



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

SUMMER – 19 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

Important Instructions to examiners:

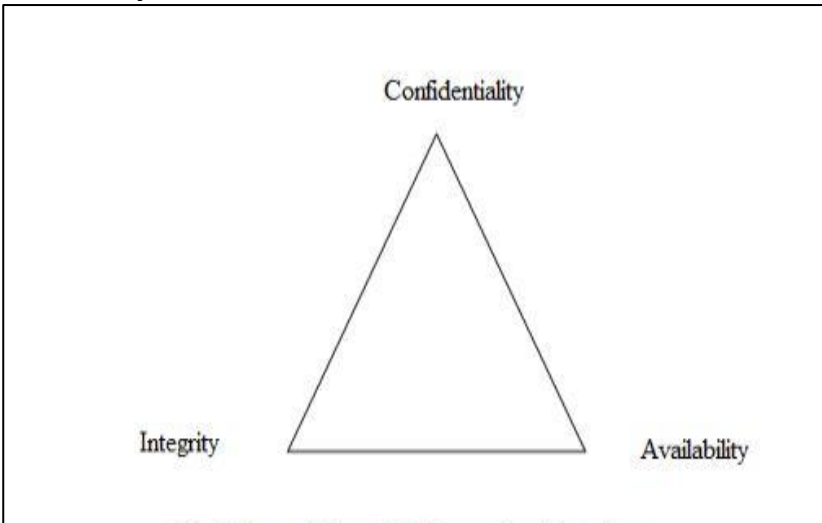
- 1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
- 2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
- 3) The language errors such as grammatical, spelling 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	Attempt any THREE of the following :	12 M
	a	Describe Bell-LaPadula model of confidentiality.	4 M
	Ans	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. Bell – LaPadula: - The Bell-La Padula (BLP) model is a classic mandatory access-control model for protecting confidentiality. The BLP model is derived from the military multilevel security paradigm, which has been traditionally used in military organizations for document classification and personnel clearance. 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	Relevant explanation: 4M

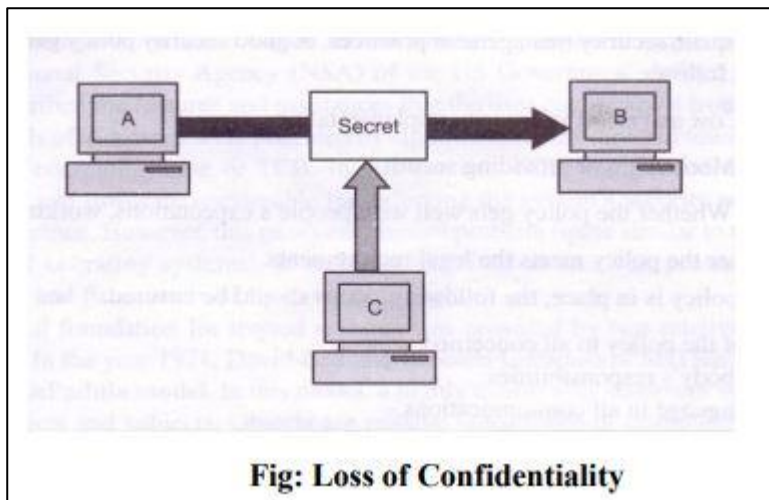


		documents with the corresponding level of security or below. How Bell LaPadula Works? The security levels in BLP form a partial order, Each object, x, is assigned to a security level, $L(x)$. Similarly, each user, u, is assigned to a security level, $L(u)$. Access to objects by users is controlled by the following two rules: • Simple security property. A user u can read an object x only if $L(x) < L(u)$ • A user u can write (create, edit, or append to) an object x only if $L(u) < L(x)$ • The simple security property is also called the —no read up rule, as it prevents users from viewing objects with security levels higher than their own. • The property is also called the —no write down rule. It is meant to prevent propagation of information to users with a lower security level.	
	b	How Cyber Crimes are investigated?	4 M
	Ans	Cybercrime 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	Relevant explanation: 4M



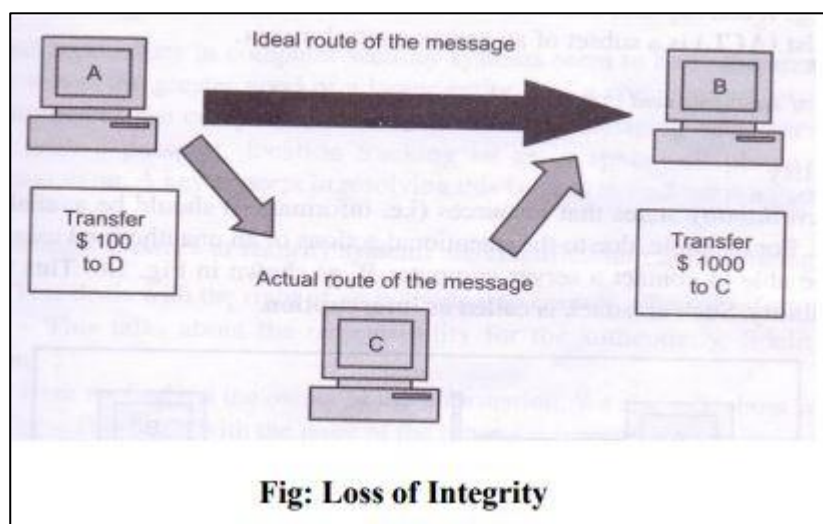
		next course of action. Obtaining and Serving Search Warrants. If it is believed that the suspect has crucial evidence at his or her home or office, a search warrant will be required to seize the evidence. Surveillance Two forms of surveillance are used in computer crime investigations: physical and computer. 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. Computer forensics is the study of computer technology as it relates to the law. This generally means analyzing the system by using a variety of forensic tools & processes, and that the examination of the suspect system may lead to other victims and other suspects.	
	c	State Pillars of information security. Describe with neat diagram.	4 M
	Ans	Three pillars of information security: 1) Confidentiality 2) Integrity 3) Availability  Fig: Three pillars of Information Security	List 2M, Description of any one pillar with diagram 2M

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.

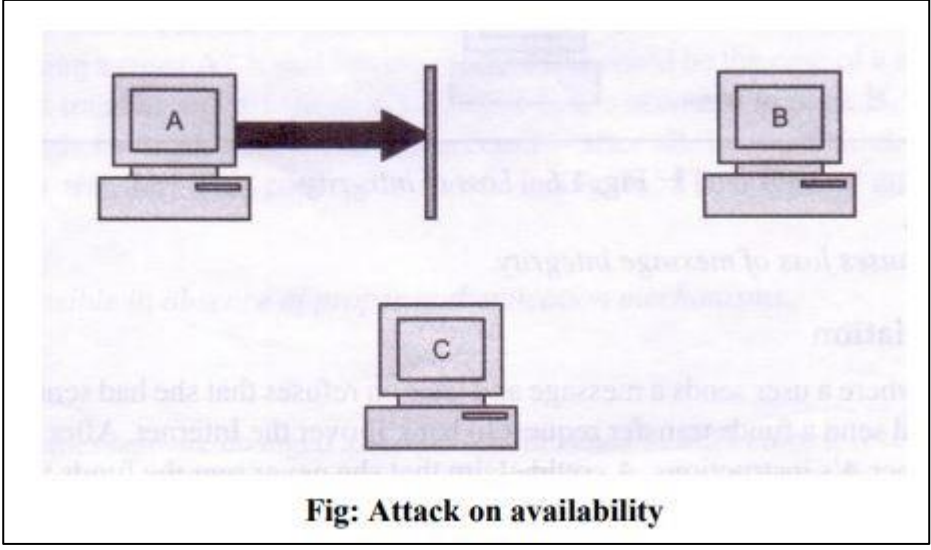


2) **Integrity:** The concept of integrity ensures that

- 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.





		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	
	d	Define the following terms: 1) Plain text 2) Cipher text 3) Cryptography 4) Cryptanalysis	4 M
	Ans	1) 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. 2) Cipher text: When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text. 3) Cryptography: Cryptography is the art and science of achieving security by encoding messages to make them non-readable. 4) Cryptanalysis: Cryptanalysis is the technique of decoding messages from a	Correct definition, each 1M



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.	
	B	Attempt any ONE of the following :	6 M
	a	What is data recovery? How deleted files can be recovered?	6 M
	Ans	Data Recovery: Data recovery is retrieving deleted/inaccessible data from electronic storage media (hard drives, removable media, optical devices, etc.) Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible for some reason. When files have been mistakenly deleted and need to be recovered, data recovery is necessary. Deleted file recovery There is no such thing as a permanently deleted file. If a recycle bin is empty, or a file is deleted with Shift + Delete button, it will simply kill the path that directs to the exact physical location where the file is stored. In hard drives, tracks are concentric circles and sectors are on the tracks like wedges. The disk rotates When want to access a file and the head reads the file from that sector. The same head also writes new data on sectors marked as available space Procedure to recover deleted files: • 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 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	Explanation of Data Recovery: 3M, Relevant explanation: 3M

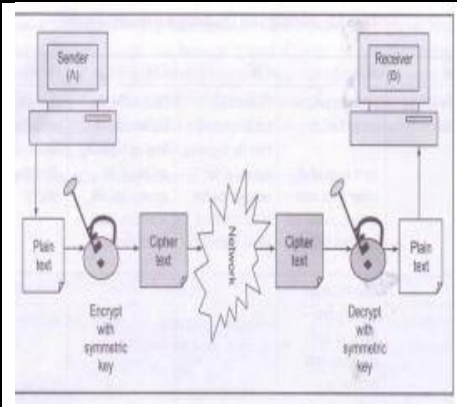
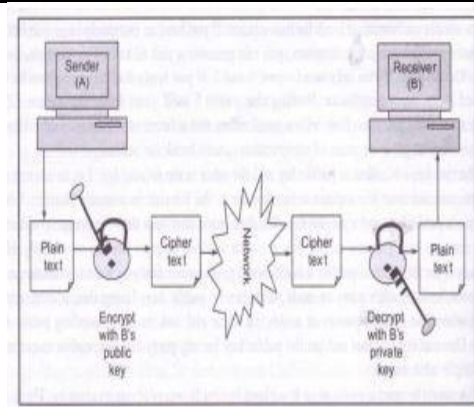


MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		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.															
	b	Differentiate between symmetric and asymmetric key cryptography.	6 M														
	Ans	<table><tr><th>Symmetric Key Cryptography</th><th>Asymmetric Key Cryptography</th></tr><tr><td>1. In symmetric key cryptography only one key is used and the same key is used for both encryption and decryption of messages.</td><td>1. In asymmetric key cryptography two different keys are used. One key is used for encryption and other key is used for decryption.</td></tr><tr><td>2. It is also referred to as Secret Key Cryptography or Private Key Cryptography</td><td>2. It is also referred to as Public Key Cryptography.</td></tr><tr><td>3. In this method, the key that deciphers the cipher text is the same as (or can be easily derived from) the key enciphers the clear text.</td><td>3. In this method the two keys are mathematically interrelated, but it's impossible to derive one key from the other.</td></tr><tr><td>4. Symmetric-key confirms sender's identity by knowing who can encrypt the message or decode the message in other words, by knowing who has the key</td><td>4. Asymmetric-key confirms the sender's identity by double the encryption.</td></tr><tr><td>5. The most widely used symmetric ciphers are DES and AES.</td><td>5. Well-known asymmetric ciphers are the Diffie-Hellman algorithm, RSA, and DSA.</td></tr><tr><td>6. Diagram</td><td>6. Digram</td></tr></table>	Symmetric Key Cryptography	Asymmetric Key Cryptography	1. In symmetric key cryptography only one key is used and the same key is used for both encryption and decryption of messages.	1. In asymmetric key cryptography two different keys are used. One key is used for encryption and other key is used for decryption.	2. It is also referred to as Secret Key Cryptography or Private Key Cryptography	2. It is also referred to as Public Key Cryptography.	3. In this method, the key that deciphers the cipher text is the same as (or can be easily derived from) the key enciphers the clear text.	3. In this method the two keys are mathematically interrelated, but it's impossible to derive one key from the other.	4. Symmetric-key confirms sender's identity by knowing who can encrypt the message or decode the message in other words, by knowing who has the key	4. Asymmetric-key confirms the sender's identity by double the encryption.	5. The most widely used symmetric ciphers are DES and AES.	5. Well-known asymmetric ciphers are the Diffie-Hellman algorithm, RSA, and DSA.	6. Diagram	6. Digram	Each Point :1M, 6 Points Expected
Symmetric Key Cryptography	Asymmetric Key Cryptography																
1. In symmetric key cryptography only one key is used and the same key is used for both encryption and decryption of messages.	1. In asymmetric key cryptography two different keys are used. One key is used for encryption and other key is used for decryption.																
2. It is also referred to as Secret Key Cryptography or Private Key Cryptography	2. It is also referred to as Public Key Cryptography.																
3. In this method, the key that deciphers the cipher text is the same as (or can be easily derived from) the key enciphers the clear text.	3. In this method the two keys are mathematically interrelated, but it's impossible to derive one key from the other.																
4. Symmetric-key confirms sender's identity by knowing who can encrypt the message or decode the message in other words, by knowing who has the key	4. Asymmetric-key confirms the sender's identity by double the encryption.																
5. The most widely used symmetric ciphers are DES and AES.	5. Well-known asymmetric ciphers are the Diffie-Hellman algorithm, RSA, and DSA.																
6. Diagram	6. Digram																



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		 	
2		Attempt any TWO of the following :	16 M
	a	Describe any Eight Protection Mechanism in ‘Trusted Computing Base’	8 M
	Ans	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 when data or information at one level is available at another level (Higher or Lower), then it	Any 8 mechanisms $\frac{1}{2}$ M each



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		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	Describe levels of information classification and explain any three criteria for classification of information.	8 M
	Ans	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 grave damage to the country's national security.	Elaboration with the any Five terms: 5M, Any Three criteria: 3M



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		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.	
	c	Describe 'IT Act-2000' and 'IT Act 2008'.	8 M
	Ans	The IT Act 2000 gives very good solution to the cybercrimes these solutions are provided in the following ways. In this Act several sections and Chapters are there which are defined in the following manner: 1. 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. 2. 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. 3. 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. 4. 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. 5. 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 as shown in table below. 6. Section 71 indicates the offence 'Misrepresentation of material fact from the controller or Certifying Authority for obtaining any license or Digital Signature Certificate'. In which bailable warrant may be issued	Any 4 relevant points each 1M, 4M for IT ACT 2000 and 4M for IT ACT 2008



	covered in the table below. 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 ecommerce, to provide e-governance facility and to stop 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. Validation of electronic signatures and contracts.	
--	--	--



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		• 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.	
3		Attempt any FOUR of the following :	16 M
	a	Describe COBIT Framework.	4 M
	Ans	COBIT: 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 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.	Description 3M, Diagram 1M



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

	b	Explain following with reference to information security: (i) Security Policy (ii) Standards (iii) Guidelines (iv) Procedures	4 M
	Ans	Security policy: An information security policy consists of high level statements relating to the protection of information across the business and should be produced by senior management. • The policy outlines security roles and responsibilities, defines the scope of	1M each



	information to be protected, and provides a high level description of the controls that must be in place to protect information. • Policies are of following types: • Senior Management Policy • Regulatory Policy • Advisory Policy • Informative Policy Standards: Standard consists of specific low level mandatory controls that help 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. Guidelines: 1. It should consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place. 2. It should view as best practices that neither are nor usually 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. Procedures Procedures are the most specific type of security document. They are characterized by their very detailed, step-by-step approach toward implementing security standards and guidelines that support the policies. Procedures are often used in the configuration of operating systems, network hardware, and databases. Furthermore, procedures are used in instructing how to add new software, systems, and users, among others. Since organizations differ from one another and no two organizations are exactly the same, procedures will likewise differ between organizations. However, there are certain types of procedures that may be present in most, if not all organizations, such as the following: • Incident response—These are procedures that direct members of the organization on how to detect an incident and how to respond	
--	--	--



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		accordingly. A step-by-step guide as to when the management, as well as external parties like law enforcement agencies, should step in and take over. • Auditing–Since auditing is an integral and sensitive matter, procedures should include details on what to audit, why the audits are being done, and how to maintain the audit logs. • Environmental/Physical–Examples of such procedures cover the protection of Ethernet cables and keeping them safe from wiretapping attempts, as well as controlling the room temperatures where key equipment is stored. • Administrative–This type of procedure helps to distinguish and separate the tasks and duties of employees who are directly in charge of the organization’s systems. An excellent example is showing that database administrators should not meddle with the company’s firewall logs. Configuration–This type of procedure deals with operating systems, firewalls, and routers, to name a few.	
	c	Describe various physical Access threats.	4 M
	Ans	Physical Access Threats: The following list classifies the physical threats into three main categories; 1) Internal: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc. • Energy: Electricity, magnetism, radio wave anomalies, etc. • Equipment: Mechanical or electronic component failure, etc. 2) External: These threats include Lightning, floods, earthquakes, etc. • Weather: Temperature, humidity, water, flood, wind snow, lightening, etc. • Fire and Chemical: Explosion, smoke, toxic, material. Industrial pollutions, etc. • Earth Movement: Earthquake, volcano, slide, etc. • Object Movement: Building collapse, falling object, car, truck, plane, etc. 3) Human: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.	Any 4 Threats 1 M each
	d	Describe any four authentication protocols.	4 M



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

Ans	An authentication protocol is a type of computer communications protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. It allows to authenticate the connecting entity (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for authentication as well as syntax. It is the most important layer of protection needed for secure communication within computer networks. 1) CHAP: It is a Challenge Handshake Authentication Protocol. This protocol is used by servers to validate the identity of remote client. CHAP verifies the identity by using 3- way handshaking and by using shared secret • After establishment of link, the server sends a challenge message to the client. Then client responds with a value obtained by using a one-way hash function. • Server compares the response i.e. hash value with its own calculated hash value. If the value matches, then the authentication is acknowledged or else the connection is terminated. 2) EAP: It is Extensible Authentication Protocol and mainly used for wireless networks and point to point connections. It may support various authentication mechanisms like tokens, certificate, one-time password, smart cards etc. In EAP protocol • A user requests connection to WLAN through an access point. • Then the access point requests identification (ID) data from the user and transmits that data to an authentication server. • The authentication server then request the access point for proof of the validity of the ID. • After the verification from the user, access point sends it back to the authentication server and the user is connected to the network. 3) PAP: It is Password Authentication Protocol. It is used by Point to Point Protocol to validate users before allowing them access to server resources. In this protocol, a user's name and password are transmitted over a network and compared to a table of name-password pairs. It is a two way handshaking protocol. • Client sends username and password. • Server sends "authentication-ack", if credentials are OK or "authentication-nak". 4) SPAP: It is Shiva Password Authentication Protocol and it is an encrypting authentication protocol used by Shiva remote access servers. SPAP offers a higher level of security than other authentication protocols such as PAP, but it is not as secure as CHAP. 5) DES: It is a Data Encryption Standard (DES) is the classic among the	Any 4 protocols 1 M for each Protocol
------------	---	---



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		symmetric block cipher algorithms. DES was developed in the 1970s as a US-government standard for protecting non-classified information. DES encrypts 64-bit clear-text blocks under the control of 56-bit keys. Each key is extended by a parity byte to give a 64-bit working key. It uses both substitutions as well as transposition techniques of cryptography. 6) RADIUS: It is a Remote Authentication Dial-In User Service protocol. It is a client/server protocol and used for authentication and authorization of users who are dialing in remotely to servers on the network. • RADIUS client sends username and encrypted password to the RADIUS server. • RADIUS server responds with Accept, Reject, or Challenge. • The RADIUS client acts upon services and services parameters bundled with Accept or Reject. 7) S/KEY: It is a one-time password system developed for operating systems like UNIX. One-time password allows you to log on only once with a password, after which that password is no longer valid. Instead of memorizing passwords, list of passwords are given and that may be maintained by hardware device. Each time you login, you ask the hardware device for the next password. 8) TACACS: It is a Terminal Access Controller Access Control System. It is an older authentication protocol used mainly in UNIX networks. It allows a remote access server to pass a user's login password to an authentication server to check whether access can be allowed to a given system or not. TACACS is an encryption protocol and therefore less secure. 9) MS-CHAP(MD4): It is a Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). It is based on CHAP and was developed to authenticate remote Windows-based workstations. It uses the Message Digest 4 (MD4) hashing algorithm and the Data Encryption Standard (DES) encryption algorithm to generate the challenge and response. It also provides mechanisms for reporting connection errors and for changing the user's password. It only works on Microsoft Systems. 10) SKID (SKID2 and SKID3): SKID2 and SKID3 are secret key identification protocols. SKID2 provides unilateral entity authentication whereas SKID3 provides mutual entity authentication.	
	e	Describe the term "Software Piracy".	4 M
	Ans	Cybercrime Investigation Cell of India defines —software piracy as theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.	Description: 4 M

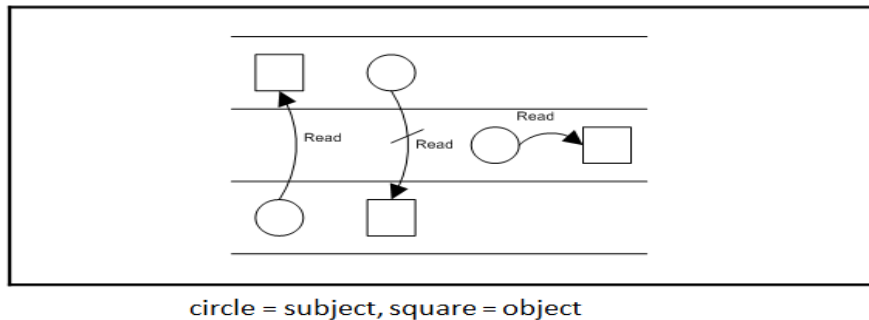


		Software piracy can be defined as —copying and using commercial Software purchased by someone else. Software piracy is illegal Each pirated piece of software takes away from company profits, reducing funds for further software development initiatives. Making duplication of software is an act of copyright infringement, and it's illegal. Providing unauthorized access to software or to serial numbers used to register software can also be illegal. Ways to Deal With/Minimize Software Piracy : • Have a central location for software programs. Know which applications are being added, modified or deleted. • Secure master copies of software and associate documentation, while providing faculty access to those programs when needed. • Never lend or give commercial software to unlicensed users. • Permit only authorized users to install software. • Train and make staff aware of software use and security procedures which reduce likelihood of software piracy.	
4	A	Attempt any THREE of the following :	12 M
	a	Describe Biba Model of Integrity.	4 M
	Ans	The Biba model has a similar structure to the BLP model, but it addresses integrity rather than confidentiality. Objects and users are assigned integrity levels that form a partial order, similar to the BLP model. The integrity levels in the Biba model indicate degrees of trust worthiness, or accuracy, for objects and users, rather than levels for determining confidentiality <i>The Biba Model</i> The major drawback of the BLP model was that it only considered the confidentiality of data. Consideration is not given to —need to know principle. Data is freely available to user to read data to its own level and lower level. • The BIBA model addresses the problem with the star property of the Bell-LaPadula model, which does not restrict a subject from writing to a more trusted object.	Description: 4 M

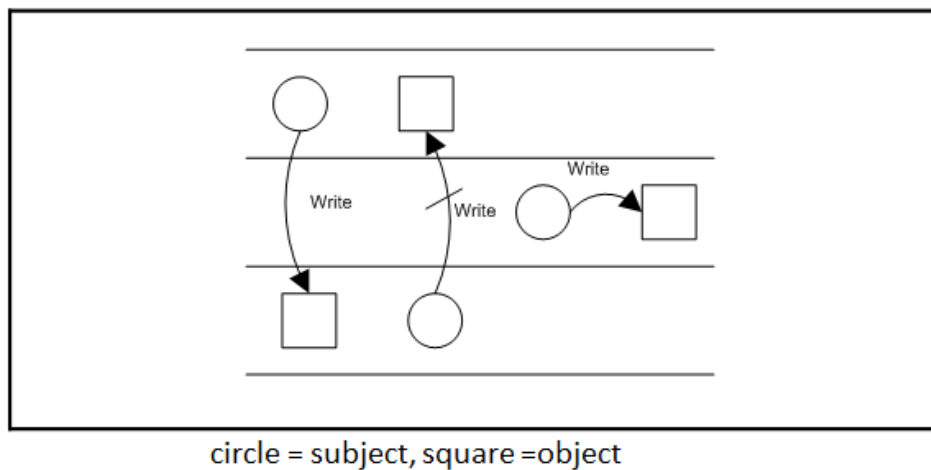
- Hence Ken Biba developed a model in 1977 that considered data integrity. It focuses on commercial sector where, data integrity is more important than confidentiality.
- Integrity is the protection of system data from intentional or accidental unauthorized changes.
- Although the security program cannot 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 has following three properties:

1. Simple Integrity Property (No Read-Down): - Data can be read from higher integrity level.



2. Star Integrity property: - Data can be written to lower integrity level.





MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		3. Invocation Property: - User cannot request services from higher integrity level. BIBA is the opposite of BLP where BLP is a WURD model (write up, read down), BIBA is RUWD model (Read up, write down)	
	b	Explain the following terms : (i) Authorization (ii) Authentication	4 M
	Ans	Authorization: It is a process of verifying that the known person has the authority to perform certain operation. It cannot occur without authentication. It is nothing but granting permissions and rights to individual so that he can use these rights to access computer resources or information. In general, authorization can be handled in one of three ways: 1. Authorization for each authenticated user, in which the system performs an authentication process to verify each entity and then grants access to resources for only that entity. This quickly becomes a complex and resource-intensive process in a computer system. 2. Authorization for members of a group, in which the system matches authenticated entities to a list of group memberships, and then grants access to resources based on the group's access rights. This is the most common authorization method. 3. Authorization across multiple systems, in which a central authentication and authorization system verifies entity identity and grants it a set of credentials. Authentication: Authentication is the process of determining identity of a user or other entity. It is performed during log on process where user has to submit his/her username and password. There are three widely used authentication mechanisms, or authentication factors: 1. Something a supplicant knows 2. Something a supplicant has 3. Something a supplicant is 1) Something a Supplicant Knows This factor of authentication relies upon what the supplicant knows and can recall. For example, a password, passphrase, or other unique	2M Authorization 2M Authentication

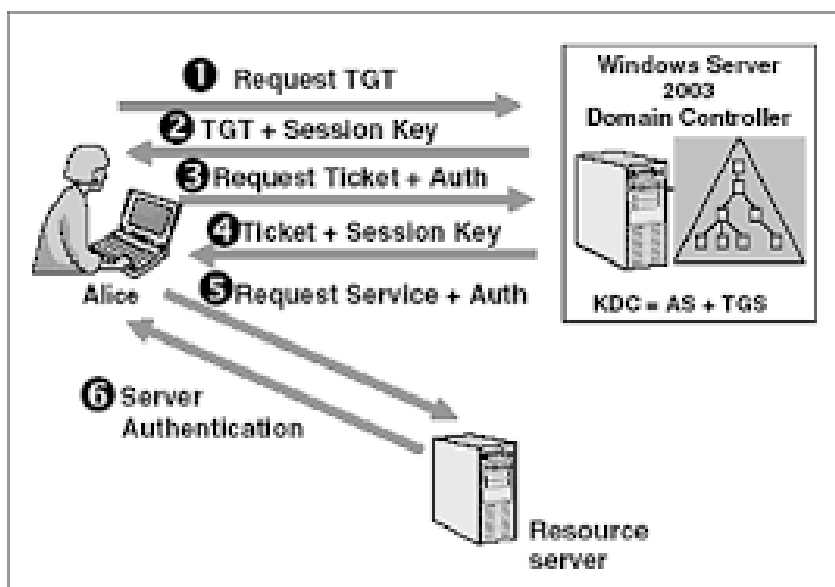


		authentication code, such as a personal identification number (PIN). A password is a private word or combination of characters that only the user should know. 2) Something a Supplicant Has This authentication factor relies upon something a supplicant has and can produce when necessary. One example is dumb cards, such as ID cards or ATM cards with magnetic stripes containing the digital (and often encrypted) user PIN, against which the number a user input is compared. The smart card contains a computer chip that can verify and validate a number of pieces of information instead of just a PIN. Another common device is the token, a card or key fob with a computer chip and a liquid crystal display that shows a computer-generated number used to support remote login authentication. Tokens are synchronous or asynchronous. Once synchronous tokens are synchronized with a server, both devices (server and token) use the same time or a time-based database to generate a number that must be entered during the user login phase. Something a Supplicant Is or Can Produce This authentication factor relies upon individual characteristics, such as fingerprints, palm prints, hand topography, hand geometry, or retina and iris scans, or something a supplicant can produce on demand, such as voice patterns, signatures, or keyboard kinetic measurements.	
	c	What is Kerberos? How it works?	4 M
	Ans	Kerberos is a network authentication protocol and it is designed to provide strong authentication for Client /Server Applications. It uses secret- key Cryptography. Kerberos is a protocol which was created by MIT as a solution to network security problems. It uses strong cryptography hence a client can prove its identity to a server and vice versa over an in secure network connection. Basics of Kerberos The basic Kerberos Model has the following participants: • A Client • A Server • A key distribution center (KDC) consisting of, ○ An Authentication Server (AS) ○ A Ticket Granting Server (TGS) ○ Database with strong passwords. Kerberos Process: Suppose client wants to communicate with server. • User logs in to gain network access. • This user will need a ticket to get tickets (TGT). • In Kerberos, the key distribution center (KDC) has an authentication service (AS) which gives TGT such that user has	Description-4 M



- to decrypt the response with the password hash.
- The user then sends the same and asks for service ticket.
 - The ticket granting service (TGS) will send service ticket.

This service ticket is used to authenticate the user at the network server side so that the user can make use of the server or client server session begins.



	d	Consider plain text “INFORMATION” and convert given plain text into cipher text using ‘Caesar Cipher’ with shift of position three. Write down steps in encryption.	4 M																																																				
	Ans	Caesar Cipher The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. Let us assign a numerical equivalent to each letter: <table><tr><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td></tr><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td></tr></table> <table><tr><td>K</td><td>L</td><td>M</td><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td></tr><tr><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td></tr></table> <table><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr><tr><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr></table> Then the algorithm can be expressed as follows. For each plaintext letter , substitute the cipher text letter A shift may be of any amount, so that the general Caesar algorithm is	A	B	C	D	E	F	G	H	I	J	0	1	2	3	4	5	6	7	8	9	K	L	M	N	O	P	Q	R	S	T	10	11	12	13	14	15	16	17	18	19	U	V	W	X	Y	Z	20	21	22	23	24	25	Steps:3 M Correct Ans-1M
A	B	C	D	E	F	G	H	I	J																																														
0	1	2	3	4	5	6	7	8	9																																														
K	L	M	N	O	P	Q	R	S	T																																														
10	11	12	13	14	15	16	17	18	19																																														
U	V	W	X	Y	Z																																																		
20	21	22	23	24	25																																																		



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		$C=E(K,P)=(K+P) \bmod 26$ In our case $K=3$ hence formula is : $C=E(3,P)=(3+P) \bmod 26$ The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. <table><tr><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td></tr><tr><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td></tr></table><table><tr><td>K</td><td>L</td><td>M</td><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td></tr><tr><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td></tr></table><table><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr><tr><td>X</td><td>Y</td><td>Z</td><td>A</td><td>B</td><td>C</td></tr></table> Plain Text : INFORMATION Cipher Text: LQIRPDWLRQ	A	B	C	D	E	F	G	H	I	J	D	E	F	G	H	I	J	K	L	M	K	L	M	N	O	P	Q	R	S	T	N	O	P	Q	R	S	T	U	V	W	U	V	W	X	Y	Z	X	Y	Z	A	B	C	
A	B	C	D	E	F	G	H	I	J																																														
D	E	F	G	H	I	J	K	L	M																																														
K	L	M	N	O	P	Q	R	S	T																																														
N	O	P	Q	R	S	T	U	V	W																																														
U	V	W	X	Y	Z																																																		
X	Y	Z	A	B	C																																																		
	B	Attempt any ONE of the following :	6 M																																																				
	a	Define security. Describe different types of securities in organization	6 M																																																				
	Ans	Security: It is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical) A successful organization should have the following multiple layers of security in place to protect its operations: 1. Physical security, to protect physical items, objects, or areas from unauthorized access and misuse 2. Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations 3. Operations security, to protect the details of a particular operation or series of activities 4. Communications security, to protect communications media, technology, and content 5. Network security, to protect networking components, connections, and contents 6. Information security: To protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology. Definition: 2 marks, List: 2 marks, Description of any 4: 1 mark each																																																					



	b	Explain Working of biometric system with neat sketch.	6 M
	Ans	<pre> graph LR Sensor[Sensor] --> Pre[Pre-processing] Pre --> FE[Feature Extractor] FE --> TG[Template Generator] TG --> M[Matcher] M --> AD[Application Device] TG -- Enrollment --> ST[Stored Templates] ST -- Test --> M TG -- Test --> M subgraph Biometric_System [Biometric System] FE TG M end </pre> 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. 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	Diagram 2 marks Description – 2 marks



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		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 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 characteristic measurements and user requirements.	
5		Attempt any TWO of the following :	16 M
	a	What is trusted computer security evaluation criteria? Explain various divisions used in TCSEC	8 M
	Ans	Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DOD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information. Policy: The security policy must be explicit, well-defined and enforced by the computer system. There are three basic security policies: • Mandatory Security Policy - Enforces access control rules based directly on an individual's clearance, authorization for the information and the confidentiality level of the information being sought. Other	4M for TCSEC, 4M for Divisions



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

	indirect factors are physical and environmental. This policy must also accurately reflect the laws, general policies and other relevant guidance from which the rules are derived. • Marking - Systems designed to enforce a mandatory security policy must store and preserve the integrity of access control labels and retain the labels if the object is exported. • Discretionary Security Policy - Enforces a consistent set of rules for controlling and limiting access based on identified individuals who have been determined to have a need-to-know for the information. Accountability: Individual accountability regardless of policy must be enforced. A secure means must exist to ensure the access of an authorized and competent agent which can then evaluate the accountability information within a reasonable amount of time and without undue difficulty. There are three requirements under the accountability objective: • Identification - The process used to recognize an individual user. • Authentication - The verification of an individual user's authorization to specific categories of information. • Auditing - Audit information must be selectively kept and protected so that actions affecting security can be traced to the authenticated individual. Divisions and classes The TCSEC defines four divisions: D, C, B and A where division A has the highest security. Each division represents a significant difference in the trust an individual or organization can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1. Each division and class expands or modifies as indicated the requirements of the immediately prior division or class. D — Minimal protection Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division C — Discretionary protection C1 — Discretionary Security Protection C2 — Controlled Access Protection B — Mandatory protection B1 — Labeled Security Protection B2 — Structured Protection B3 — Security Domains A — Verified protection A1 — Verified Design Beyond A1	
--	---	--



	b	Explain ‘Play fair cipher’ encryption process with respect to following terms: (i) Preparing plain text and key matrix (ii) Encryption process with operation rule.	8 M																									
	Ans	The Play fair cipher or Play Fair 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 2 parts. (i) Preparing plain text and key matrix 1. Creation of the matrix: a. Enter the key matrix (Ex Playfair example)in the matrix row-wise left to right and then top to bottom b. Drop duplicate letters c. Fill the remaining spaces in the matrix with the rest of the English Alphabets (A – Z) that were not part of the keyword. Combine I & J in the same cell of the table. d. If I or J is a part of the keyword, disregard both I and J while filling the remaining slots. <table border="1"><tr><td>P</td><td>L</td><td>A</td><td>Y</td><td>F</td></tr><tr><td>I</td><td>R</td><td>E</td><td>X</td><td>M</td></tr><tr><td>B</td><td>C</td><td>D</td><td>G</td><td>H</td></tr><tr><td>K</td><td>N</td><td>O</td><td>Q</td><td>S</td></tr><tr><td>T</td><td>U</td><td>V</td><td>W</td><td>Z</td></tr></table> (ii) Encryption process with operation rule. 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. 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. Eg. Plain text : “I am Rahul” Key : “Play fair Example” a. Plain text is broken into groups of two alphabets I AM RAHUL becomes IA MR AH UL. b. Taking each pair the rules are applied for encryption, as given below. 1. IA: From the matrix, since the two alphabets do not appear on the same row and column, replace the text with the diagonally opposite text, EP.	P	L	A	Y	F	I	R	E	X	M	B	C	D	G	H	K	N	O	Q	S	T	U	V	W	Z	Explanation 4M, Example 4M
P	L	A	Y	F																								
I	R	E	X	M																								
B	C	D	G	H																								
K	N	O	Q	S																								
T	U	V	W	Z																								



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		<table><tr><td>P</td><td>L</td><td>A</td><td>Y</td><td>F</td></tr><tr><td>I</td><td>R</td><td>E</td><td>X</td><td>M</td></tr><tr><td>B</td><td>C</td><td>D</td><td>G</td><td>H</td></tr><tr><td>K</td><td>N</td><td>O</td><td>Q</td><td>S</td></tr><tr><td>T</td><td>U</td><td>V</td><td>W</td><td>Z</td></tr></table> 2. MR: Since these two alphabets appear in the same row, replace them with their immediate right text as, IE. (The right side alphabet is replaced by wrapping around to the left side of row) <table><tr><td>P</td><td>L</td><td>A</td><td>Y</td><td>F</td></tr><tr><td>I</td><td>R</td><td>E</td><td>X</td><td>M</td></tr><tr><td>B</td><td>C</td><td>D</td><td>G</td><td>H</td></tr><tr><td>K</td><td>N</td><td>O</td><td>Q</td><td>S</td></tr><tr><td>T</td><td>U</td><td>V</td><td>W</td><td>Z</td></tr></table> 3. AH: From the matrix, since the two alphabets do not appear on the same row and column, replace the text with the diagonally opposite text, FD. <table><tr><td>P</td><td>L</td><td>A</td><td>Y</td><td>F</td></tr><tr><td>I</td><td>R</td><td>E</td><td>X</td><td>M</td></tr><tr><td>B</td><td>C</td><td>D</td><td>G</td><td>H</td></tr><tr><td>K</td><td>N</td><td>O</td><td>Q</td><td>S</td></tr><tr><td>T</td><td>U</td><td>V</td><td>W</td><td>Z</td></tr></table> 4. UL: Since these two alphabets appear in the same column, replace them with their immediately below text as LR. (The bottom side alphabet is replaced by wrapping around to the top side of the row) <table><tr><td>P</td><td>L</td><td>A</td><td>Y</td><td>F</td></tr><tr><td>I</td><td>R</td><td>E</td><td>X</td><td>M</td></tr><tr><td>B</td><td>C</td><td>D</td><td>G</td><td>H</td></tr><tr><td>K</td><td>N</td><td>O</td><td>Q</td><td>S</td></tr><tr><td>T</td><td>U</td><td>V</td><td>W</td><td>Z</td></tr></table>	P	L	A	Y	F	I	R	E	X	M	B	C	D	G	H	K	N	O	Q	S	T	U	V	W	Z	P	L	A	Y	F	I	R	E	X	M	B	C	D	G	H	K	N	O	Q	S	T	U	V	W	Z	P	L	A	Y	F	I	R	E	X	M	B	C	D	G	H	K	N	O	Q	S	T	U	V	W	Z	P	L	A	Y	F	I	R	E	X	M	B	C	D	G	H	K	N	O	Q	S	T	U	V	W	Z	
P	L	A	Y	F																																																																																																			
I	R	E	X	M																																																																																																			
B	C	D	G	H																																																																																																			
K	N	O	Q	S																																																																																																			
T	U	V	W	Z																																																																																																			
P	L	A	Y	F																																																																																																			
I	R	E	X	M																																																																																																			
B	C	D	G	H																																																																																																			
K	N	O	Q	S																																																																																																			
T	U	V	W	Z																																																																																																			
P	L	A	Y	F																																																																																																			
I	R	E	X	M																																																																																																			
B	C	D	G	H																																																																																																			
K	N	O	Q	S																																																																																																			
T	U	V	W	Z																																																																																																			
P	L	A	Y	F																																																																																																			
I	R	E	X	M																																																																																																			
B	C	D	G	H																																																																																																			
K	N	O	Q	S																																																																																																			
T	U	V	W	Z																																																																																																			
c	List any six data recovery tools. Explain data recovery procedure.	8 M																																																																																																					
Ans	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 Data recovery Procedure (i) There is no such thing as a permanently deleted file. If a recycle bin is empty, or a file is deleted with Shift + Delete button, it will simply kill the path that directs to the exact physical location where	8 points 8M																																																																																																					



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		the file is stored. (ii) In hard drives, tracks are concentric circles and sectors are on the tracks like wedges. The disk rotates. When we want to access a file and the head reads the file from that sector. The same head also writes new data on sectors marked as available space. (iii) For example : When storing files into hard disk, system would firstly write file names and size in FAT and successively write file content on FAT at the data field starting location in accordance with free space, then it begins to write real content in data field to complete 'file storage'. So, when anyone deletes a file, it does not disappear. (iv) Every computer file is a set of binary data i.e. in forms of 1s and 0s. The physical space is declared as available space for new data to be written when a file is deleted. So if anyone performs any new activity on a disk after deleting a file, then there is a chance that the file would be replaced partially or completely by new data. (v) For example : When deleting a file, system will just write a mark in the front of this file within FAT to mean this file is deleted and space it occupies is released for other files. Therefore, user is only required to employ a tool to remove the deletion mark when he wants to recover data. Certainly, all these should be performed under the requirement of no new files are written to occupy previous space of lost file in same way, if anyone performs disk defragmentation, the file may be over-written. In defragmentation, the utility copies files in closer sectors and tracks. This will help the computer to access a file quickly and it improves system's speed. Thus, it also involves a lot of over-writing on available space (where your deleted files may be). (vi) Hence, performing any new activity on the hard drive before recovering the file is a bad idea. 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 recovery software. (vii) 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. (viii) 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.	
6		Attempt any FOUR of the following :	16 M



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

a	Explain the concepts of system security assurance.	4 M
Ans	System Security Assurance Concepts: In IT security system, there are two types of requirements: • Functional requirement: It tells what system should do according to design. • Assurance requirement: It tells in what way the functional requirement should be implemented and tested. Both the above mentioned requirements should be able to answer- whether system does the right things in right way or not. 1. Goals of security Testing 2. Formal Security Testing Models 1. Goals of security Testing: • Security testing will show the flaws in security mechanisms of an information system which protect the data/information and functionality as expected. • This will verify the functions which are designed to achieve security and also validate the implementation of these functions - they are not faulty or random. • Such type of testing will be done by expert users not by causal users. • Security assurance and testing are ties together with many different concepts as well as principals and it is unfamiliar to many employees who are involved in IT development. 2. Formal Security Testing Models: 1) TCSEC: Trusted computer system evaluation criteria 2) ITSEC: Information Technology Security Evaluation Criteria 3) CTCPEC: Canadian Trusted Computer Product Evaluation 4) FC: Federal Criteria 5) Common Criteria: TCSEC, CTCPEC and ITSEC are joint to support international separate criteria into a single set of IT security criteria and the name given as Common Criteria (CC).	4M Explanation
b	Describe the working of digital signature with neat diagram.	4 M
Ans	Digital Signatures: 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	2M Diagram, 2M Explanation



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-

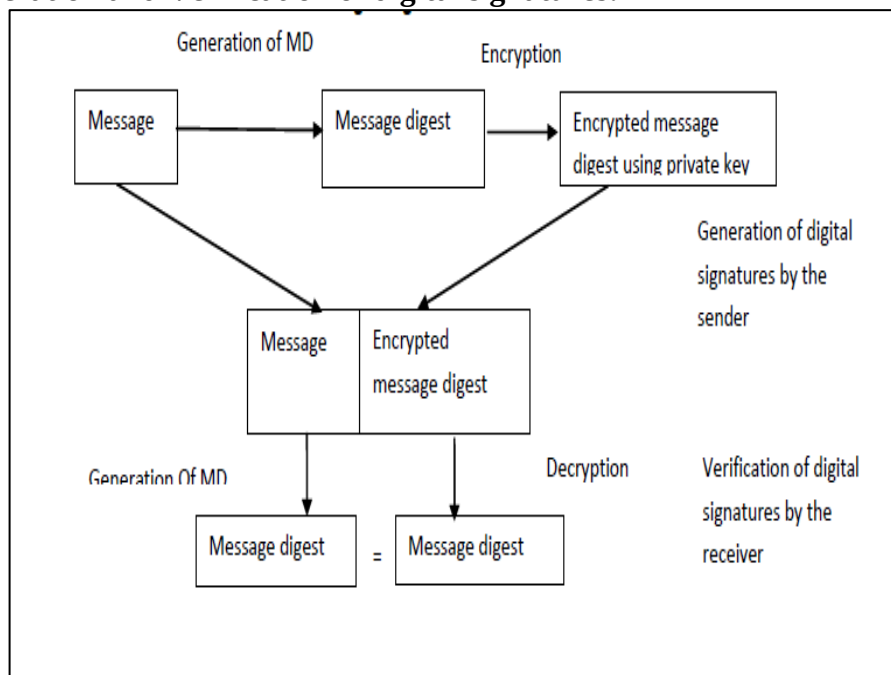
a. Signing part

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.

Generation and Verification of digital signatures:



Procedure:

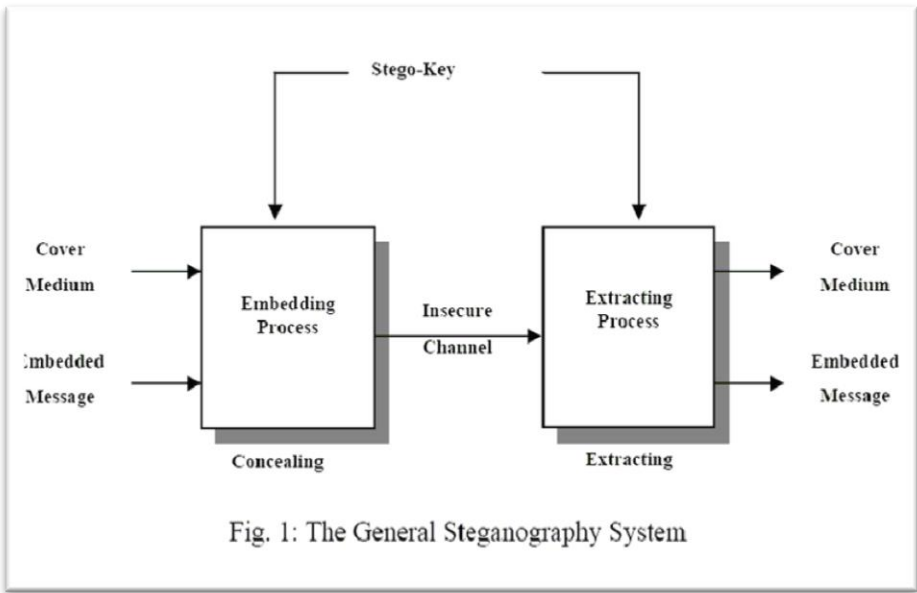
1. Message digest is used to generate the signature. The message digest (MD) is calculated from the plaintext or message.

2. The message digest is encrypted using user's private key.

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

4. The receiver calculates the message digest from the plain text or message he received.

5. Receiver decrypts the encrypted message digest using the sender's public key. If both the MDs are not same then the plaintext or message is modified after signing.

c	What is steganography? List terminologies used in steganography.	4 M
Ans	• 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. • 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. • In modern steganography, data is first encrypted 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.  The diagram illustrates the general steganography system. It consists of two main processes: the Embedding Process (labeled 'Concealing') and the Extracting Process (labeled 'Extracting'). The Embedding Process takes a 'Cover Medium' and an 'Embedded Message' as inputs and produces a 'Stego-Medium'. The Extracting Process takes the 'Stego-Medium' as input and produces the 'Cover Medium' and the 'Embedded Message'. Both processes use a 'Stego-Key' for encryption/decryption. The communication between the two processes is labeled 'Insecure Channel'. Fig. 1: The General Steganography System Steganography process: Cover-media + Hidden data + Stego-key = Stego-medium • 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. • Stenography 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. • Stenography has a number of drawbacks when compared to encryption. It requires a lot of overhead to hide a relatively few bits of information. (Consider any other relevant diagram) Terminologies of steganography • Carrier or Cover File - A Original message or a file in which hidden information will be stored inside of it.	Explanation 2M, 1M Diagram, 1M List Terminology

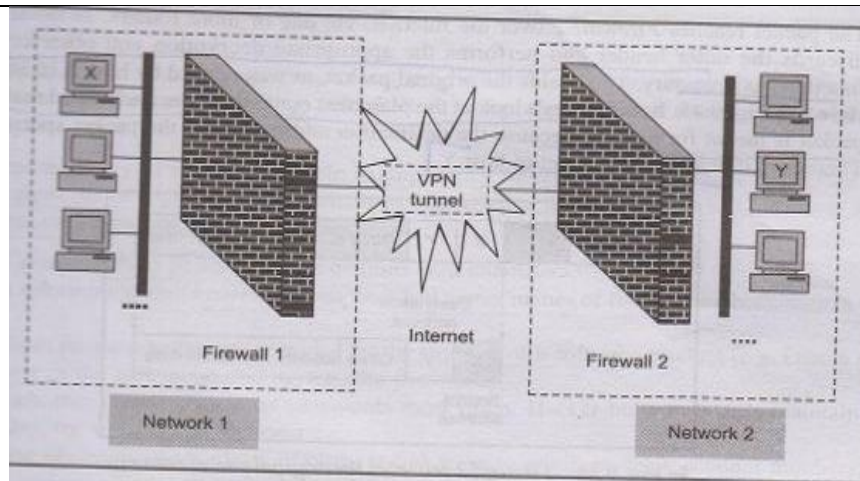


MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

		• Stego-Medium - The medium in which the information is hidden. • Embedded or Payload - The information which is to be hidden or concealed. • Steganalysis - The process of detecting hidden information inside a file.	
	d	Explain the importance of “Intellectual property” rights is cyber crime.	4 M
	Ans	Intellectual proper is a generic term for legal entitlements attached to certain names, written and recorded media and inventions. The holders of these legal entitlements may exercise various exclusive rights in relation to the subject matter of the intellectual property. The word intellectual indicates the fact that this term concerns a process of the mind. The property implies that ideation is analogous to the construction of tangible objects. Intellectual property law and enforcement vary widely from jurisdiction to jurisdiction. Intellectual property laws confer a bundle of exclusive rights in relation to the particular form or manner in which ideas or information are expressed or manifested, and not in relation to the ideas or concepts themselves. The term intellectual property denotes the specific legal rights that authors, inventors and other intellectual property holders may hold and exercise and not the intellectual work itself. Intellectual property laws are designed to protect different forms of subject matter, although in some cases there is a degree of overlap: 1. Copyrights 2. Patents 3. Trademark 4. Trade Secret 5. Trade Name 6. Domain Name. Traditionally, businesses have thought of their physical assets, such as land, buildings, and equipment as the most important. Increasingly, however, a company’s intellectual assets are the most important.	4M Explanation
	e	Explain “virtual private network” with neat diagram.	4 M
	Ans	A VPN is a mechanism of employing encryption, authentication, and integrity protection so that we can use a public network as if it is a private network. 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 VPN approach. In such case we set up two firewalls, Firewall 1 and Firewall 2. The encryption and decryption are performed by firewalls. Network 1 connects to the Internet via a firewall named Firewall 1 and Network 2 connects to the Internet with its own firewall, Firewall 2.	2M diagram, 2M explanation



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)



Working Let us assume that host X on Network 1 wants to send a data packet to host Y on Network 2.

- 1) 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.
- 2) The packet reaches Firewall 1. Firewall 1 now adds new headers to the packet. It changes the source IP address of the packet from that of host X to its own address (i.e. IP address of Firewall 1, F1).
- 3) It also changes the destination IP address of the packet from that of host Y to the IP address of Firewall 2, F2. It also performs the packet encryption and authentication, depending on the settings and sends the modified packet over the Internet
- 4) The packet reaches to firewall 2 over the Internet, via routers. Firewall 2 discards the outer header and performs the appropriate decryption. It then takes a look at the plain text contents of the packet and realizes that the packet is meant for host Y. It delivers the packet to host Y Diagram (1 marks)