MODEL ANSWER

WINTER - 2017 EXAMINATION

Subject: Information Security **Subject Code:** **17518**

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)** **(a)** **Ans.**	**Attempt any THREE:** **What is Information Security? Explain three pillars of information security.** **Information Security**: Information security is the method which makes the accessibility of information or system more reliable. Security means to protect information or system from unauthorized user like attackers, who do harm to system or to network intentionally or unintentionally. Security is not only to protect information or network, but also allow authorized user to access the system or network. Three pillars of information security: 1.Confidentiality 2.Integrity 3.Availability	**3 x 4=12** **4M** ***1M for information security, 1M each for three pillars***

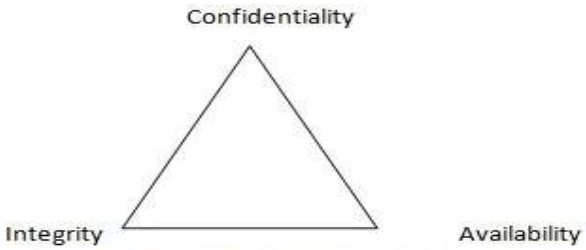


Fig: Three pillars of Information Security

1. Confidentiality: It is used as an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many ways such as through the intentional release of private company information or through a misapplication of networks right.

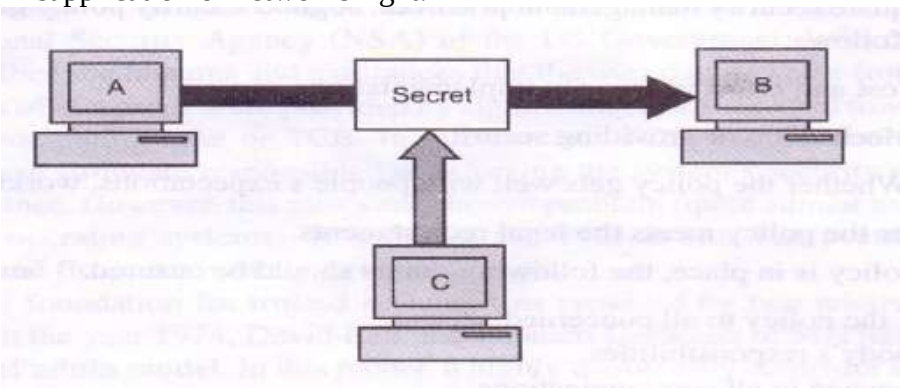


Fig: Loss of Confidentiality

2. Integrity: The concept of integrity ensures that i. Modifications are not made to data by unauthorized person or processes. ii. Unauthorized modifications are not made to the data by authorized person or processes. iii. The data is internally and externally consistent.

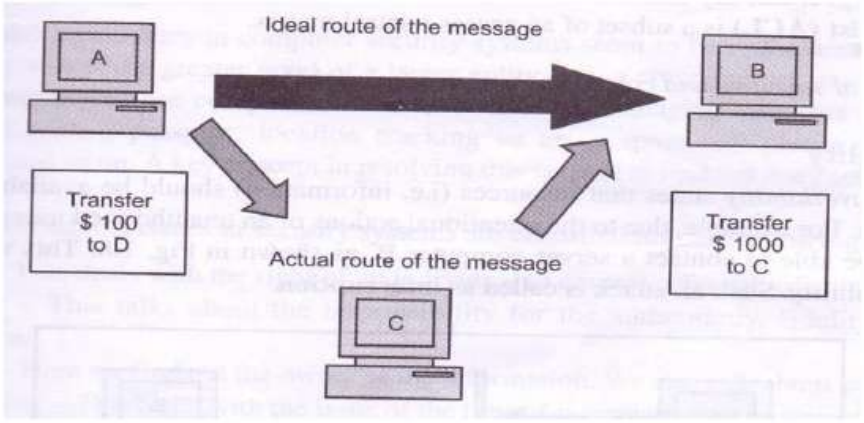


Fig: Loss of Integrity

3. Availability: The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate person. Availability guarantees that the systems are up and running when they are needed. In addition, this concept guarantees that the security services needed by the security practitioner are in working order.

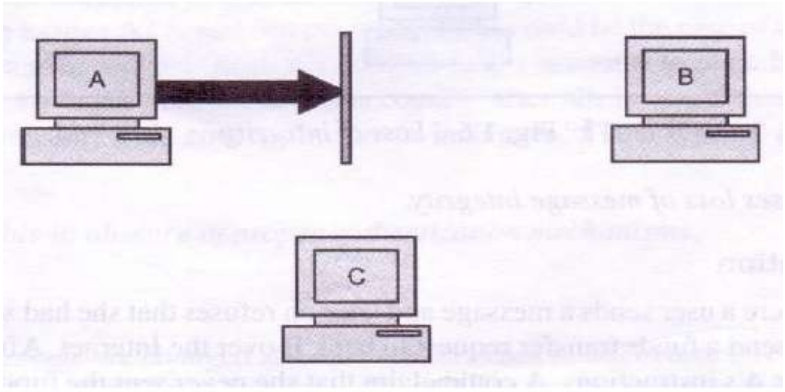


Fig: Attack on availability

	(B) Ans.	**Define Risk. Describe qualitative and quantitative risk analysis.** **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) The adverse impacts that would arise if the circumstance or event occurs; and (ii) The likelihood of occurrence. **Quantitative Risk Analysis:** A Process of assigning a numeric value	**4M** ***Risk 1M***

		to the probability of loss based on known risks, on financial values of the assets and on probability of threats. It is used to determine potential direct and indirect costs to the company based on values assigned to company assets and their exposure to risk. Assets can be rated as the cost of replacing an asset, the cost of lost productivity, or the cost of diminished brand reputation. In this 100% quantitative risk analysis is not possible. **Qualitative Risk Analysis:** A collaborative process of assigning relative values to assets, assessing their risk exposure and estimating the cost of controlling the risk. It utilizes relative measures and approximate costs rather than precise valuation and cost determination. Assets can be rated based on criticality - very important, important, not-important etc. Vulnerabilities can be rated based on how it is fixed - fixed soon, should be fixed, fix if suitable etc. Threats can be rated based on scale of likely - likely, unlikely, very likely etc In this 100% qualitative risk analysis is feasible.	***Description of analysis $1^{1/2}$M each***
	(c) **Ans.**	**Define following terms:** **(i) Plain Text** **(ii) Cipher Text** **(iii) Encryption** **(iv) Decryption** **(i) Plain Text:** Plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to the message. **(ii) Cipher Text:** The resultant message after coding a plain text by using some suitable method is known as Cipher Text. **(iii) Encryption:** The process of encoding plain text into cipher text message is known as Encryption. **(iv) Decryption:** The process of transforming cipher text message into plain text or original text is known as Decryption.	**4M** ***Each Definition 1M***
	(d) **Ans.**	**State different causes of data recovery. Describe any one data recovery tool.** ***(Note: Any other tool shall be considered)*** Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible for some reason.	**4M**

		When files have been mistakenly deleted and need to be recovered, data recovery is necessary. This is the act of retrieving deleted or erased files using one of several methods. Data can be lost because of reasons: • Accident deletion of files Due to disk malfunction or failure • Due to accidentally formatting the storage device • Due to problem with system and/or application software • Due to physical damage to the storage device **Data recovery tools:** 1. NTFS Data recovery tools 2. FAT data recovery tool 3. Digital Camera Data recovery tool 4. Removable media data recovery tool 5. Recovery of deleted files 6. Recovery of formatted partition **1. NTFS Data Recovery Tools:** NTFS Recovery is a fully automatic utility that recovers data from damaged or formatted disks. It is designed with a home user in mind. You don't need to have any special knowledge in disk recovery. *Example*: - Diskinternal's NTFS Data Recovery tool. The tool supports • A disk volume containing valuable info was damaged due to a system malfunction. • A disk volume was damaged due by a dangerous virus. • Windows cannot access a disk drive. • Disk was damaged • You have mistakenly formatted a disk volume • Files or folders are not readable • Corrupt or damaged partition table **2. FAT Data Recovery Tools:** FAT Recovery is a fully automatic utility that recovers data from damaged or formatted disks. The program scans the disk first and then restores the original structure of files and folders. *Example:* - Diskinternal's FAT Data Recovery tool. Works for all:	***Causes 1M*** ***Any one data recovery tool 3M***

		• Formatted drive (to NTFS, to/from FAT32/FAT16) • Inaccessible drive • Drive not booting • Missing or deleted file or directory • Corrupt or damaged partition table. • Damaged Dynamic Disks FAT Recovery is fully wizard-based, meaning there is no technical knowledge needed. Any person can recover data from damaged or formatted disks on their own, without hiring a technician. FAT Recovery does not write anything to the damaged disk, therefore you can try the program without any risk of losing data you want to be recovered. It does not matter whether Windows recognizes a disk or not, nor does it matter if all directory information is missing – all recoverable data will be recovered and the original disk structure will be restored. Because the program scans every single sector, it never misses recoverable data. Another important advantage of FAT Recovery is its capability to recover data from virtual disks, and it does not matter if the data was deleted prior to recovery or not. FAT Recovery supports the following file systems - FAT12, FAT16, FAT32, and VFAT. Files up to 64 KB are recovered by FAT Recovery. **3. Digital Camera Data recovery tool:** Digital camera data recovery has the leading photo recovery software for memory card used by digital camera or phone. It can effectively recover lost, deleted, corrupted or formatted photos and video files from various memory cards. It supports almost all memory card types including SD Card, MicroSD, SDHC, CF (Compact Flash) Card, xD Picture Card, Memory Stick and more. *Example:* - Diskinternal's Digital Camera Data Recovery tool. Features : • Recover deleted photos from memory cards • Recover lost photos from memory cards • Recover lost movies from memory cards • Recover photos from formatted memory cards • Recover photos from damaged, unreadable or defective memory cards • Recover pictures from removable storage including flash drives	

		• Recover images, video files from mobile phones **4. Removable media data recovery tool:** The process of recovery is a very straightforward one - insert disk, press "Recover" and get the files you need. The software is easy to use and does not require any additional skills. We tried to make working with it as comfortable as possible. The program starts working automatically and doesn't require the additional set up change. Comfortable Recovery Wizard will do everything for you. The result of the Wizard work is the list of all the recoverable files. All you have to do is to choose the necessary files and press a Recover button. The innovational scanning technology economizes greatly your time that otherwise would be spent on a damaged disc recovery. The advanced users can use a manual recovering. In this case you can work individually with each session\track and chose the file system depending on session. *Example:-* • Card Recovery • PhotoRec • Recover My Files • Recuva	
1.	**(B)** **(a)** **Ans.**	**Attempt any ONE:** **What is information classification? Describe criteria for information classification.** **Information classification:** Classification of information is used to prevent the unauthorized disclosure and the resultant failure of confidentiality. Terms for information classification: 1. **Unclassified**: Information that is neither sensitive nor classified. The public release of this information does not violet confidentiality. 2. **Sensitive but Unclassified (SBU):** Information that has been designated as a minor secret but may not create serious damage if disclosed. 3. **Confidential**: The unauthorized disclosure of confidential information could cause some damage to the country‘s national security. 4. **Secret**: The unauthorized disclosure of this information could cause serious damage to the countries national security. 5. **Top secret**: This is the highest level of information classification. Any unauthorized disclosure of top secret information will cause	**1 x 6=6** **6M** ***Classification 2M***

		grave damage to the country's national security. **Criteria for information Classification:** 1. **Value:** It is the most commonly used criteria for classifying data in private sector. If the information is valuable to an organization it needs to be classified. 2**. Age:** The classification of the information may be lowered if the information value decreases over the time. 3. **Useful Life:** If the information has been made available to new information, important changes to the information can be often considered. 4**. Personal association:** If the information is personally associated with specific individual or is addressed by a privacy law then it may need to be classified.	***Criteria 4M***
	(b) **Ans.**	**Explain play fair cipher with an example.** ***(Note: Any other correct example may also be considered).*** The Playfair cipher or Playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher. It uses group of two letters to generate cipher text. The encryption process is divided into 3parts. **a) Preparing plain text:** 1. To prepare plain text write all letters of plain text in lowercase, in pairs without punctuation. 2. In plain text if j is present, all j's are replaced with i's. 3. In plain text if double letters occur in a pair, divide them by X or a Z. For e.g. 'full' in a plain text becomes 'fulxl'. 4. If there are an odd number of letters in plain text, an extra letter is chosen and it is added at the end. **b) Preparing a key matrix:** 1. A key matrix is a five-by-five matrix of letters constructed using a keyword. 2. The key phrase is first written without repeating any letters. The remaining letters of the alphabet are filled in the alphabetic order. **c) Encryption process:** The plain text is encrypted two letters at a time using the following steps: 1. Each letter in a pair that is on the same row is replaced by the letter to the right.	**6M** ***Explanation 3M***

2. Letters in the same column are replaced by the next letter below in the same column.
3. When the letters are neither in the same row nor in the same column, then the substitution based upon their intersection. Start with the first letter and move across until it is lined up with the second letter. Then start with the second, and move up or down until it is lined up with the first. Perform the transformation for each pair of letters in the modified plain text and remove the spaces.

Example:

Plaintext: We live in a world full of beauty.

Keyword: Another

Step 1: Preparing plain text

The plain text matrix is:

we	li	ve	in	aw
or	ld	fu	lx	lo
fb	ea	ut	yz	

Step 2: Preparing key matrix

The key matrix is:

A	N	O	T	H
E	R	B	C	D
F	G	I/J	K	L
M	P	Q	S	U
V	W	X	Y	Z

Step 3: Encryption

By following the above rules for encryption of plain text the cipher text is:

VRFKAFGONVNBULLMIZIHIEFESHZY

Example 3M

2. **Attempt any TWO:** **2 x 8=16**

(a) Ans. **Explain confidentiality and integrity model with an example.** **8M**

Bell-La Padula (BLP) model for confidentiality:

- It is used to describe what actions must be taken to ensure the confidentiality of information.
- It can specify how security tools are used to achieve the desired level of confidentiality.
- It is a classic mandatory access-control model for protecting

Confidentiality model 4M

		confidentiality. • It is derived from the military multilevel security paradigm, which has been traditionally used in military organizations for document classification and personnel clearance. **Working:** The BLP model has a strict, linear ordering on the security of levels of documents, so that each document has a specific security level in this ordering and each user is assigned a strict level of access that allows them to view all documents with the corresponding level of security or below. BLP security rules prevent information from being moved from a level of higher security to a lower level. Each object, x, is assigned to a security level, L(x). Similarly, each user, u, is assigned to a security level, L(u). Access modes can be of two types: Simple security and * Star property. **Simple security property:** A user u can read an object x only if L(x) <L(u). It is also called the 'no read up' rule, as it prevents users from viewing objects with security levels higher than their own. *** (star) Property** : A user u can write (create, edit, or append to) an object x only if L(u) < L(x). It is also called the 'no write down' rule. It is meant to prevent propagation of information to users with a lower security level. In short, subjects (users) can read down and objects can write or append up. Thus this principle follows "no read up, no write down". **BIBA model of integrity:** • Integrity is the protection of system data from intentional or accidental unauthorized changes. • Biba Model is based on the principle that higher levels of integrity are more worthy of trust than the lower ones. • Although the security program cannot improve the accuracy of data, it can help to ensure that any changes are intended and correctly applied. • Additional element of integrity is the need to protect the process and program used to manipulate the data from unauthorized modification. The BIBA model assigns integrity levels to subjects and objects using two properties:	***Integrity Model 4M***

		1. Simple Integrity (read) Property: - Data can be read from higher integrity level. Thus a subject has read access to an object only if the subject's security level is lower than or equal to the level of an object. 2. Star (*) Integrity property: - Data can be written to lower integrity level. This permits a subject to have write access to an object only if the subject's security level is equal to or higher than that of object. Thus Biba model ensures that no information from subject can be passed on to an object in a higher security level. This prevents modification of data of higher integrity with data of lower integrity. BIBA is the opposite of BLP, "no write up, no read down" principle.	
	(b) **Ans.**	**Explain following:** **(i) Row Transposition Cipher with example.** **(ii) Digital signature.** ***(Note: keyword with/without alphabetical order shall be considered in the example)*** **(i) Row Transposition Cipher with example:** Transposition technique replaces one alphabet with another and also performs some permutation over the plain text alphabet. Algorithm Steps:- 1. Write the plain text message row by row in a rectangle of a predefined size (keyword size) 2. Read the message column by column, however, it need not be in the order of columns, it can be any random order. 3. The message thus obtained is the cipher text message. *Example:* Plain Text: "Come Home Tomorrow" Keyword: ZEBRAS Consider a rectangle with six column and. Therefore, when the message is written in the rectangle row by row it will look as follow	**8M** ***Row Transposition explanation 2M*** ***Example 2M***

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
C	O	M	E	H	O
M	E	T	O	M	O
R	R	O	W		

Now, decide the order of columns as some random order, say, 4, 6, 1, 2, 5, 3
Then read the text in the order of these columns.

The cipher text obtained from it would be: EOW OO CMR OER HM MTO While Decryption phase the cipher is written back in same rectangle with same size and all ciphers are placed as per the key.

(iii) Digital signature:

1. Digital signature is a strong method of authentication in an electronic form.
2. It includes message authentication code (MAC), hash value of a message and digital pen pad devices. It also includes cryptographically based signature protocols.
3. Digital Signature is used for authentication of the message and the sender to verify the integrity of the message.
4. Digital Signature may be in the form of text, symbol, image or audio.
5. In today's world of electronic transaction, digital signature plays a major role in authentication. For example, one can fill his income tax return online using his digital signature, which avoids the use of paper and makes the process faster.
6. Asymmetric key encryption techniques and public key infrastructure are used in digital signature.
7. Digital signature algorithms are divided into two parts:
   a. Signing part: It allows the sender to create his digital signature.
   b. Verification part: It is used by the receiver for verifying the signature after receiving the message.

Digital Signature explanation 2M

Generation and Verification of digital signatures:

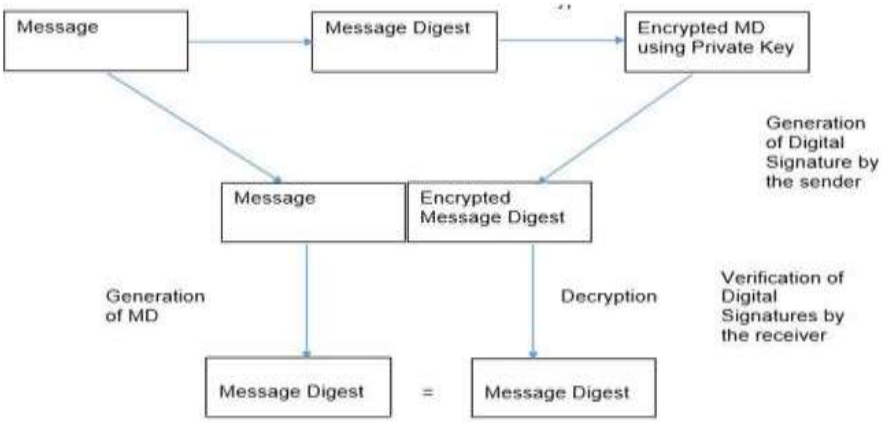
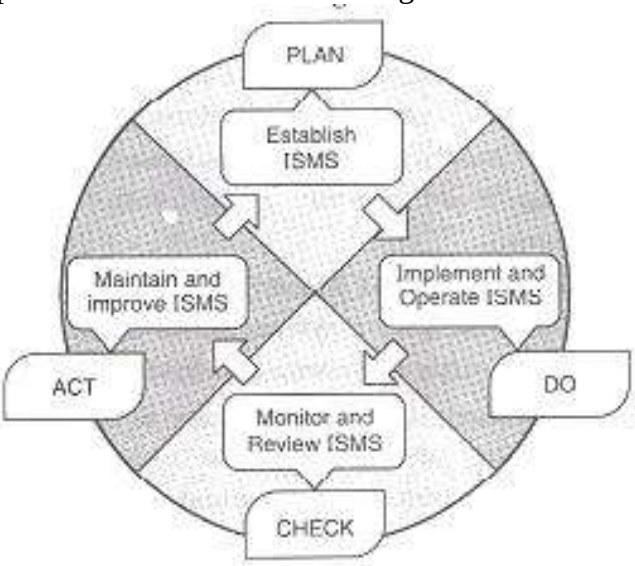


Diagram 2M

	(c) Ans.	**Describe ISO 27001 and ISO 20000.** **ISO 27001:** The international organization for standard (ISO) is established in year 1997. It is nongovernmental international body that collaborates with the International Electro technical commission (IEC) and the International Telecommunication Union (ITU) on information and communication technology (ICT) standards. ISO 27001 describes following processes: • Definition of Information Security Policy • Definition of Scope of ISMS • Security Risk Assessment • Manage the identified risk • Select controls for implementation • Prepare SoA (Statement of Applicability) ISO 27 001 uses PDCA (Plan-Do-Check-Act) approach and this is used to improve the effectiveness of an organization:  **Plan:** This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls. **Do:** This phase includes carrying out everything that was planned during the previous phase. **Check:** The purpose of this phase is to monitor the functioning of the ISMS through various channels‖, and check whether the results meet	**8M** ***Each explanation 4M***

		the set objectives. **Act:** The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase. ISO 27001 allows selection of objectives and controls of security which shows the unique security risks and requirements. This information is used to prepare SoA and then SoA is used to prepare Risk Treatment Plan. **ISO 20000:** • ISO 20000 is an industry standard like ISO 9000/9001, and like ISO 9000/9001, ISO 20000 offers organizational certification. • ISO 20000 standards show IT how to manage improve IT while establishing audit criteria. It also provides auditors with a documented standard to use for measuring IT compliance. • The ITIL offers certifications for individuals but ISO 20000 is an organizational certification with international recognition. • ISO 20000 Was basically developed to use best practice guidance provided in ITIL framework. This standard was developed/ published in December 2005. • ISO 20000 have two specifications. ➢ **ISO 20000-1**. is the specification for Service Management. It defines the processes and provides assessment criteria and recommendations for those who are responsible for IT Service Management. Organizational certification uses this section. It includes following sections: • Scope • Terms and Definitions • Requirements for a Management System • Planning and Implementing Service Management • Planning and Implementing New or Changed Services • The Service Delivery Process • Relationship Processes • Resolution Processes • Release Process • Control Processes ➢ ISO 20000-2 documents a code of practice that explains how to manage IT with regard to ISO 20000-1 audits. It includes all the	

		sections from part 1 except requirements for a management system. Both ISO 20000-1 and ISO 20000-2 derive directly from the ITIL best practice. • Already, several governments have stated that ISO 20000 is a requirement for outsourced IT services. As the industry recognizes the value of ISO 20000, more and more companies will require their partners and vendors to reach ISO 20000 certification. • ISO 20000 also includes more than Service Delivery and Service Support. It includes sections on managing suppliers and the business; as Well as Security Management. • ISO 20000 can assist the organization in benchmarking its IT service management, improving its services, demonstrating an ability to meet customer requirements and create a framework for an independent assessment. • Some of the most common benefits of ISO 20000 certification for service providers are as follows: (1) It offers competitive differentiation by demonstrating reliability and high quality of service. (2) It gives access to key markets, as many organizations in the public sector mandate that their IT service providers demonstrate compliance with ISO/IEC 20000.	
3.	**(a) Ans.**	**Attempt any FOUR:** **Describe data obfuscation with an example.** **Data obfuscation:** • Data obfuscation involves protection of sensitive information with technique other than encryption. • Data obfuscation is one of the solutions for data theft. Obfuscate means to make the data unclear. • It is an effective method which involves chopping the text into segments and re-arranging it. • Sometimes data is obfuscated by using a simple substitution cipher. ***Example:*** A good example of data obfuscation would be an audit report on a medical system. In this report only required field of patients are disclosed to the auditor. Details which are not required such as patient's contact number and address are made obfuscate.	**4 x 4=16** **4M** ***Relevant Explanation 2M*** ***Example 2M***

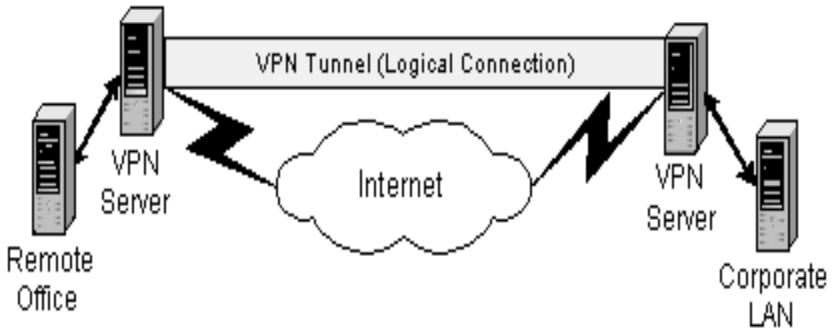
	(b) Ans.	**Explain Information Security policy framework with diagram.**  **Fig: Information Security Policy framework** **a) Security policy:** Information security policy consists of higher level statements related to the protection of information across the business by senior management. Businesses may have a single encompassing policy or several specific policies that target different areas like 1. Senior Management Statement of Policy 2. Regulatory Policy 3. Advisory Policy 4. Informative Policy **b) Standards:** Standard consists of specific low level mandatory controls that help to enforce and support the information security policy. Standard helps to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or software. For example, a password standard may set out rules for password complexity and a Windows standard may set out the rules for hardening Windows clients. **c) Guidelines:** 1. It should consist of recommended, non-mandatory controls that help to support standards or serve as a reference when no applicable standard is in place. 2. It should be viewed as best practices that neither are nor usually	**4M** ***Diagram 2M*** ***Explanation 2M***

		requirements, but are strongly recommended. 3. It can be consisting of additional recommended controls that support a standard or help to fill in the gaps where no specific standard applies. 4. A standard may require specific technical controls for accessing the internet securely and separate guidelines may be outline the best practices for using it. **d) Procedures:** Procedures are the detailed, step by step activities that are followed to implement a process or configure system for compliance to a guideline. They may also be step by step security processes, which assure repeatability and accountability of personnel performing the procedure.	
	(c) Ans.	**Explain Ceasor cipher with an example.** **Caesar cipher:** It is proposed by Julius Caesar. In cryptography Caesar cipher also known as Caesar cipher/code, shift cipher/code. It is one of the simplest and most widely known encryption techniques. It is a type of substitution technique in which each letter in the plain text is replaced by a letter some fixed number of position down the alphabet. ***For example,*** with a shift of 3, A would be replaced by D, B would became E, and so on as shown in the table below. Using this scheme, the **plain text "INFORMATION"** encrypts as **Cipher text "LQIRUPDWLRQ".** To allow someone to read the cipher text, you tell them that the **key is 3**	**4M** ***Explanation 2M*** ***Example 2M***

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

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

		Algorithm to break Caesar cipher: 1. Read each alphabet in the cipher text message, and search for it in the second row of the table above. 2. When a match in found, replace that alphabet in the cipher text message with the corresponding alphabet in the same column but the first row of the table. (For example, if the alphabet cipher text is J, replace it with G). 3. Repeat the process for all alphabets in the cipher text message.	
	(d) Ans.	**Describe cyber crime investigation.** **Cyber crime investigation process**: The computer crime investigation should start immediately following the report of any alleged criminal activity. Many processes ranging from reporting and containment to analysis and eradication should be accomplished as soon as possible after the attack. An incident response plan should be formulated, and a Computer Emergency Response Team (CERT) should be organized before the attack. The incident response plan will help set the objective of the investigation and will identify each of the steps in the investigative process. **Detection and Containment** Before any investigation can take place, the system intrusion or abusive conduct must first be detected. **Report to Management** All incidents should be reported to management as soon as possible. Prompt internal reporting is imperative to collect and preserve potential evidence. It is important that information about the investigation be limited to as few people as possible.. **Determine if Disclosure is Required** Determine if a disclosure is required or warranted due to laws or regulations. **Investigation Considerations** Once the preliminary investigation is complete and the victim organization has made a decision related to disclosure, the organization must decide on the next course of action. **Obtaining and Serving Search Warrants** If it is believed that the suspect has crucial evidence at his or her home or office, a search warrant will be required to seize the evidence.	**4M** ***Any relevant description 4M***

		Surveillance Two forms of surveillance are used in computer crime investigations: physical and computer. **Physical surveillance** can be generated at the time of the abuse, through CCTV security cameras, or after the fact. **Computer surveillance** is achieved in a number of ways. It is done passively through audit logs or actively by way of electronic monitoring. The goal of the investigation is to identify all available facts related to the case. The investigative report should provide a detailed account of the incident, highlighting any discrepancies in witness statements. The report should be a well-organized document that contains a description of the incident.	
	(e) Ans.	**Describe VPN (Virtual Private Network) with a neat diagram.** A VPN or Virtual Private Network is a network connection that enables you to create a secure connection over the public Internet to private networks at a remote location. With a VPN, all network traffic (data, voice, and video) goes through a secure virtual tunnel between the host device (client) and the VPN provider's servers, and is encrypted. VPN technology uses a combination of features such as encryption, tunneling protocols, data encapsulation, and certified connections to provide you with a secure connection to private networks and to protect your identity.VPN connections technically give you all the benefits of a Local Area Network (LAN), which is similar to that found in many offices but without requiring a hard-wired connection. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.  **OR**	**4M** ***Explanation 2M*** ***Diagram 2M***

VPN architecture and working:

VPN is a mechanism of employing encryption, authentication and integrity protection so that we can use a public network (the Internet) as Information Technology it is a private network.

VPN offers high amount of security and yet does not require any special cabling on behalf of the organization that wants to use it. Thus VPN combines the advantages of public network (cheap and easily available) with those of a private network (secure and reliable).

Working:

Suppose an organization has two networks, Network 1 and Network 2 which are physically apart from each other and we want to connect them using the VPN approach. In such case we set up two firewalls, Firewall1 and Firewall2.

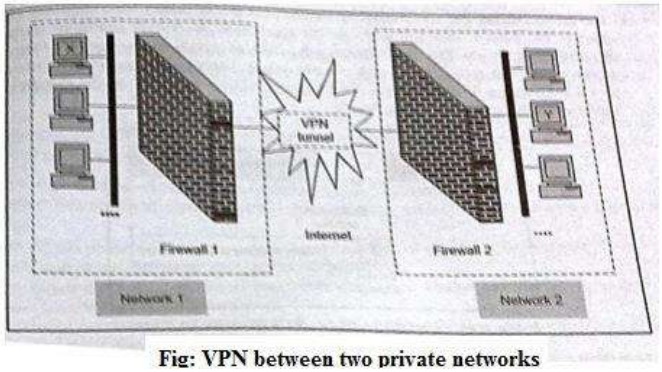
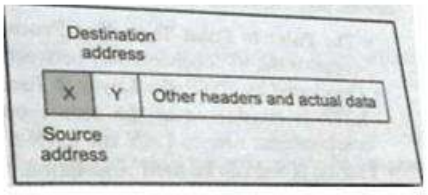


Fig: VPN between two private networks

Assume that host X on Network 1 wants to send a data packet to host Y on Network 2. This transmission would work as follows:

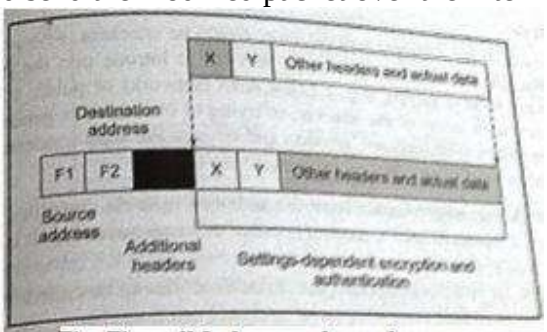
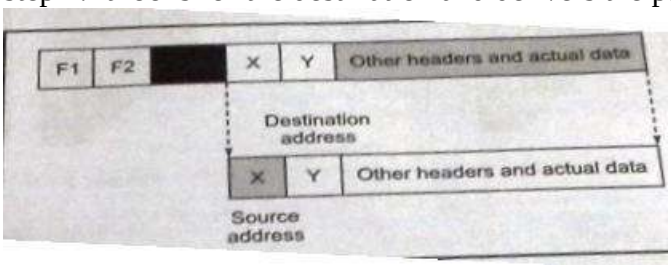
Host X creates the packet, inserts its own IP address as the source address and the IP address of host Y as the destination address.

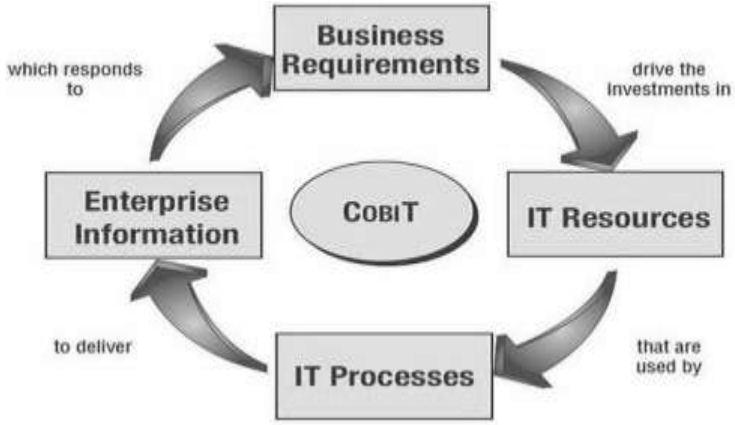
Step 1: Original Packet

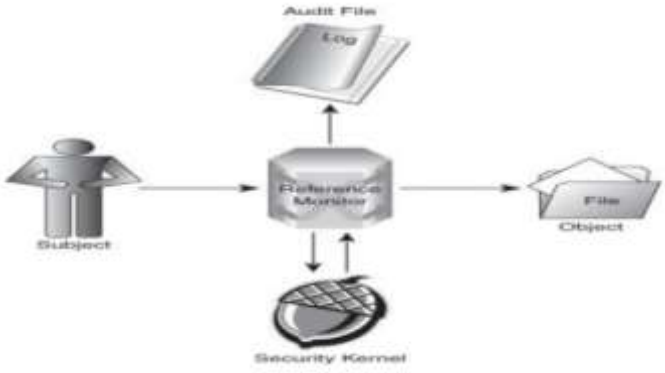


Step 2: Firewall 1 changes the packet contents

The packet reaches Firewall 1. Firewall1 adds new headers to the packet. In these new headers it changes the source IP address of the packet from that of host X to its own address (i.e. the IP address of

		Firewall1 say F1). It also changes the destination IP address of the packet from that of host Y to the IP address of Firewall say F2). It also performs the packet encryption and authentication depending on the settings and send the modified packet over the Internet.  **Fig: Firewall 1 changes the packet contents** **Step 3: Firewall 2 retrieves the original packet contents.** The packet reaches Firewall2 over the Internet via one or more routers. Firewall2 discards the outer header and performs the appropriate decryption and other cryptographic functions as necessary. This yields the original packet as was created by host X in step 1. It looks for the destination and delivers the packet to host Y.  Thus the data/information from X to Y is transferred via public (internet) network through secure tunnel/protocol. The three main VPN protocols which can be used are, PPTP (Point to Point Tunneling Protocol, L2TP (Layer 2 Tunneling Protocol and IPSEC.	
4.	**(A)** **(a)** **Ans.**	**Attempt any THREE:** **Explain COBIT framework.** The Control Objectives for Information and related Technology (COBIT) is ―a control framework that links IT initiatives to business requirements, organizes IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and	**3 x 4=12** **4M**

		defines the management control objectives to be considered. The IT GOVERNANCE INSTITUTE (ITGI) first released it in 1995, and the latest update is version 4.1, published in 2007. COBIT 4.1 consists of 7 sections, which are 1) Executive overview, 2) COBIT framework, 3) Plan and Organize, 4) Acquire and Implement, 5) Deliver and Support, 6) Monitor and Evaluate, and 7) Appendices, including a glossary. Its core content can be divided according to the 34 IT processes. COBIT is increasingly accepted internationally as a set of guidance materials for IT governance that allows managers to bridge the gap between control requirements, technical issues and business risks. Based on COBIT 4.1, the COBIT Security Baseline focuses on the specific risks around IT security in a way that is simple to follow and implement for small and large organizations. COBIT can be found at ITGI or the Information Systems Audit and Control Association (ISACA) websites.  **Services provided by the COBIT:** 1. Manage operations 2. Manage service request and incidence 3. Manage problems 4. Manage continuity	***Explanation 2M*** ***Diagram 2M***

		5. Manage security services 6. Manage business process control	
	(b) **Ans.**	**Explain trusted computing base with respect to Information Security.**  **Fig: Trusted Computing Base** The trusted computing base (TCB) is the sum total of all software and hardware required to enforce security • Typically, all of hardware, the core OS that is involved in protection, and all programs that operate with system privileges • Desirable properties: – Small – Separable, well-defined – Independently-auditable Reference Monitor • A reference monitor is a separable module that enforces access control decisions • All sensitive operations are routed through the reference monitor • The monitor then decides if the operation should proceed It stand s between Subjects and Objects and its role is to verify the subject, meets the minimum requirements for an access to an object as shown in figure. **The reference monitor has three properties:** 1. Can not be bypassed and controls all access. 2. Can not be altered and is protected from modification or change. 3. Can be verified and tested to be correct. In Unix/Linux security kernel acts as a Reference Monitor which will handle all user application requests for access to system resources.	**4M** ***Explanation 4M***

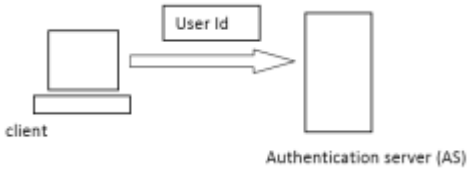
		In trusted system Object is something that people want to access. These objects (data) are labeled according to their level of sensitivity. Subjects (users) should have same level of classification while accessing object.	
	(c)	**State the meaning of following terms:** **(i) Spam (ii) Hacking** **(iii) Cracking (iv) Spying**	**4M**
	Ans.	**(i) Spam:** It is an irrelevant or unsolicited messages (or email) sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc. **(ii) Hacking:** Every act committed towards breaking into a computer and/or network is hacking and it is an offence. Hackers write or use readymade computer programs to attack the target computer. They possess the desire to destruct and they get enjoyment out of such destruction. Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are hot on hacker's target listsand attacks on government websites receive wide press coverage. **(iii) Cracking:** A cracker is someone who breaks into someone else computer system, often on a network by passing passwords or licenses in computer programs or in other ways intentionally breaches computer security. A cracker can be doing this for Profit maliciously, for some selfless purpose or cause, or because the challenge is there. **(iv) Spying:** This is an activity to monitor or keep an eye on the computer system or application or website (using cookies) and gather information about the user. Credit Card copying (Skimming) is another cyber crime that comes under spying as well as fraud. As a person swipes his card at the ATM, or presents his card at a restaurant or shop for billing, the swipe machine may have a skimmer attached to it which transfers confidential information to the card to a third party, other than the credit card company.	***Each term 1M***
	(d)	**Explain Kerberos process with a neat diagram.**	**4M**
	Ans.	1. Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by	

using secret-key cryptography.
2. It is a solution to network security problems.
3. It provides tools for authentication and strong cryptography over the network to help you secure your information system
4. There are 4 parties involved in Kerberos protocol
   i. User
   ii. Authentication service (AS)
   iii. Ticket granting server (TGS)
   iv. Service server

Correct steps 2M, Diagram 2M

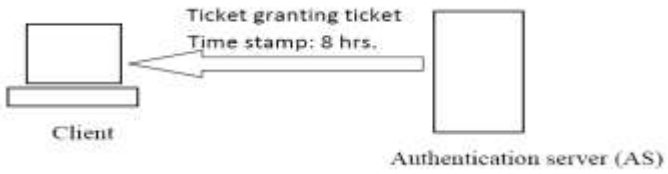
Working of Kerberos:

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

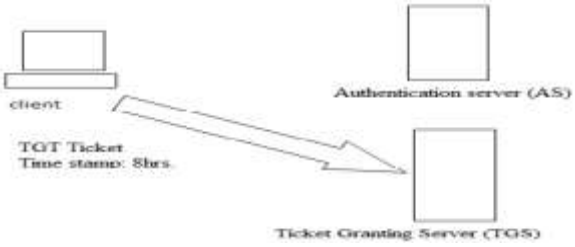


2. Upon verification, a timestamp is created. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours. The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless.

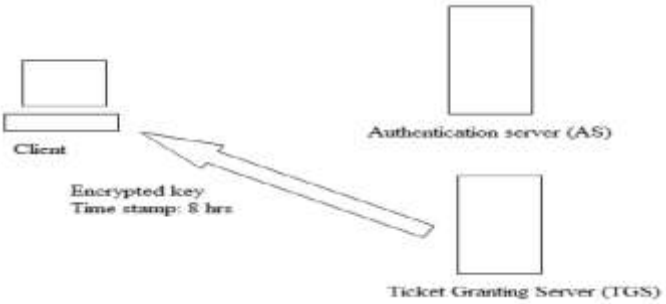
3. The key is sent back to the client in the form of a ticket-granting ticket, or TGT. This is a simple ticket that is issued by the authentication service (AS). It is used for authentication the client for future reference.



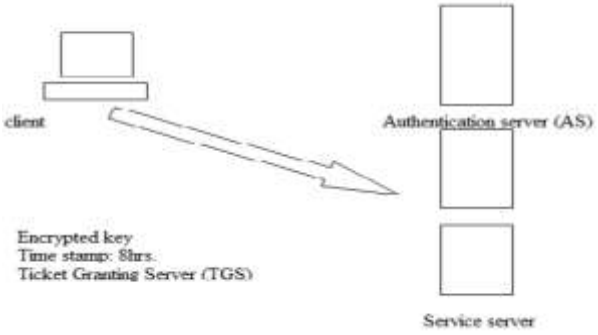
4. The client submits the ticket-granting ticket to the ticket-granting server, or TGS, to get authenticated.



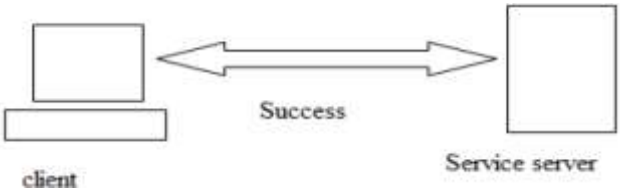
5. The TGS creates an encrypted key with a timestamp, and grants the client a service ticket.



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



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.	
4.	**(B)** **(a)** **Ans.**	**Attempt any ONE:** **Describe six types of protection mechanism in trusted computing base.** **Types of Protection Mechanisms in a Trusted Computing base is as follows:** **1. Process Isolation:** Each process has its own address space to store data and code of application. We can prevent other processes from accessing the other process's data. It will prevent data leakage as well as modification in the memory. 2. **Principle of least privilege:** For allowing normal functioning it will limit the access to minimum level. This will prevent data exploitation. 3. **Hardware Segmentation:** It is the process of dividing memory into multiple segments or sections. For every process, Kernel allocates some memory to store its process data, application code, and application data. It will prevent the user processes from accessing other process's memory. 4. **Layering:** Dividing process of operation into number of layers to perform various functions is called as Layering. a. Each layer is responsible for particular type of actions. b. Lower layers will perform all basic functions while higher layers will perform more complex and protected functions 5. **Abstraction:** By ignoring implementation details it will provide security. It will define particular set of permissible values as well as operations for an object. 6. **Data / Information hiding :** It is the process of assuring that	**1 x 6=6** **6M** ***Description of any six protection mechanisms 1M Each***

		when data or information at one level is available at another level (Higher or Lower), then it cannot be available to another level (Higher or Lower) 7. **Information Storage:** It is the process of retaining the physical state of information for specific interval time, for example at the time of poor fluctuation. **8. Closed and open System:** In closed system very less interfaces are available that can connect to other systems. Users have limited access to application and programming language in this system. **9. Multitasking , Multiprogramming , Multiprocessing :** a. Capability of running multiple tasks at a time in synchronized way is called **Multitasking**. b. Capability of allowing execution of multiple programs is called **Multiprogramming**. c. Capability of a processor of allowing simultaneous execution of multiple programs called **Multiprocessing.** 10. **Finite State Machine:** It is a device which stores a current state of process at that time. a. Output of finite state of machine is based upon the input given to device. b. New state is depending upon the old state and input.	
	(b) Ans.	**Explain OTP (one time pad) with example.** 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)	**6M** ***Explanation 3M***

		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"**.	***Any Example 3M***
5.	**(a)** **Ans.**	**Attempt any TWO:** **Explain IT Act, 2000 and IT ACT, 2008 with advantages and disadvantages. (any 2).** **IT act 2000:** The IT Act 2000 gives very good solution to the cyber crimes. In this Act several sections and Chapters are there which are defined in the following manner: • Chapter 1 the preliminary chapter of IT Act 2000 gives all of the information about the short title, territory up to which it is extendable, and the basic application of related laws. • Chapter 2 to 7 of this Act defines 'access', 'addressee', 'adjudicating officer', 'affixing digital signature', 'Asymmetric Cryptography', 'cyber', 'computer', 'digital signature', 'Digital Signature Certificate' and other numerous basic terms, which are defined in its appendix. • Other chapters of this Act define those crimes which can be considered as cognizable offences, i.e. for which the police can arrest the wrongdoer immediately. • Section 80 of this Act gives a freedom to the police officer to search, arrest the offender who is indulged in that crime or going to commit it. • Section 65 to 70 covers all of the cognizable offences, namely, 'tampering of documents', 'hacking of the personal computer', 'obscene information transmission or publication', 'failure of compliance by certifying authority or its employees, of orders of the Controller of certifying authorities', 'Access or attempt to access by any unauthorized person, a protected system notified by Govt. in the Official Gazette' in which non-bailable warrant is issued or no warrant is required. • Section 71 indicates the offence 'Misrepresentation of material fact from the controller or Certifying Authority for obtaining any	**2 x 8=16** **8M** ***IT Act, 2000 explanation 2M***

		license or Digital Signature Certificate'. **Advantages:** • Email is considered as the valid and legal form of communication. • Digital signatures have been given legal validity and sanction • Companies can carry out e-business using legal infrastructure. • Corporate companies can become certifying authorities for issuing digital signatures certificates. • Enables government to issue notifications or any other type of documents through internet bringing e-governance. • Enables businesses to file forms, applications or any other type of document with any office, body, institute in an electronic form. • Enables the corporations and businesses to have statutory remedy in case of any act of intrusion into their computer system or network, which causes damages or copies data. The Act provides remedy in the form of monetary damages up to 1 crore. **Disadvantages :** • No mention on IPR (Intellectual Property Rights). • No provisions for copy-righting, trade marking or patenting of electronic information and data. • The law does not consists of the rights and liabilities available to the domain name holders. • Not considered the regulation of electronic payments gateway, thus making the banking and financial sectors indecisive (weak) in their stands. • No mention on security of internet while using the IT laws. **IT act 2008:** • It is the information Technology Amendment Act, 2008 also known as ITA-2008 • It is a considerable addition to the ITA-2000 and is administered by the Indian Computer Emergency Response Team (CERT-In) in year 2008. • Basically, the act was developed for IT industries, to control e-commerce, to provide e-governance facility and to stop	***IT Act, 2000 any 2 advantages 1M*** ***IT Act, 2000 any 2 disadvantages 1M***

		cybercrime attacks. • The alterations are made to address some issues like the original bill failed to cover, to accommodate the development of IT and security of e-commerce transactions. **The modification includes:** • Redefinition of terms like communication device which reflect the current use. • Validation of electronic signatures and contracts. • The owner of an IP address is responsible for content that are accessed or distributed through it. • Organizations are responsible for implementation of effective data security practices. **Following are the characteristics of IT ACT 2008:** • This Act provides legal recognition for the transaction i.e. Electronic Data Interchange (EDI) and other electronic communications. Electronic commerce is the alternative to paper based methods of communication to store information. • This Act also gives facilities for electronic filling of information with the Government agencies and further to change the Indian Penal Code-Indian Evidence Act 1872, Bankers code Evidence Act 1891 and Reserve Bank of India Act, 1934 and for matter connected therewith or incidental thereto. • The General Assembly of the United Nations by resolution A/RES/51/162, dated 30 January 1997 has adopted the model law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. • This recommends that all States give favorable consideration to the above said model law when they enact or revise their laws, in terms of need for uniformity of the law applicable to alternative to paper based methods of communication and storage of information. • 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. **Advantages:** • Redefinition of terms like communication device which reflect the current use.	***IT Act, 2008 explanation 2M***

		• Validation of electronic signatures and contracts. • The owner of an IP address is responsible for content that are accessed or distributed through it. • Organizations are responsible for implementation of effective data security practices. **Disadvantages:** • Liability of ISPs has been revisited and responsibility shall lie on complainant to prove lack of due diligence or presence of actual knowledge by intermediary, as proving conspiracy would be difficult. • Cyber law enforcement teams will face with more challenges. • The power of interception of traffic data and communications over internet will need to be exercised, deliberating powers of monitoring, collection , decryption or interception. • Power for blocking websites should also be exercised carefully and should not transgress into areas that amounts to unreasonable censorship. • Many of the offences added to the Act are cognizable but bailable which increases the likelihood of tampering of evidence by cybercriminal once he is released on bail.	***IT Act, 2008 any 2 advantages 1M*** ***IT Act, 2008 any 2 disadvantages 1M***
	(b) Ans.	**Describe Hill cipher with example.** **Hill Cipher** This is a polygraphic substitution cipher. This is based on linear algebra. Lester S Hill invented this cipher, which uses basic matrix multiplication. So, the alphabets are converted into numbers. Each letter from A to Z is assigned a digit from 0 to 25 such that A = 0, B = 1, C = 2…. Z = 25. The total encryption process is divided into three parts: 1. Preparing the plain text 2. Preparing the key 3. Encryption **1. Preparing the Plain text:** ∗ Each letter in the message is converted into numbers as A =0, B = 1, and so on. ∗ These numbers are written in columnar form. Number of letters in	**8M** ***Explanation 4M***

each column depends on the key matrix size.

* If the last column contains less elements, then append necessary numbers to complete it.

Example:

Plain text : "COE", If matrix size 3 X 3,

C = 2, O = 14, E = 4.

Plain text Matrix = $\begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix}$

Example 4M

2. Preparing the key :

The key matrix is a square matrix. If key = ANOTHERBZ,

Key Matrix is written as, K = $\begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix}$

3. Encryption :

The encryption is the multiplication of key matrix K and plain text matrix P. The number used for letters are base 26, so mod 26 is used to generate plain text.

Cipher Text C.T. = K * P Mod 26

$$C.T. = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix} * \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix} \text{ Mod } 26$$

$$= \begin{bmatrix} 2\,X\,0 + 14\,X\,13 + 4\,X\,14 \\ 2\,X\,19 + 14\,X\,6 + 4\,X\,4 \\ 2\,X\,17 + 14\,X\,1 + 4\,X\,25 \end{bmatrix} \text{ Mod } 26$$

$$= \begin{bmatrix} 238 \\ 138 \\ 148 \end{bmatrix} \text{ Mod } 26$$

$$= \begin{bmatrix} 4 \\ 8 \\ 18 \end{bmatrix}$$

$$= \begin{bmatrix} E \\ I \\ S \end{bmatrix}$$

C.T. = 'E I S'

OR

Decryption:

To convert the cipher text into plain text, again perform multiplication. Here, the inverse of key matrix is multiplied by the cipher text matrix to generate the plain text matrix.

$P = K^{-1} * C \text{ Mod } 26$

$K^{-1} = \frac{1}{\det |K|} .$ adjoint (K)

K^{-1} can be found by

- Replace original elements of the matrix by the adjoint of those elements in the matrix.
- Transpose the matrix
- Divide every element by the determinant of the original matrix.

Example: Cipher Text ='EIS', Key K = 'ANOTHERBZ'

- **Adjoint of K** is found by,

At [0,0] = 6 X 25 – 1 X 4 = 150 - 4 = 146

At [0,1] = -(19 X 25 – 17 X 14) = -(475-68) = -407

At [0,2] = 19 X 1 – 17 X 6 = 19 - 102 = -83

At [1,0] = -(13 X 25 – 1 X 14) = -(325-14) = -311

At [1,1] = -(0 X 25 – 17 X 14) = 0-238 = -238

At [1,2] = -(0 X 1 – 17 X 13) = -(0-221) = 221

At [2,0] = 13 X 4 – 6X 14 = 52 - 84 = -32

At [2,1] = -(0 X 4 – 19X 14) = -(0-266) = 266

At [2,2] = 0 X 6 – 19X 13 = 0 - 247 = -247

$$\begin{bmatrix} 146 & -407 & -83 \\ -311 & -238 & 221 \\ -32 & 266 & -247 \end{bmatrix}$$

* **Transpose of the matrix,**

$$\begin{bmatrix} 146 & -311 & -32 \\ -407 & -238 & 266 \\ -83 & 221 & -247 \end{bmatrix} \text{ Mod } 26$$

$$= \begin{bmatrix} 16 & -25 & -6 \\ -17 & -4 & 6 \\ -5 & 13 & -13 \end{bmatrix}$$

* **Determinant** of the key matrix $\begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix}$ is,

D = 0(6 x 25 – 4 x 1) – 13 (19 x 25 – 17 x 4) + 14 (19 x 1 – 17 x 6)
= -6453.

⇨ -6453 Mod 26 = -5.

Instead of diving by -5, multiply by the multiplicative inverse of -5 = -21.

Thus K^{-1} = -21 $\begin{bmatrix} 16 & -25 & -6 \\ -17 & -4 & 6 \\ -5 & 13 & -13 \end{bmatrix}$

$$= \begin{bmatrix} -336 & 525 & 126 \\ 357 & 84 & -126 \\ 105 & -273 & 273 \end{bmatrix} \text{ Mod } 26$$

$$= \begin{bmatrix} -24 & 5 & 22 \\ 19 & 6 & -22 \\ 1 & -13 & -13 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 2 & 5 & 22 \\ 19 & 6 & 4 \\ 1 & 13 & 13 \end{bmatrix}$$

		For decryption, **Plain Text = K^{-1} * C Mod 26** $= \begin{bmatrix} 2 & 5 & 22 \\ 19 & 6 & 4 \\ 1 & 13 & 13 \end{bmatrix} * \begin{bmatrix} 4 \\ 8 \\ 18 \end{bmatrix} Mod\ 26$ $= \begin{bmatrix} 2 \text{ x } 4 & 5 \text{ x } 8 & 22 \text{ x } 18 \\ 19 \text{ x } 4 & 6 \text{ x } 8 & 4 \text{ x } 18 \\ 1 \text{ x } 4 & 13 \text{ x } 8 & 13 \text{ x } 18 \end{bmatrix} = \begin{bmatrix} 444 \\ 196 \\ 342 \end{bmatrix} = \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix} = \begin{bmatrix} C \\ O \\ E \end{bmatrix}$ = 'COE'. Thus the cipher text 'EIS' is decrypted as original plain text 'COE'.	
	(c) **Ans.**	**Define physical access. What is physical access control? List and explain physical access threats.** **Physical Access**: Physical access refers to the access of data, information or any object in a system at a physical location or place. **Physical access control:** This is the control mechanism in place to minimize the risk of attacks from physical threats. Physical Access Controls also use the mechanism to identify individuals who are attempting to enter a facility, area or system. The various physical access threats are, Major categories of physical security threats are: 1. **Extreme Weather**: Temperature, humidity, water, flood, wind, snow, lightening, etc. 2. **Fire:** Explosion, heat, smoke 3. **Chemical/ liquid leakages:** Liquid fall, oxic material, war gases, Industrial pollutions, etc. 4. **Movement:** Earthquake, Shearing, Shaking, volcano, slide, Building collapse, falling object, sliding, etc. 5. **Energy anomalies:** Electricity disruption, magnetism, static electricity, radiation: sound, light, radio, microwave, electromagnetic etc. 6. **Biological:** Virus, bacteria, animal, insect, etc. 7. **Equipment :** Mechanical or electronic component failure, etc 8. **Human/People:** Theft, Strike, war, sabotage, etc.	**8M** ***Definition 1M*** ***Physical access control 1M*** ***List (any 4) 2M***

		Explanation: ∗ **Weather**: environmental failure is a type of disaster that includes any interruption in the supply of controlled environmental support provided to the center. Temperature, humidity levels are always controlled and any extreme change to this is a threat to the system. ∗ **Lightning**: An electric charge of air can cause either direct lightning strikes to the facility or surges affecting electricity supply. ∗ **Fire**: Fire affects the system through heat, smoke. ∗ **Earthquake**: The violent ground motion that results from the movement of the earth's surface causes high risks of damage to the physical asset. ∗ **Liquid leakage**: This include all types of liquid leakage, ranging from small accidents which can happen through individuals working to burst or leaking pipes and accidental discharge of sprinklers or chemicals also.	***Explanation(any 2) 2M each***
6.	**(a) Ans.**	**Attempt any FOUR:** **Describe ITSEC with its target of evaluation levels.** **ITSEC(Information Technology Security Evaluation Criteria**) with its target evaluation levels : ITSEC is developed by European country for security equation criteria. 1. ITSEC focuses more on integrity and availability. It tries to provide a uniform approach to product and system. 2. ITSEC will also provide security targets like: i. Policy for system security ii. Required mechanism for security iii. Required rating to claim for minimum strength iv. Level for evaluating targets –functional as well as evaluation(F- xx and E – yy) ITSEC classes contain non- hierarchical structure which are specialized classes are as given below. (F- xx) ∗ F-IN for high integrity. ∗ F-AV for high availability. ∗ F-DI for high data integrity. ∗ F-DX for networks that require high demands for	**4 x 4=16** **4M** ***Description 2M***

		confidentiality and integrity during data exchanges. **ITSEC uses following evaluation (Assurance) classes from E0 to E6 to evaluate the security.** E0 – Minimal protection, levels which fail to meet E1 requirements. E1 – Security target and informal architecture design containing informal description must be produced. E2 – E1 requirements plus an informal detailed design and test document must be produced. E3 – E2 requirements plus source code or hardware drawing to be produced. Correspondence must be shown between source codes of detailed design. E4 – E3 requirements plus formal model of Security and Semi – formal specification of Security function architecture and detailed design to be produced. E5 – E4 requirements plus architecture design to explain the inter relationship between security component. E6 – E5 requirements plus formal description of architecture and Security function to be produced in addition to consistency with the formal security model.	***Levels 2M***
	(b) Ans.	**Explain event classification in Information Security.** **Event classification:** The various events in the organizations are classified in order to deal with disaster recovery planning, which are, 1. Disaster 2. Crisis 3. Catastrophe 1. **Disaster:** Disaster is an event that causes permanent and substantial damage or destruction to the property, equipment, information, staff or services of the business. The objects can be assigned the labels according to its value and appropriate security and protection mechanisms can be assigned. 2. **Crisis:** This is an abnormal situation that presents some extra ordinary high risks to a business and that will develop into a disaster unless carefully managed. Before a crisis develops into a disaster, necessary actions are taken so that damage to the system can be minimized. 3. **Catastrophe:** Major disruptions resulting from the destruction of critical equipment processing. This is a situation resulted from the	**4M** ***List 1M*** ***Explanation 1M each***

		disaster occurred in the organization.	
	(c) **Ans.**	**Explain followings:** **(i) Mail Bombs** **(ii) Bug Exploits** **(i) Mail Bombs:** ∗ E-mail ―bombing is characterized by abusers repeatedly sending an identical email message to a particular address. ∗ A mail bomb is the sending of a massive amount of e-mail to a specific person or system. ∗ A huge amount of mail may simply fill up the recipient‘s disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop functioning. ∗ Mail bombs not only inconvenience the intended target but they are also likely to inconvenience everybody using the server. ∗ Senders of mail bombs should be wary of exposing themselves to reciprocal mail bombs or to legal actions. **(ii) Bug Exploits:** ∗ An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). ∗ Such behavior frequently includes things like gaining control of a computer system.	**4M** ***Explanation of Mail Bombs & Bug Exploits 2M each***
	(d) **Ans.**	**Define Biometric system with a neat diagram.** **Biometric System:** Biometrics refers to metrics related to human characteristics and traits. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control.	**4M**

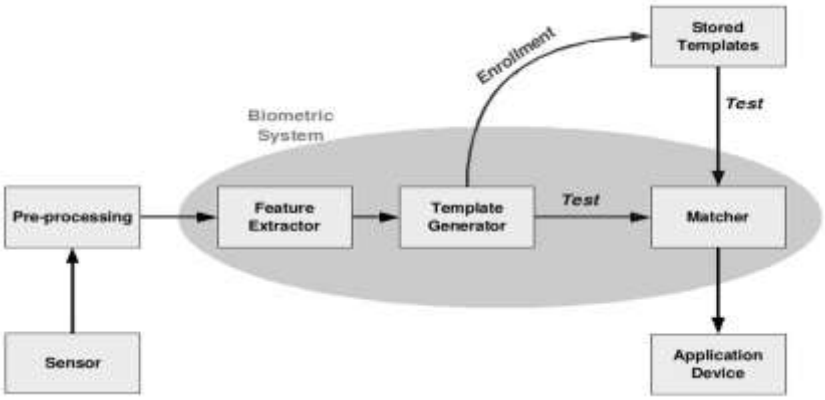


Diagram 2M

1. The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database.
2. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison.
3. Second, in identification mode the system performs a one-to-many comparison against biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.
4. The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an

Description 2M

		individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. 5. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. 6. During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements.	
	(e)	**What is Data recovery? Explain procedure for deleted files recovery.** ***(Note: Procedure using any data recovery tool may also be considered)***	**4M**
	Ans.	**Data Recovery :** Data recovery is retrieving deleted/inaccessible data from electronic storage media (hard drives, removable media, optical devices, etc.) **<u>Procedure to recover deleted files:</u>** • If the file is deleted from the recycle bin, or by using shift + delete button, the simplest and easiest way to recover deleted file is by using a data recover software. • In this, the data recovery tool will scan the storage drive from which the file is deleted. • The tool shows the list of all the files which are deleted, corrupt or damaged. • The file to be recovered can be chosen and restored in either the	***Definition 1M*** ***Procedure 3M***

		same drive or in any other location. • If the file has been partially over written, there are some data recovery software applications which will perform better to recover the maximum of data. • It is important to save the recovered file in a separate location like a flash drive. • A file can only be permanently lost if it is over written. So do not over write, do not install or create new data on the file location.	