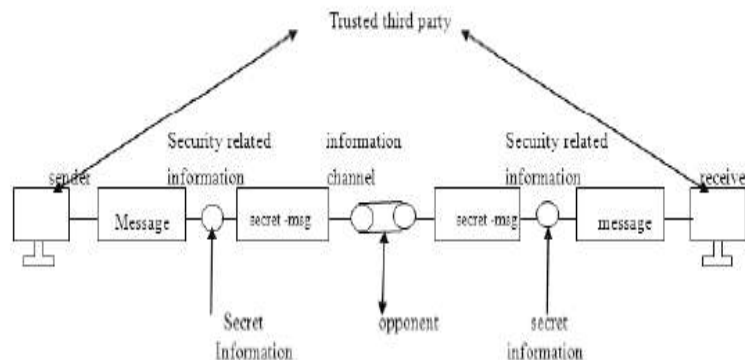


**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514



A message is to be transferred from one user to another user in secret form using this security system it can be two or more parties accessing information via Internet.

Sender & receiver are principals of transaction and must cooperate for exchange to take place.

**Model shows four basic tasks:**

1. Design algorithm in such a way that an opponent cannot defeat its purpose. This algorithm is used for security related information.
2. Generate secret information that can be used with algorithm.
3. Develop method for distributing and sharing of secret information.
4. Specify a protocol which can be used by two principals that make use of security algorithm and secret information to achieve a security service. An information channel is established by defining a route through Internet from source to destination with the help of communication protocol like TCP/IP or using normal PC to PC communication through any media.

Techniques for providing security have following components:-

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

**OR**

**(2 mark for each point)**

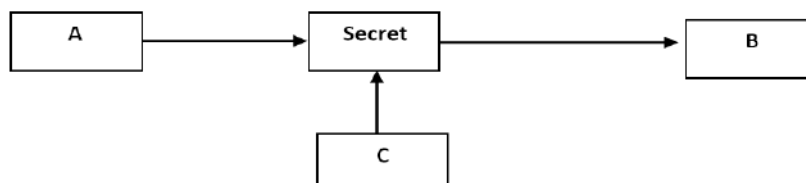
**Model for security:**

**1. Confidentiality:**

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



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

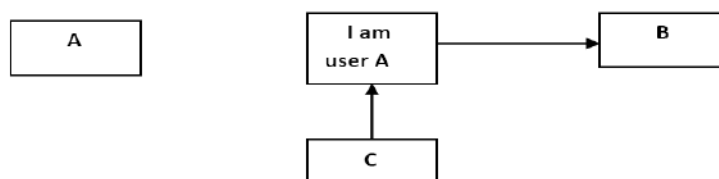


**Fig. Loss of confidentiality**

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

## **2. 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**

## **3. 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



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

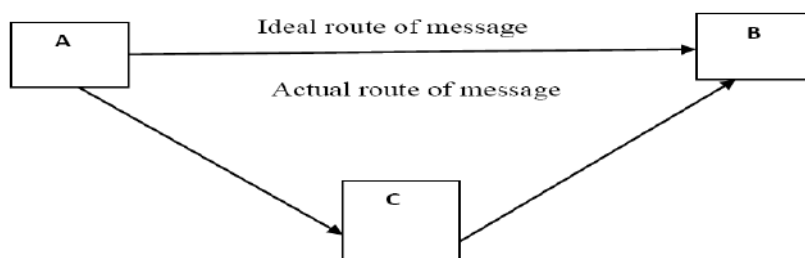
**Subject Title: Computer Security**

**Subject Code:**

**17514**

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**

**(b) Describe the process of formatted partition recovery.**

**6M**

**Ans: Formatted partition recovery:**

- 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 of the following:**

**16Marks**

**(a) Describe the following term:**

**8M**

- Sniffing**
- Spoofing**



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

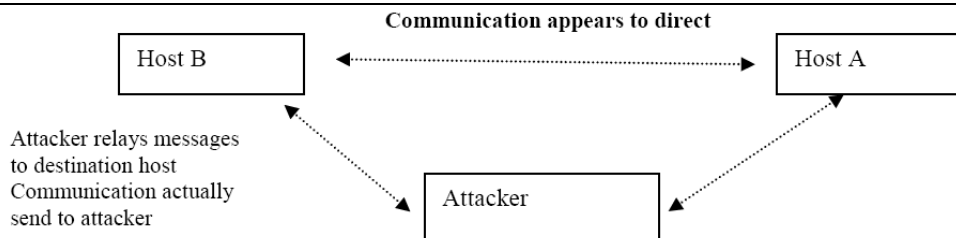
**Subject Title: Computer Security**

**Subject Code:**

**17514**

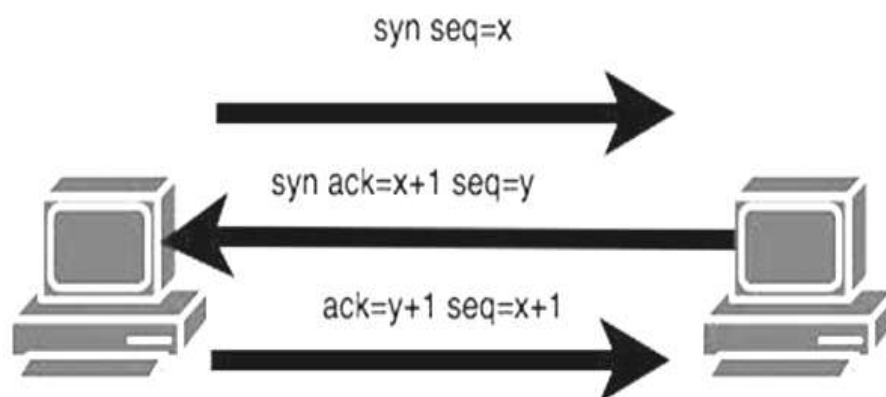
		<b>iii) Man-in-the middle</b> <b>iv) TCP/IP Hijack</b>	
	<b>Ans:</b>	<p><b>i) Sniffing:</b></p> <ul style="list-style-type: none"><li>• This is software or hardware that is used to observe traffic as it passes through a network on shared broadcast media.</li><li>• It can be used to view all traffic or target specific protocol, service, or string of characters like logins.</li><li>• Some network sniffers are not just designed to observe the all traffic but also modify the traffic.</li><li>• Network administrators use sniffers for monitoring traffic.</li><li>• They can also use for network bandwidth analysis and to troubleshoot certain problems such as duplicate MAC addresses.</li></ul> <p><b>ii) Spoofing:</b></p> <ul style="list-style-type: none"><li>• Spoofing is nothing more than making data look like it has come from a different source.</li><li>• 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.</li><li>• When a packet is sent from one system to another, it includes not only the destination IP address and port but the source IP address as well which is one of the forms of Spoofing.</li><li>• Example of spoofing: e-mail spoofing, URL spoofing, IP address spoofing.</li></ul> <p><b>iii) Man-in-the middle:</b></p> <ul style="list-style-type: none"><li>• 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.</li><li>• This is done by making sure that all communication going to or from the target host is routed through the attacker's host.</li><li>• Then the attacker is able to observe all traffic before transmitting it and can actually modify or block traffic.</li><li>• To the target host, communication is occurring normally, since all expected replies are received.</li><li>• To prevent this attack both sender and receiver must authenticate each other.</li></ul>	<b>(2 marks for Each)</b>





**iv) TCP/IP Hijack:**

- TCP/IP Hijacking is when an authorized user gains access to a genuine network connection of another user.
- It is done in order to bypass the password authentication which is normally the start of a session.
- In theory, a TCP/IP connection is established as shown below



- To hijack this connection, there are two possibilities –
- Find the seq which is a number that increases by 1, but there is no chance to predict it.
- The second possibility is to use the Man-in-the-Middle attack which, in simple words, is a type of network sniffing. For sniffing, we use tools like Wireshark or Ethercap.
- **Example:**
- An attacker monitors the data transmission over a network and discovers the IP's of two devices that participate in a connection.
- When the hacker discovers the IP of one of the users, he can put down the connection of the other user by DoS attack and then resume communication by spoofing the IP of the disconnected user.



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514

(b)	Describe Biometric security mechanism with suitable diagram.	8M
Ans:	<div data-bbox="311 415 1344 940"><p>The diagram illustrates the biometric security mechanism. It starts with a 'Sensor' box at the bottom left, which points to a 'Preprocessing' box. An arrow from 'Preprocessing' leads to a 'Feature extractor' box. From 'Feature extractor', an arrow points to a 'Template generator' box. An arrow from 'Template generator' points to a 'Matcher' box. Above the 'Matcher' box is a 'Stored templates' box, with an arrow pointing down to it. Below the 'Matcher' box is an 'Application device' box, with an arrow pointing down to it. A large oval labeled 'Enrollment' encircles the 'Feature extractor', 'Template generator', and 'Matcher' boxes. An arrow also points from 'Stored templates' to the 'Matcher' box.</p></div> <ul style="list-style-type: none"><li>• <b>Biometric</b> refers study of methods for uniquely recognizing humans based upon one or more intrinsic <b>physical</b> or <b>behavioral</b> characteristics.</li><li>• Biometric identification is used on the basis of some unique physical attribute of the user that positively identifies the user.</li><li>• Example: finger print recognition, retina and face scan technic, voice synthesis and recognition and so on.</li><li>• Physiological are related to shape of the body.</li><li>• For example finger print, face recognition, DNA, palm print, iris recognition and so on.</li><li>• Behavioral are related to the behavior of a person.</li><li>• For example typing rhythm, gait, signature and voice.</li><li>• The first time an individual uses a biometric system is called an enrollment.</li><li>• During the enrollment, biometric information from an individual is stored.</li><li>• In the subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment.</li></ul> <ol style="list-style-type: none"><li>1. Preprocessing</li><li>2. Sensor</li><li>3. Feature extractor</li><li>4. Template generator</li><li>5. Matcher</li><li>6. Stored templates</li><li>7. Application device</li><li>8. Enrollment</li></ol>	(Diagram: 2 mark, Explanation: 4 marks, Example: 2 mark)



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

**Subject Title: Computer Security**

**Subject Code:**

**17514**

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

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

**Step 3)** The third block extracts necessary features. This step is an important step as the correct features need to be extracted in the optimal way.

**Step 4)** If enrollment is being performed the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm. The matching program will analyze the template with the input. This will then be output for any specified use or purpose.

- List of various biometrics used for computer security:
- Finger print
- Hand print
- Iris scan
- Face recognition
- DNA recognition
- Voice pattern
- Signature recognition
- Keystrokes

• **Example:**

**Fingerprint registration & verification process**

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

	(c)	<b>Describe DES Algorithm with suitable diagram.</b>	<b>8M</b>
	<b>Ans:</b>	<p>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.</p>	<p><b>(Definition: 1 mark ;</b></p> <p><b>Diagram: 1m; process Diagram: 1 mark, for each step: 1</b></p>

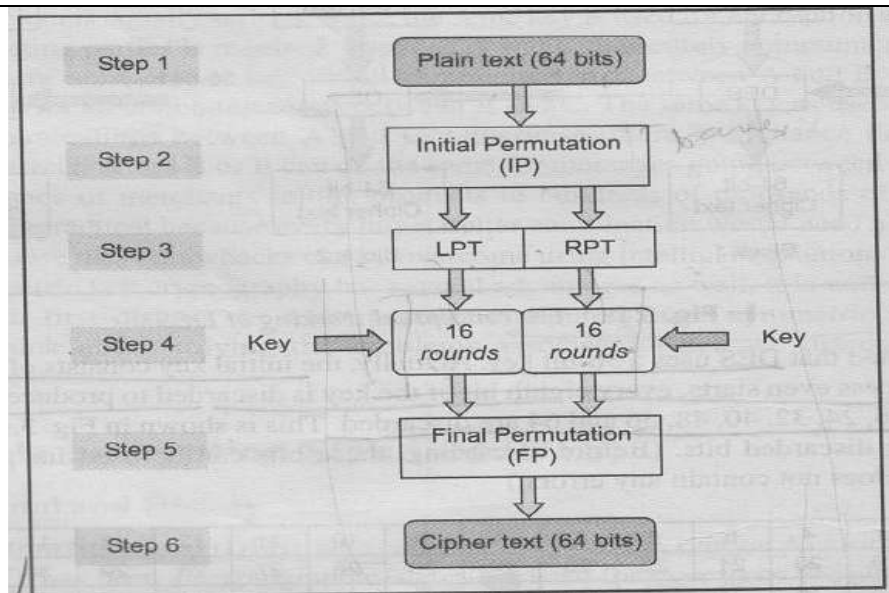


**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

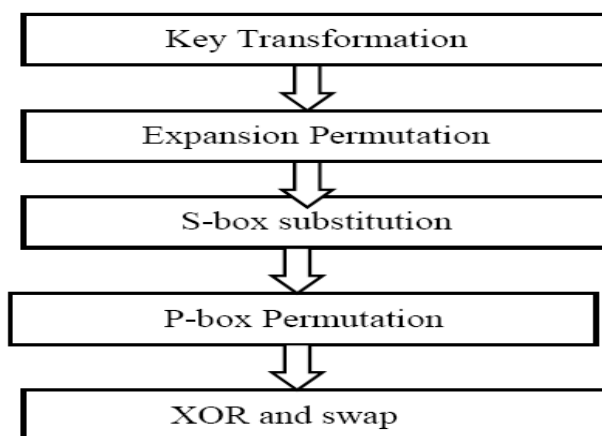
Subject Code:

17514



mark)

**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



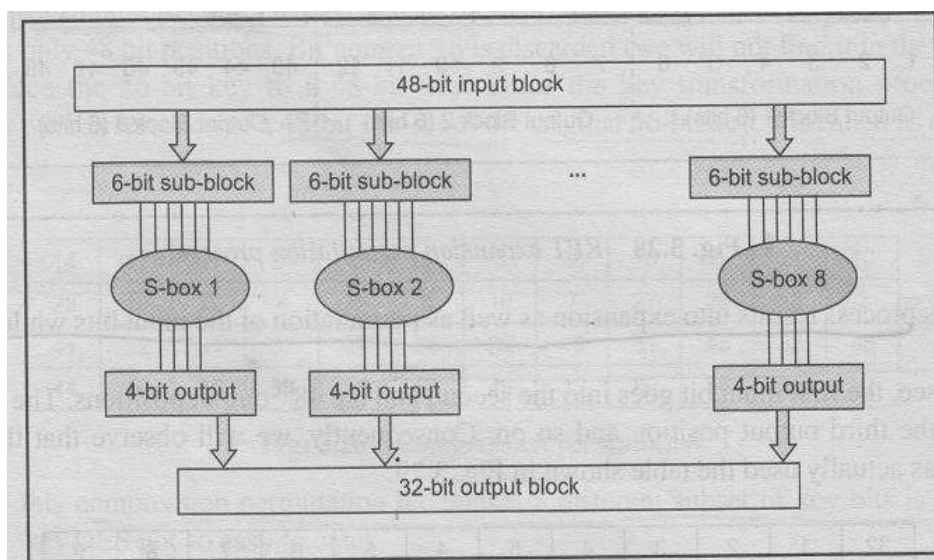
S-box substitution

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.

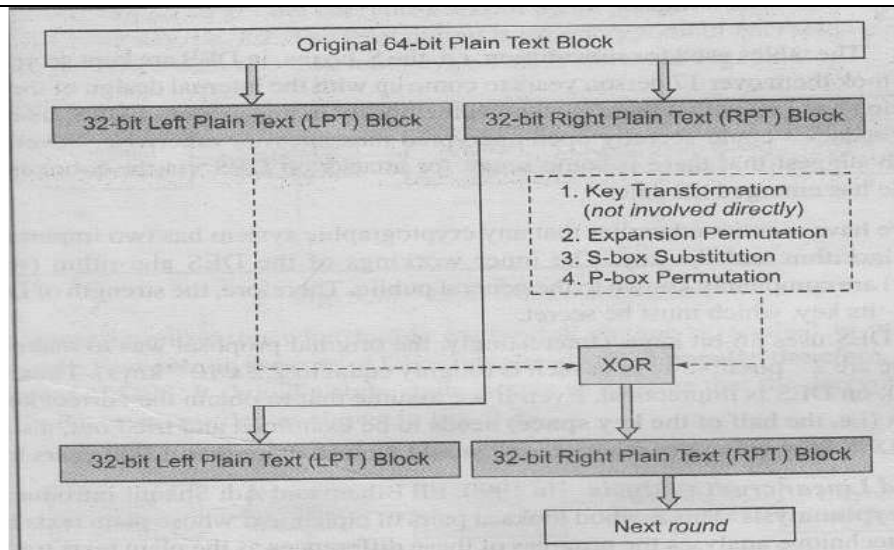


**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514



**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.

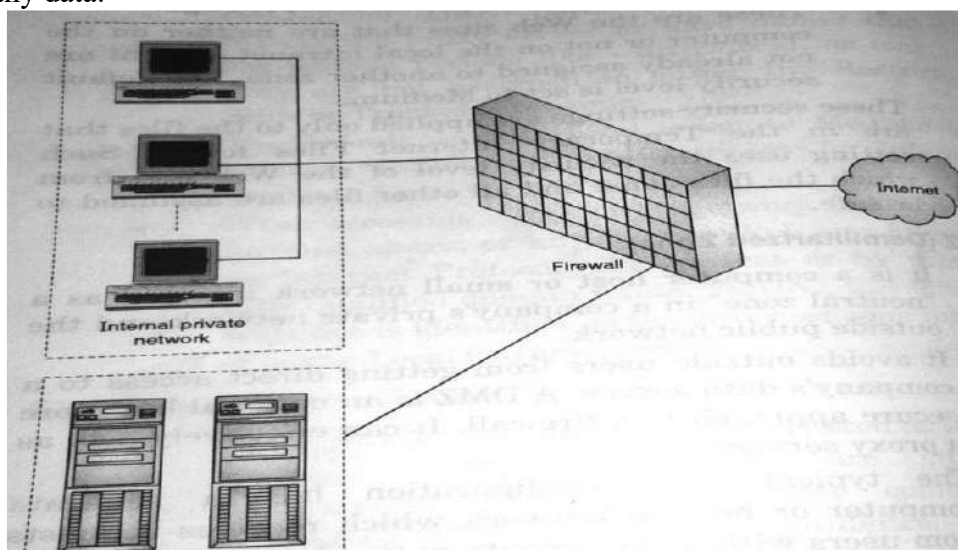
3. Attempt any FOUR of the following:

16Marks

(a) Describe DMZ with suitable diagram.

4M

**Ans:** It is a computer host or a small network inserted as a neutral zone between company's private network and outside public network. It prevents direct Access to a server that has company data.



(Relevant Diagram: 2 marks, 1 mark per point)

- It avoids outside users from getting direct access to a company's data server. A DMZ is an optional but more secure approach to a firewall. It can effectively acts as a



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

**Subject Title: Computer Security**

**Subject Code:**

**17514**

		<p>proxy server.</p> <ul style="list-style-type: none"><li>• The typical DMZ configuration has a separate computer or host in network which receives requests from users within the private network to access a web sites or public network.</li><li>• Then DMZ host initiates sessions for such requests on the public network but it is not able to initiate a session back into the private network. It can only forward packets which have been requested by a host.</li><li>• The public network's users who are outside the company can access only the DMZ host.</li><li>• It can store the company's web pages which can be served to the outside users. Hence, the DMZ can't give access to the other company's data.</li><li>• By any way, if an outsider penetrates the DMZ's security the web pages may get corrupted but other company's information can be safe.</li></ul>	
	<b>(b)</b>	<b>State the importance of security awareness. How it can be achieved?</b>	<b>4M</b>
	<b>Ans:</b>	<p>Security awareness program is most effective method to oppose potential social engineering attacks when organization's security goals and policies are established. An important element that should concentrate in training is which information is sensitive for organization and which may be the target of a social engineering attack</p> <ul style="list-style-type: none"><li>• An unaware user is as dangerous to the system as the attacker.</li><li>• An active security awareness program is most effective method to oppose potential social engineering attacks.</li><li>• User should be able to create their own easy to remember passwords, but should not be easy for someone else to guess or obtain using password cracking utilities.</li><li>• Password should meet some essential guidelines for e.g. password should contain some special characters etc.</li><li>• It should not consist of dictionary words.</li><li>• An approach of following closely behind a person who has just used their own access card or PIN to gain physical access. In this way an attacker can gain access to the facility without knowing the access code.</li><li>• An attacker positions themselves in such a way that he is able to observe the authorized user entering the correct access code.</li><li>• Because of possible risks, many organizations do not allow their users to load software or install new hardware without the information and help of administrators. Organizations also restrict what an individual do by received e-mails.</li><li>• An attacker can get physical access to a facility then there are many chances of obtaining enough information to enter into computer systems and networks. Many organizations restrict their employees to wear identification symbols at work.</li></ul>	<b>(Importance: 2 marks, Relevant point for acquiring security: 1mark)</b>



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514

	(c)	<b>What is steganography? What are its applications?</b>	<b>4M</b>
	<b>Ans:</b>	<ul style="list-style-type: none"> <li>Steganography is a technique that facilitates hiding of message that is to keep secret inside other message.</li> <li>Steganography is the art and science of writing hidden message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.</li> <li>Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, html or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text or even images.</li> <li>In modern steganography, data is first <b>encrypted</b> by the usual means and then inserted, using a special algorithm, into redundant data that is part of a particular file format such as a JPEG image.</li> <li>Steganography process :</li> <li>Cover-media + Hidden data + Stego-key = Stego-medium</li> <li>Cover media is the file in which we will hide the hidden data, which may also be encrypted using stego-key. The resultant file is stego-medium. Cover-media can be image or audio file.</li> <li>Steganography takes cryptography a step further by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.</li> <li><b>Applications :</b> <ol style="list-style-type: none"> <li>Confidential communication and secret data storing</li> <li>Protection of data alteration</li> <li>Access control system for digital content distribution</li> <li>Media Database systems</li> </ol> </li> </ul>	<b>(Explanation : 2 marks ,Applications : 2 mark, Any 2 applications expected )</b>
	(d)	<b>Describe IP based VLAN in detail.</b>	<b>4M</b>
	<b>Ans:</b>	<p>A Virtual Local Area Network (VLAN) is a logical network allowing systems on different physical networks to interact as if they were connected to the same physical network.</p> <p>IP Subnet VLANs</p> <div data-bbox="532 1625 1084 1892"> <pre> graph TD     Switch[Switch] --- PC1[PC 1 10.100.5.1]     Switch --- PC2[PC 2 10.100.5.30]     </pre> </div> <p>In this type of VLAN, all the incoming traffic will be divided according to the IP subnet address of each source/destination. This will provide great flexibility in network because</p>	<b>(Explanation : 3 marks, Diagram: 1 mark)</b>



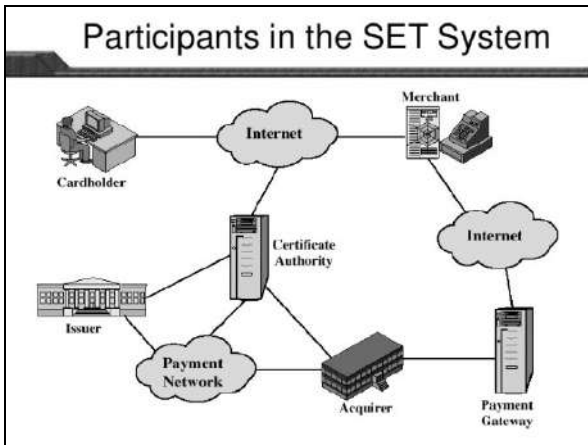


**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514

		the users can move computers from one location to another location and can remain in the same VLAN. The disadvantage of VLAN is that it needs additional processing for the layer 3 header and therefore it adds more latency than the other VLAN segments.	
	(e)	<b>Describe SET participants.</b>	<b>4M</b>
	<b>Ans:</b>	<p>For secure electronic transaction SET participant are there.</p> <ol style="list-style-type: none"> <li><b>1) Cardholders-</b> cardholder is an authorized holder of payment card like Master card, visa that has been issued by an issuer.</li> <li><b>2) Merchant-</b> A merchant is a person or organization that has goods or services to sell to cardholder.</li> <li><b>3) Issuer-</b> This is financial institution like bank.</li> <li><b>4) Acquirer-</b> This is a financial institution that establishes account with merchant &amp; process payment card authorization &amp; payment.</li> <li><b>5) Payment Gateway-</b> This is a function operated by acquire.</li> <li><b>6) The payment gateway process between SET &amp; existing bankcard payment networks .For authorization &amp; payment function.</b></li> <li><b>7) The merchant exchanges SET messages with payment gateway over internet.</b></li> <li><b>8) Certificate Authority-</b> This is an entity that is trusted to issue public key for cardholder, merchant &amp; payment gateways.</li> </ol>	<b>(Each participants: 1 mark , Any 4 participants expected )</b>
		 <p>The diagram illustrates the participants in the SET system and their interactions. At the top, a Cardholder and a Merchant are connected via the Internet. The Merchant is also connected to a Payment Gateway. The Payment Gateway is connected to an Acquirer. The Acquirer is connected to a Payment Network. The Payment Network is connected to an Issuer. The Issuer is connected to a Certificate Authority. The Certificate Authority is connected to the Cardholder, the Merchant, and the Payment Gateway. The Payment Gateway is also connected to the Certificate Authority.</p>	
4.	(A)	<b>Attempt any THREE:</b>	<b>12Marks</b>
	(a)	<p><b>Convert plain text into cipher text by using simple columnas technique of the following sentence:</b></p> <p><b>‘ALL IS WELL FOR YOUR EXAM’</b></p>	<b>4M</b>
	<b>Ans:</b>	<p>ALL IS WELL FOR YOUR EXAM</p> <p>The columnar transposition cipher is a transposition cipher that follows a simple rule for Mixing up the characters in the plaintext to form the cipher-text. It can be combined</p>	<b>(4 marks for Correct step )</b>



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

**Subject Title: Computer Security**

**Subject Code:**

**17514**

with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on its own. The cipher uses a columnar transposition to greatly improve its security.

**Algorithm:**

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

**Example**

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

To encrypt a below plaintext

ALL IS WELL FOR YOUR EXAM

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

The Encrypted text or Cipher text is:

**SFUM ILOA LLYX AWOR LERE**



	(b)	<b>Describe IPsec configuration.</b>	<b>4M</b>
	<b>Ans:</b>	<div data-bbox="435 380 1188 1087"></div> <p><b>IP sec overview:</b> It encrypts and seal the transport and application layer data during transmission. It also offers integrity protection for internet layer. It sits between transport and internet layer of conventional TCP/IP protocol</p> <p><b>1. Secure remote internet access:</b> Using IPsec make a local call to our internet services provider (ISP) so as to connect to organization network in a secure fashion from our house or hotel from there; to access the corporate network facilities or access remote desktop/servers.</p> <p><b>2. Secure branch office connectivity:</b> Rather than subscribing to an expensive leased line for connecting its branches across cities, an organization can setup an IPsec enabled network for security.</p> <p><b>3. Setup communication with other organization:</b> Just as IPsec allow connectivity between various branches of an organization, it can also be used to connect the network of different organization together in a secure &amp; inexpensive fashion.</p> <p><b>Basic Concept of IPsec Protocol:</b> IP packet consist two position IP header &amp; actual data IPsec feature are implemented in the form of additional headers called as extension header to the standard, default IP header. IPsec offers two main services authentication &amp; confidentiality. Each of these requires its own extension header. Therefore, to support these two main services, IPsec defines two IP extension header one for authentication &amp; another for confidentiality.</p>	<b>(Diagram: 2 marks , Explanation: 2 marks )</b>



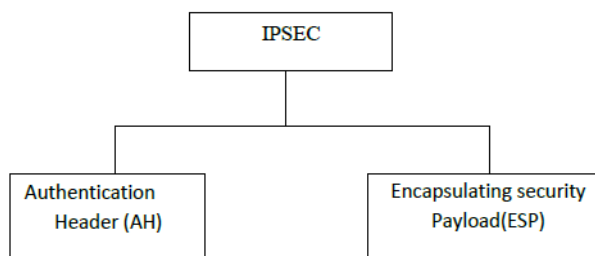
**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

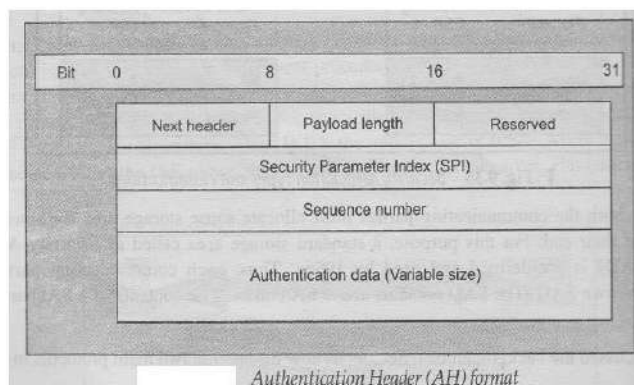
Subject Code:

17514

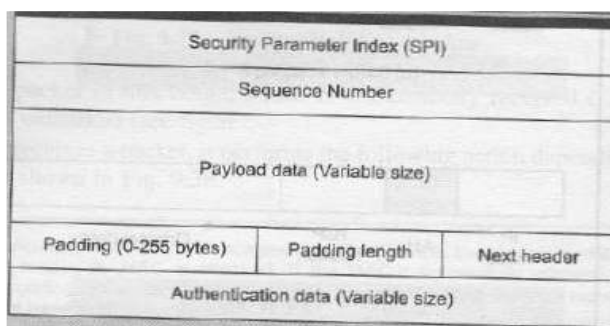
It consists of two main protocols



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



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





**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514

	(c)	<b>Describe the process of cyber crime investigation.</b>	<b>4M</b>
	<b>Ans:</b>	<ul style="list-style-type: none"> <li>• Cybercrime investigation is done to determine the nature of crime and collect evidence e.g. hardware, software related with the crime.</li> <li>• This is used to stop a crime in progress, report crime which was done in the past.</li> <li>• Relevant IT training is necessary for Cybercrime investigation.</li> <li>• First step of investigation team is to secure computers, networks &amp; components that are connected with crime.</li> <li>• Investigators may clone the system to explore it. They can take a detailed audit of a computer</li> <li>• <b>Interviews:</b> Investigators arrange interviews with victims, witness.</li> <li>• <b>Surveillance:</b> Investigators checks the digital activities, monitors all elements of suspect.</li> <li>• <b>Forensics:</b> Mining a computer for all related information to detect potential evidence.</li> <li>• <b>Undercover:</b> Steps to uncover to trap criminals using fake online identities.</li> <li>• Obtain a search warrant and seize the victims equipment</li> <li>• Identify the victim's configuration.</li> <li>• Acquire the evidence carefully.</li> </ul>	<b>(Each step: 1 mark, Any four steps expected)</b>
	(d)	<b>What is an application hardening? How it can be achieved?</b>	<b>4M</b>
	<b>Ans:</b>	<p><b>Application Hardening:</b> It is to secure an application against local &amp; Internet-based attacks. In this the functions or components are removed which are not needed, Restrict the access where you can and make sure the application is kept up to date with patches. It includes:</p> <p><b>1. Application Patches-</b> Application patches are supplied from the vendor who sells the application. They are probably come in three varieties: hot fixes, patches &amp; up-grades. <b>Hotfixes:</b> 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. <b>Patch:</b> This term is generally applied to more formal, larger s/w updates that may address several or many s/w problems. Patches often contain improvement or additional capabilities &amp; fixes for known bugs. <b>Upgrades:</b> Upgrades are another popular method of patching application &amp; they are likely to be received with a more positive role than patches.</p> <p><b>2. Web servers:</b> Web servers are the most common Internet server-side application in use. These are mainly designed to provide content &amp; functionality to remote users through a standard web browser.</p>	<b>(Definition: 2 marks, steps: 2 marks, Any two steps expected)</b>



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514

**3. Active directory:** Active Directory allows single login access to multiple Applications, data sources and systems and it includes advanced encryption capabilities like Kerberos and PKI.

**(B) Attempt any ONE of the following:**

**6Marks**

**(a) What is Risk? How it can be analyzed? List various assets.**

**6M**

- Ans:**
- **A computer security risk** is any event or action that could cause a loss or damage to computer hardware, software, data, or information.
  - Some breaches to computer security are accidental, but some are planned. Any illegal act involving a computer is generally referred to as a computer crime.
  - Cybercrime refers to online or Internet-based illegal acts.
  - Some of the more common computer security risks include Computer viruses, Unauthorized access and use of computer systems ,Hardware theft and software theft, Information theft and information privacy, System failure
  - When performing risk analysis it is important to weigh how much to spend protecting each asset against the cost of losing the asset.
  - It is also important to take into account the chance of each loss occurring.
  - If a hacker makes a copy of all a company's credit card numbers it does not cost them anything directly but the loss in fine and reputation can be enormous.

**(Definition: 2 marks,  
Analyzing: 2 marks,  
Assets: 2 marks)**

An **asset** is any data, device, or other component of the environment that supports information-related activities.

Assets generally include

- hardware (e.g. servers and switches),
- software (e.g. mission critical applications and support systems)
- Confidential information.

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



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514

	(b)	State the types of attacks and describe Active and Passive attack with at least one example each.	6M
	Ans:	<p><b>Passive Attack:</b> A <b>passive attack</b> monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks.</p> <p><b>Passive attacks</b> include</p> <ul style="list-style-type: none"><li>• traffic analysis,</li><li>• release of message contents</li><li>• monitoring of unprotected communications,</li><li>• decrypting weakly encrypted traffic,</li><li>• Capturing authentication information such as passwords.</li></ul> <p><b>Passive attacks</b> are in the nature of eavesdropping on, or monitoring of, transmissions.</p> <ul style="list-style-type: none"><li>• The goal of the opponent is to obtain information that is being transmitted.</li><li>• 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.</li><li>• A second type of passive attack, traffic analysis.</li><li>• 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.</li><li>• Passive attacks are very difficult to detect because they do not involve any alteration of the data.</li><li>• 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.</li><li>• 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.</li></ul> <p><b>Active Attack:</b></p> <ul style="list-style-type: none"><li>• In an <b>active attack</b>, the attacker tries to bypass or break into secured systems.</li><li>• This can be done through stealth, viruses, worms, or Trojan horses.</li><li>• Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information.</li><li>• These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user</li></ul>	(Explanation Each types: 2 marks, Example Each types:1 mark)



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

**Subject Title: Computer Security**

**Subject Code:**

**17514**

		<p>during an attempt to connect to an enclave.</p> <ul style="list-style-type: none"> <li>Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.</li> </ul> <p>Active attacks can be divided into four categories:</p> <ul style="list-style-type: none"> <li>masquerade,</li> <li>replay,</li> <li>modification of messages,</li> <li>Denial of Service(DoS)</li> </ul> <ul style="list-style-type: none"> <li>A <b>masquerade</b> takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.</li> <li>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.</li> <li>Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.</li> <li>Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning "Allow Ajay to read confidential accounts" is modified to mean "Allow Vijay to read confidential accounts."</li> </ul>	
5.		<b>Attempt any TWO of the following:</b>	<b>16Marks</b>
	(a)	<b>What is a password? Describe various policies for password selection.</b>	<b>8M</b>
	<b>Ans:</b>	<p><b>Password:</b> Password is a secret word or expression used by authorized persons to prove their right to access, information, etc.</p> <p><b>Components of good password:</b></p> <ol style="list-style-type: none"> <li>It should be at least eight characters long.</li> <li>It should include uppercase and lowercase letters, numbers, special characters or punctuation marks.</li> <li>It should not contain dictionary words.</li> <li>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.</li> <li>It should not be the same as the user's login name.</li> </ol>	<b>(Password: 4 marks, Four selection Policies: 1 marks each)</b>





6. It should not be the default passwords as supplied by the system vendor such as password, guest, and admin and so on.

**Policies for Password selection:**

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

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

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

**Proactive password checking:** The most promising approach to improved password security is a proactive password checker. In this scheme, a user is allowed to select his or her password. However, at the time of selection, the system checks to see if the password is allowable and if not, rejects it. Such checkers are based on the philosophy that with sufficient guidance from the system, users can select memorable passwords from a fairly large password space that are not likely to be guessed in a dictionary attack. The trick with a proactive password checker is to strike a balance between user acceptability and strength. If the system rejects too many passwords, users will complain that it is too hard to select a password. If the system uses some simple

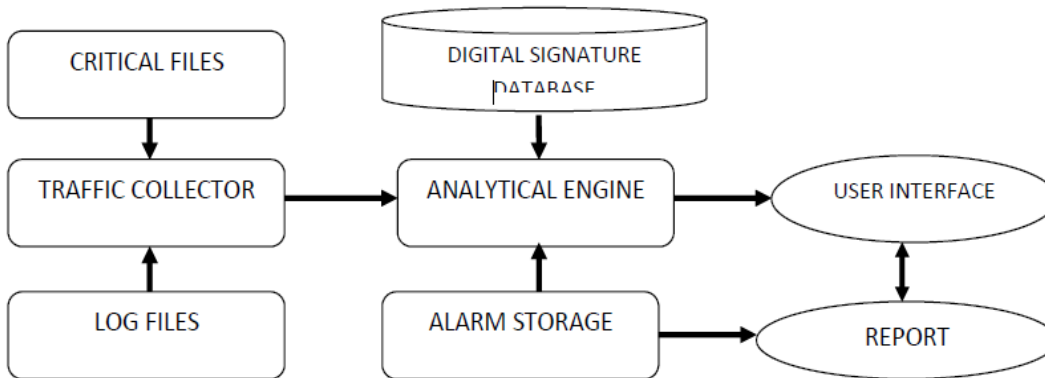


**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

**Subject Title: Computer Security**

**Subject Code:**

**17514**

		algorithm to define what is acceptable, this provides guidance to password crackers to refine their guessing technique. In the remainder of this subsection, we look at possible approaches to proactive password checking.	
	<b>(b)</b>	<b>Describe with suitable diagram Intrusion Detection System.</b>	<b>8M</b>
	<b>Ans:</b>	<p>An IDS (Intrusion detection system) is intrusion detection system is process of monitoring the events occurring in computer system or network &amp; analyzing tem for signs of possible incident which are threats of computer security. Intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways.</p>  <pre> graph LR     CF[CRITICAL FILES] --&gt; TC[TRAFFIC COLLECTOR]     LF[LOG FILES] --&gt; TC     TC --&gt; AE[ANALYTICAL ENGINE]     DS[(DIGITAL SIGNATURE DATABASE)] --&gt; AE     AE --&gt; UI([USER INTERFACE])     AS[ALARM STORAGE] --&gt; UI     UI &lt;--&gt; R([REPORT])     </pre> <p>IDS have following logical components</p> <ol style="list-style-type: none"> <li><b>1. Traffic collection:</b> 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</li> <li><b>2. Analysis Engine:</b> examines collected network traffic &amp; compares it to known patterns of suspicious or malicious activity stored in digital signature. The analysis engine act like a brain of IDS</li> <li><b>3. Signature database:</b> a collection of patterns &amp; definitions“ of known suspicious or malicious activity.</li> <li><b>4. User Interface &amp; Reporting:</b> interfaces with human element, providing alerts when suitable &amp; giving the user a means to interact with &amp; operate the IDS.</li> </ol> <p>IDS are mainly divided into two categories, depending on monitoring activity:</p> <ol style="list-style-type: none"> <li><b>1) Host-based IDS:</b> Host based IDS looks for certain activities in the log files are: <ol style="list-style-type: none"> <li>1. Logins at odd hours</li> <li>2. Login authentication failure.</li> </ol> </li> </ol>	<p><b>(IDS: 2 marks, Diagram: 2 marks, IDS components : 2 marks, Types: 2 marks)</b></p>



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.

**(c) Describe 'Kerberos' protocol with suitable diagram.**

**8M**

**Ans:**

**Kerberos:**

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

It uses secret key cryptography.

It is a solution to network security problems.

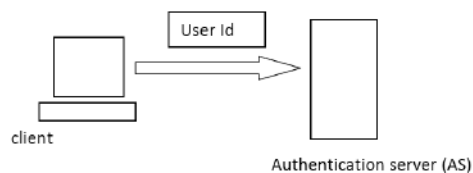
It provides tools for authentication and strong cryptography over the network to help you secure your information system

There are 4 parties involved in Kerberos protocol

- i) User
- ii) Authentication service (AS)
- iii) Ticket granting server (TGS)
- iv) Service server

**Working of Kerberos:**

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.



**(Explanation :3 marks, Diagram: 1 mark, Each step: ½ mark)**



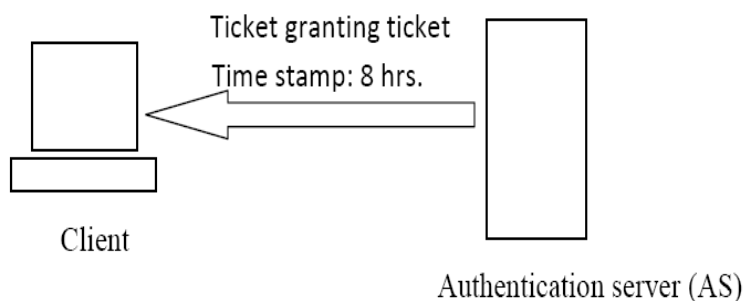
**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

**Subject Title: Computer Security**

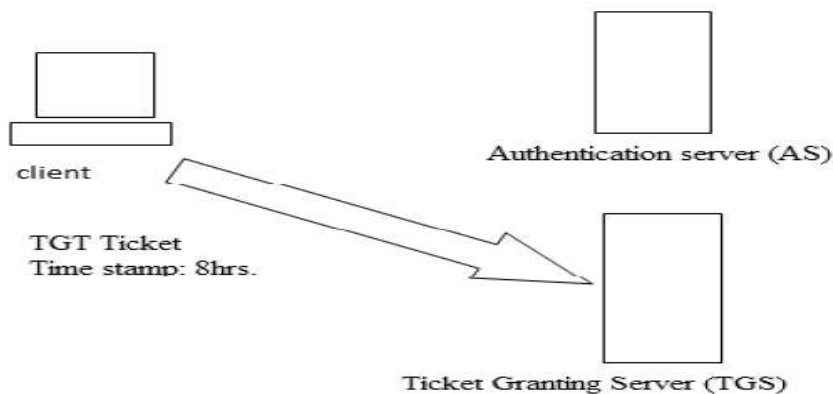
**Subject Code:**

**17514**

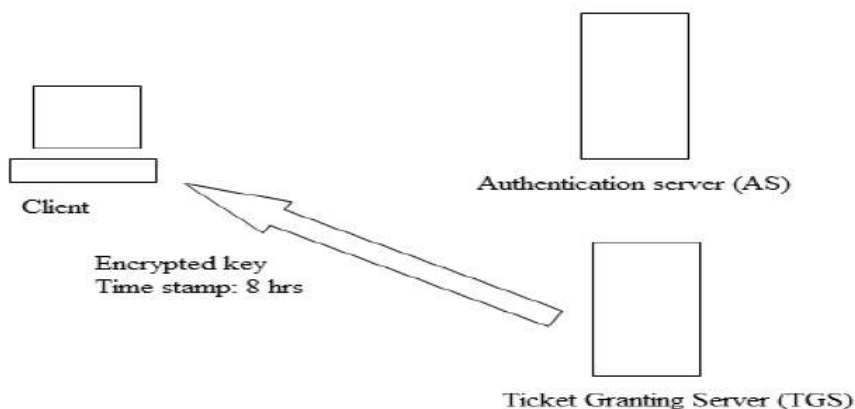
2. Upon verification, a timestamp is created. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours. The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless.
3. The key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





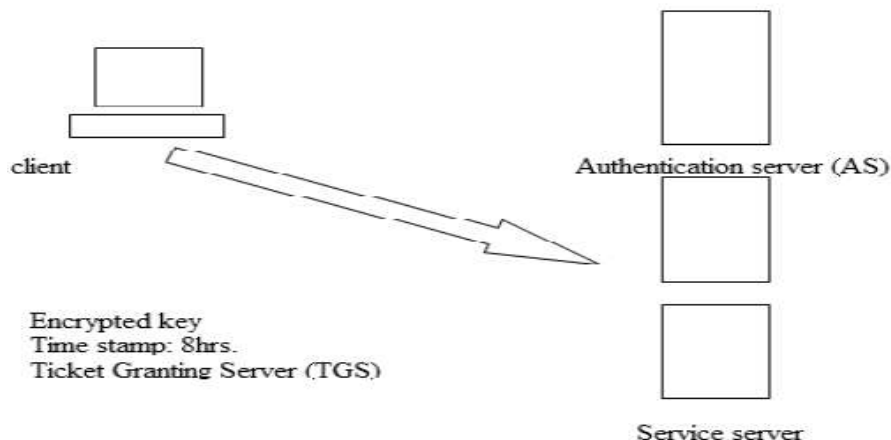
**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

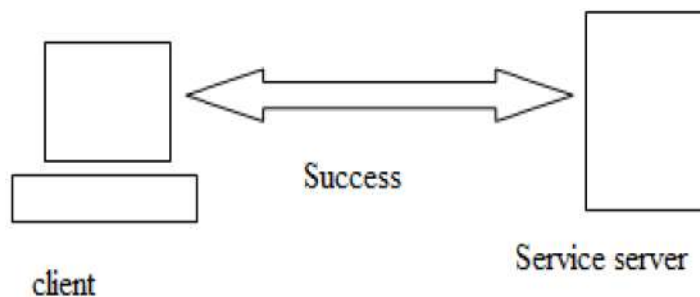
Subject Code:

17514

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 of the following:

16Marks

(a) What is piggybacking? How it can be prevented?

4M

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

**(Piggybacking: 2 marks, Prevention: 2 marks)**



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

**Subject Title: Computer Security**

**Subject Code:**

**17514**

or knowledge. It is the simple tactic of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building. An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card. Piggybacking is sometimes referred to as "Wi-Fi squatting." The usual purpose of piggybacking is simply to gain free network access rather than any malicious intent, but it can slow down data transfer for legitimate users of the network.

**Prevention:**

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

**(b) What is One Time Pad (OTP) security mechanism?**

**4M**

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

**Steps for One time pad :**

1. The key should be as long as the message
2. Key and plain text calculated modulo 26
3. There should only be 2 copies of the key (1 for sender and 1 for receiver)

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

**(Explanation : 2 marks, Example: 2 marks)**



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

Subject Title: Computer Security

Subject Code:

17514

```

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

Fig: One time pad

(c) Describe PGP with suitable diagram.

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 e-mail 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.

**(Diagram: 2 marks,  
Description: 2 marks)**

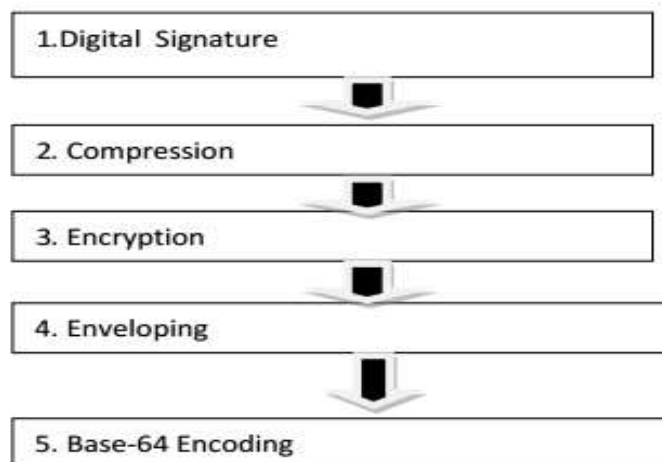


Fig. PGP

There are five steps as shown in fig.

**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



**MODEL ANSWER**  
**SUMMER- 17 EXAMINATION**

**Subject Title: Computer Security**

**Subject Code:**

**17514**

		<p>together to reduce the size of final message that will be transmitted. For this the Lempel-Ziv algorithm is used.</p> <p><b>3. Encryption:</b> 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.</p> <p><b>4. Digital enveloping:</b> 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.</p> <p><b>5. Base-64 encoding:</b> 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.</p>	
	<b>(d)</b>	<b>What is pornography?</b>	<b>4M</b>
	<b>Ans:</b>	<p><b>PORNOGRAPHY:</b> The depiction of nudity or erotic behavior, in writing, pictures, video, or otherwise, with the intent to cause sexual excitement. Is the depiction of erotic behavior (as in pictures or writing) intended to cause sexual excitement material (as books or a photograph) that depicts erotic behavior and is intended to cause sexual excitement the depiction of acts in a sensational manner so as to arouse a quick intense emotional reaction? Pornography is defined as imagery, in addition to various forms of media, that depicts actions presumed to be overtly sexual and erotic in nature. In a legal spectrum, Pornography can be defined as sexually-explicit material that is displayed or viewed with the intention of the provision of sexual gratification.</p>	<b>(Explanation : 4 marks)</b>
	<b>(e)</b>	<b>What is SSL/TLS?</b>	<b>4M</b>
	<b>Ans:</b>	<p>Transport Layer Security (TLS) and Secure Sockets Layer (SSL), both referred to as "SSL" are cryptographic protocols that provide communications security over a network. The Transport Layer security (TLS) protocol provides communications privacy over internet. The protocol allows client-server applications to communicate in a way that is designed to prevent eavesdropping, tampering or message forgery. The primary goal of the TLS protocol is to provide privacy in data integrity between two communicating applications.</p> <p><b>The protocol is composed of two layers:</b></p> <ol style="list-style-type: none"><li>1. TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption.</li><li>2. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.</li></ol>	<b>(Explanation : 4 marks)</b>