**MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION**
**(Autonomous)**
**(ISO/IEC - 27001 - 2005 Certified)**

## *MODEL ANSWER*

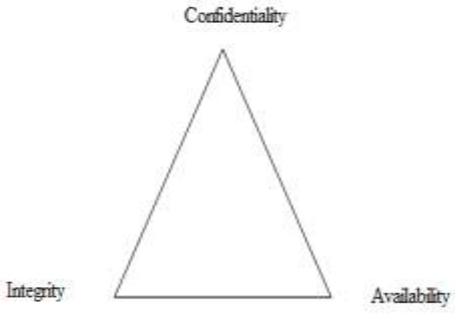
**SUMMER - 2017 EXAMINATION**

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

**Important Instructions to examiners:**

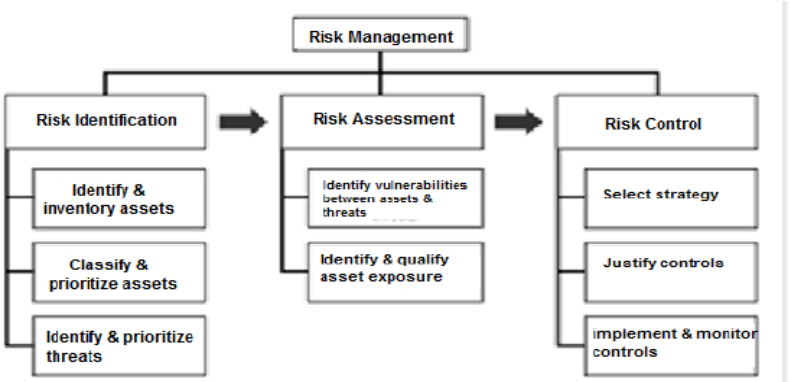
1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given moreImportance (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** |
| | **(1)** | **Define security. State need of security.** | **4M** |
| | Ans. | **Security**: 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. | ***Definition 1M*** |
| | | **Need of Security:**<br>• **Security protecting the Functionality of an Organization.**<br>General Manager and IT Manager are responsible for implementing information security that protects the functionality of an organization. Implementing information security has more to do with management then technology.<br>For e.g. Managing payroll has more to do with management then Calculating wages, other things etc.<br>• **Enabling the safe operation of application.** | ***Any 3 Needs 1M each*** |

| | | | |
|---|---|---|---|
| | | Today organization operates on integrated efficient and capable applications. A modern organization need to create an environment that safeguards these applications, specially operating system platform, email, instant messaging application etc.<br>• **Protecting data that organization use and collect.**<br>Without data an organization losses its records of transaction and ability to deliver a value to its customer. Protecting data at motion and at rest are both critical aspects of information security. The value of data motivates attackers to steal and corrupt the data.<br>• **Safeguarding technology assets in organization.**<br>To perform effectively, organizations must employ secure infrastructure service which appropriate to the size and the scope of the organization. For e.g. a small business uses an email service and secure with the personal encryption tool. When an organization grows, it must develop additional security service that uses system of software, encryption methodology and legal agreement that support entire information infrastructure. | |
| | **(2)**<br>Ans. | **Draw and explain CIA Triad.**<br>Three pillars of information security referred as CIA triad stands for :<br>1) Confidentiality<br>2) Integrity<br>3) Availability<br> <br>**1) Confidentiality:**<br>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. | **4M**<br>***Diagram 1M***<br>***Explanation 1M each*** |

| | | | |
|---|---|---|---|
| | | **2) Integrity:**<br>The concept of integrity ensures that<br>i. Modifications are not made to data by unauthorized person or processes.<br>ii. Unauthorized modifications are not made to the data by authorized person or processes.<br>iii. The data is internally and externally consistent.<br><br>**3) Availability:**<br>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. | |
| | **(3)**<br>Ans. | **What is cryptography? State its applications.**<br>**Cryptography:** It is the art and science of achieving security by encoding messages to make them non-readable.<br><br>**Application of cryptography**:<br>• **Data Hiding:** The original use of cryptography is to hide something that has been written.<br>• **Digitally Code:** Cryptography can also can be applied to software, graphics or voice that is, it can be applied to anything that can be digitally coded.<br>• **Electronic payment:** When electronic payments are sent through a network, the biggest risk is that the payment message will alter or bogus messages introduced and the risk that someone reads the messages may be minor significance.<br>• **Message Authentication:** One cannot entirely prevent someone from tampering with the network and changing the message, but if this happens it can certainly be detected. This process of checking the integrity of the transmitted message is often called message authentication. The most recent and useful development in the uses of cryptography is the digital signature. | **4M**<br>***Definition 1M***<br><br>***Any three applications 1M each*** |
| | **(4)** | **With respect to information security define the following:**<br>**(a) Security policies**<br>**(b) Standards**<br>**(c) Guidelines** | **4M** |

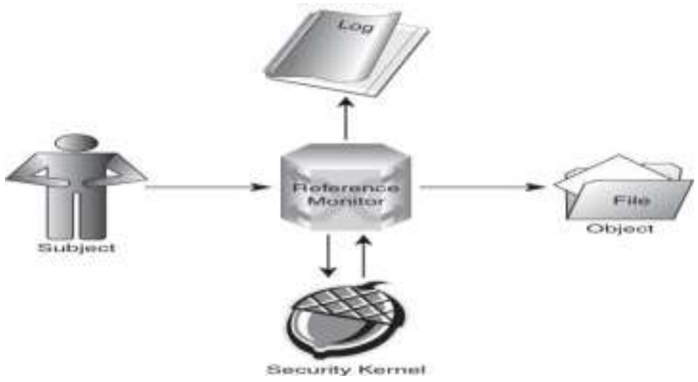
| | | | |
|---|---|---|---|
| | Ans. | **1) Security policy:** An information security policy consists of higher level statements relating to the protection of information across the business and should be produced by senior management. The policy outlines security roles and responsibilities, defines the scope of information to be protected, and provides a high level description of the controls that must be in place to protect information.<br><br>**2) Standard:** Standard consists of specific low level mandatory controls that help enforce and support the information security policy.<br>Standard helps to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or software.<br>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.<br><br>**3) Guidelines:**<br>It should consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.<br>It should view as best practices that neither are nor usually requirements, but are strongly recommended.<br>It can be consisting of additional recommended controls that support a standard or help to fill in the gaps where no specific standard applies.<br>A standard may require specific technical controls for accessing the internet securely and separate guidelines may be outline the best practices for using it. | ***Security Policy 1M***<br>***Standard and guidelines 1½M each*** |
| **1.** | **(B)**<br>**(1)**<br>Ans. | **Attempt any ONE of the following:**<br>**What is information classification? Explain the terms for information classification.**<br>**Definition of Information classification:**<br>Classification of information is used to prevent the unauthorized disclosure and the resultant failure of confidentiality<br>**Terms for information classification:**<br>**1. Unclassified**<br>Information that is neither sensitive nor classified. The public release of this information does not violet confidentiality.<br>**2. Sensitive but Unclassified (SBU)** | **6**<br>**6M**<br>***Definition 1M***<br>***Each term 1M*** |

| | | | |
|---|---|---|---|
| | | Information that has been designated as a minor secret but may not create serious damage if disclosed.<br>**3. Confidential**<br>The unauthorized disclosure of confidential information could cause some damage to the country's national security.<br>**4. Secret**<br>The unauthorized disclosure of this information could cause serious damage to the countries national security.<br>**5. Top secret**<br>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. | |
| | **(2)**<br><br>Ans. | **Define Risk Management. Explain components of risk management.**<br>**Risk Management:-**<br>The process of identifying, assessing, and responding to risk.<br>OR<br>The process of identifying risk, as represented by vulnerabilities, to an organization's information assets and infrastructure, and taking steps to reduce this risk to an acceptable level.<br>Risk management involves three major undertakings:<br>Risk identification,<br>Risk assessment,<br>Risk control.<br><br>The various components of risk management and their relationship to each other are shown in Figure<br> Risk Management<br>Risk Identification<br>Risk Assessment<br>Risk Control<br>Identify & inventory assets<br>Classify & prioritize assets<br>Identify & prioritize threats<br>Identify vulnerabilities between assets & threats<br>Identify & qualify asset exposure<br>Select strategy<br>Justify controls<br>implement & monitor controls | **6M**<br><br>***Definition 1M***<br><br>***Diagram 2M*** |

| | | | |
|---|---|---|---|
| | | **Risk identification** is the examination and documentation of the security posture of an organization‘s information technology and the risks it faces.<br><br>**Risk assessment** is the determination of the extent to which the organization‘s information assets are exposed or at risk.<br><br>**Risk control** is the application of controls to reduce the risks to an organization‘s data and information systems.<br>Risk can be calculated by using Risk Analysis which is of two types:<br>a) Quantitative Risk Analysis: A Process of assigning a numeric value to the probability of loss based on known risks, on financial values of the assets and on probability of threats.<br>b) Qualitative Risk Analysis: A collaborative process of assigning relative values to assets, assessing their risk exposure and estimating the cost of controlling the risk. | ***Explanation 3M*** |
| **2.** | **(a)**<br>Ans. | **Attempt any TWO of the following:**<br>**Explain the concept of TCB. Describe rings of trust in Standalone system.**<br>**Trusted Computing Base (TCB):**<br>• The trusted computing base (TCB) is the sum total of all software and hardware required to enforce security.<br>• TCB refers to all of hardware, the core OS that is involved in protection, and all programs that operate with system privileges.<br>• Desirable properties are Small, Separable, well-defined, Independently-auditable Reference Monitor.<br>• A reference monitor is a separable module that enforces access control decisions<br>• All sensitive operations are routed through the reference monitor<br>• The monitor then decides if the operation should proceed.<br>• It stands 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.<br>• In Unix/Linux security kernel acts as a Reference Monitor which will handle all user application requests for access to system resources.<br>• In trusted system Object is something that people want to access.<br>• These objects (data) are labeled according to their level of | **16**<br>**8M**<br><br>***TCB 4M*** |

sensitivity.

- Subjects (users) should have same level of classification while accessing object.
- The reference monitor has three properties:
- It cannot be bypassed and controls all access.
- It cannot be altered and is protected from modification or change.
- It can be verified and tested to be correct.



**Rings of Trust:**

Fig shows the rings of trust concept in the context of a single computer system. In this model, outer rings contain a lower level of security, and systems requiring higher levels of security are located inside the inner rings. Extra security mechanisms must be navigated to move from an outer ring into an inner ring. The operating system (OS) enforces how communications flow between layers using the reference monitor (within the kernel) to mediate all access and protect resources.

***Rings of trust explanation 2M***

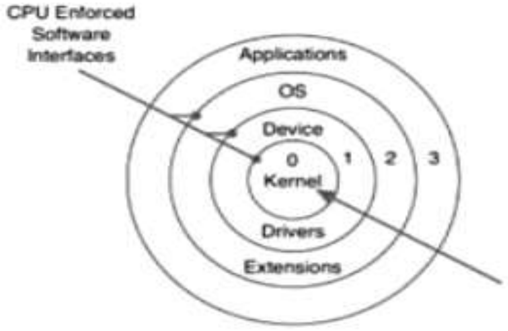


***Diagram 2M***

**(b)** **Consider the plain text “I am Rahul” convert given plain text into Cipher text using Playfair Cipher Cryptography with key as “Playfair example”. Write step-by-step procedure.** **8M**

Ans. **Playfair cipher steps:**

Given Plain text :“I am Rahul”

Key :“Playfair Example”

1. **Creation of the matrix:**
   a. Enter keyword “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. Compbine 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.

***Creation of Matrix 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 |

**2. Encryption Process:**

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.

***Encryption 1M each pair***

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 |

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)

| | | | | |
|---|---|---|---|---|
| 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 |

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.**

| | | | | |
|---|---|---|---|---|
| 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 |

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)

| | | | | |
|---|---|---|---|---|
| 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 |

Thus, the plain text blocks IA MR AH UL becomes **EP IE FD LR.**

**(c)** **Explain the following:** **8M**

**(1) Software priacy**

**(2) Copyright**

**(3) Patent**

**(4) Trademark**

Ans. 1) **Software Piracy:**

- 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.

***Each 2M***

- 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.

2) **Copyright:**

- This law is to keep control on use of the creations in a number of ways.
- These uses include making copies, issuing copies to public, public performance of the creation, broadcasting and online use.
- It also gives moral rights to be identified as the creator of those materials and protection against the distortion or modification.
- The purpose of this law is to gain economic rewards for the efforts.
- This encourages future creativity, development of new material.
- However, copyright law does not protect ideas, names, titles.
- Copyright can be considered as a kind of property, which like a person's physical assets, can be bought, sold or inherited, transferred.
- It can either Authorize or prohibit Translation into other languages. Examples.. Literary, musical, dramatic, artistic, films etc
- This law in India has 15 chapters, with terms, definitions, ownership, terms of copyrights etc.

3) **Patent**:

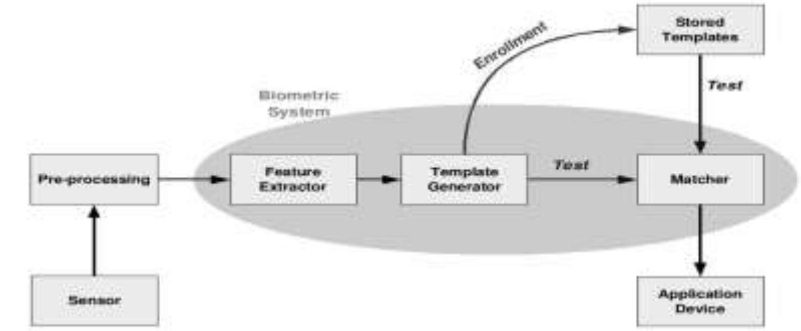
- This is a Legal right granted for limited time, as a monopoly, to owner by a country.
- Patents can be over ruled by health and safety regulation

| | | | |
|---|---|---|---|
| | | • Patents can be given away, sold, inherited, licensed away and can be abandoned.<br>• A patent gives an inventor the right, for a limited period, to stop others from making, using and selling or importing an invention without seeking the permission of the inventor. And hence called “Negative right”.<br>• Mostly concerned with technical and functional aspects.<br>• Patents lasts up to 20 years in India and most countries outside.<br>• An Indian patent is not effective outside India (territorial)<br>• Apply to The Indian Patent Office for patenting in India. Patent Agents are also available.<br><br>4) **<u>Trademarks</u>:**<br>A trademark is sign that distinguishes the goods and services of one trader from another. Signs include Slogans, Words, Logos, Colours, 3-D shapes, Sounds, Gestures. This is considered as “Badge” of Trade origin. It can be used as Marketing tool.<br>**<u>Features:</u>**<br>• Service Marks: Marks used by service industry.<br>• Well Known Marks: Which are defined and cannot be registered or used.<br>• Collective Marks : Used by Group of companies<br>• Scope of registration: Unauthorized use of certain marks used for certain class used by others are prohibited.<br>• Punishment if copied<br>• Renewed every 10 years<br>• License agreements need not be compulsorily registered.<br>• Trademarks can include colors and shape of the product also. | |
| **3.** | | **Attempt any FOUR of the following:** | **16** |
| | (a) | **Explain the following terms:**<br>**(1) Data obfuscation**<br>**(2) Event classification** | **4M** |
| | Ans. | **(1) Data obfuscation:**<br>1. Data obfuscation involves protection of sensitive information with technique other than encryption.<br>2. Data obfuscation is one of the solutions for data theft. Obfuscate means to make the data unclear.<br>3. It is an effective method which involves chopping the text into | ***Data obfuscation 2M*** |

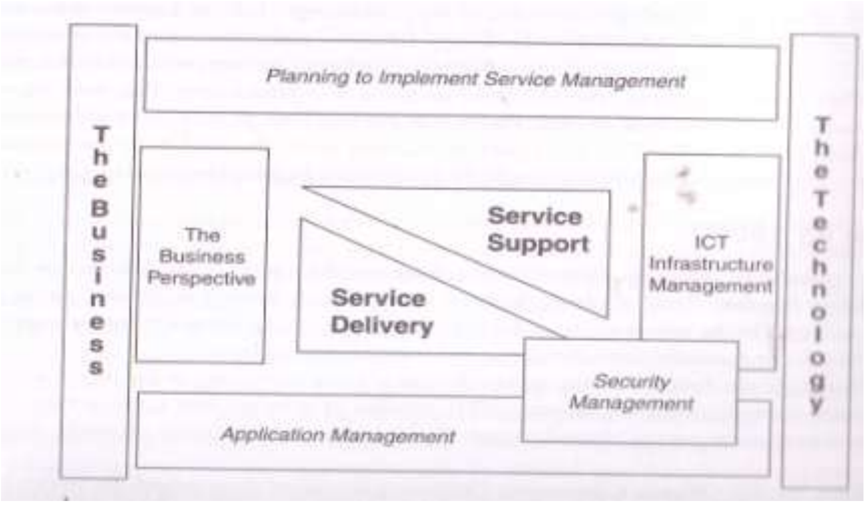
| | | | |
|---|---|---|---|
| | | segments and re-arranging it.<br>4. Sometimes data is obfuscated by using a simple substitution cipher.<br>A good example of data obfuscation would be an audit report on a medical system. In this report only required field of patients are disclosed to the auditor. Details which are not required such as patient's contact no and address are made obfuscate.<br><br>**(2) Event classification:**<br>Following are the events that can damage information security.<br>1) **Disaster:** It causes permanent and considerable harm to the assets and of an organization like hardware, information, property, staff, services etc.<br>2) **Crises:** It leads to an unstable and abnormal situation causes extra ordinary high risk of organization.<br>3) **Catastrophe**: It is large scale disaster leads to damage of critical equipment in processing. | ***Event Classification2M*** |
| | **(b)**<br>Ans. | **Describe ITSEC.**<br>**ITSEC:** Information Technology Security Evaluation Criteria.<br><br>1. ITSEC focuses more on integrity and availability. It tries to provide a uniform approach to product and system.<br>2. ITSEC will also provide security targets like:<br>i. Policy for system security<br>ii. Required mechanism for security<br>iii. Required rating to claim for minimum strength<br>iv. Level for evaluating targets –functional as well as evaluation<br><br>ITSEC classes contain hierarchical structure where every class will be added to the class above it. **This class contains some particular function**.<br>F-IN This class will provide high integrity.<br>F-AV This class will provide high availability.<br>F-DI This class will provide high data integrity.<br>F-DX This class is used for networks. Of provide high integrity while exchanging data in networking.<br><br>**ITSEC uses following I classes from E0 to E6 to evaluate the security.** | **4M**<br><br>***Accurate description along with 4 classes 4M*** |

| | | | |
|---|---|---|---|
| | | E0 – Minimal protection.<br>E1 – Security target and informal architecture design must be produced.<br>E2 – An informal detail design and test document must be produced.<br>E3 – Source code or hardware drawing to be produced. Correspondence must be shown between source codes of detailed design.<br>E4 – Formal model of Security and Semi – formal specification of Security function architecture and detailed design to be produced.<br>E5 – Architecture design explain the inter relationship between security<br>component.<br>E6 – Formal description of architecture and Security function to be produced.<br>• Information could leak from those users who were cleared to see it, down to those users who are not.design must be produced.<br>• E2 – An informal detail design and test document must be produced.<br>• E3 – Source code or hardware drawing to be produced. Correspondence must be shown between source codes of detailed design.<br>• E4 – Formal model of Security and Semi – formal specification of Security function architecture and detailed design to be produced.<br>• E5 – Architecture design explain the inter relationship between security component.<br>• E6 – Formal description of architecture and Security function to be produced. Information could leak from those users who were cleared to see it, down to those users who are not. | |
| | **(c)**<br>Ans. | **Define Hacking. Explain different types of Hackers.**<br>**Hacking:** Hacking refers to the unauthorized access of another computer system. It is the practice of modifying features of assistant in order to accomplish a goal outside of the creatures original purpose.<br><br>**There are different types of Hackers:**<br>**1. White Hat:** This type of hackers is someone who has non-malicious purpose whenever he breaks into security systems. In fact, a large number of white hat hackers are security experts themselves | **4M**<br><br>***Definition 1M***<br><br>***Any 3 types of*** |

| | | | |
|---|---|---|---|
| | | who want to push the boundaries of their own IT security ciphers and shields or event, penetration testers specifically hired to test out how vulnerable or impenetrable (at the time) a present protective setup currently is. A white hat that does vulnerability assessments and penetration tests is also known as an ethical hacker.<br><br>**2. Black Hat:** This type of hackers is also known as a cracker and he Has a malicious purpose whenever he goes about breaking into computer security systems with the use of technology such as a network, telecommunication system, or computer and without authorization. His malicious purposes can range from all sorts cybercrimes such as piracy, identity theft, credit card fraud, damage, and so forth. He may or may not utilize questionable tactics such as deploying worms and malicious sites to meet his ends.<br><br>**3. Grey Hat:** A grey hat hacker is a combination of both white hats And black hats. This is the kind of hacker that is not a penetration tester but will go ahead and surf the Internet for vulnerable systems he could exploit. Like a white hat, he will inform the administrator of the website of the vulnerabilities he found after hacking through the site. Like a black hat and unlike a pen tester, he will hack any site freely and without any prompting or authorization from owners what so ever. He will even offer to repair the vulnerable site he exposed in the first place for a small fee.<br><br>**4. Elite Hacker:** As with any society, better than average people are rewarded for their talent and treated as special. This social status among the hacker underground, the elite are the hackers among hackers in this subculture of sorts. They are the masters of deception that have a solid reputation among their peers as the cream of the hacker crop.<br><br>**5. Script Kiddie:** A script kiddie is basically an part-time or non-expert hacker, who breaks into people’s computer systems not through his knowledge in IT security and the ins and outs of given website, but through the prepackaged automated scripts (hence the name), tools, and software written by people who are real hackers, unlike him. He usually has little to know knowledge of the underlying concept behind how those scripts he has on hand works. | ***Hackers 3M*** |

| | | | |
|---|---|---|---|
| | **(d)**<br>Ans. | **What is Biometric Access Control? Explain with diagram.**<br>Biometrics refers to metrics related to human characteristics and traits. Biometrics authentication is used in computer science as a form of identification and access control.<br><br> Stored Templates<br>Enrollment<br>Test<br>Biometric System<br>Pre-processing<br>Feature Extractor<br>Template Generator<br>Test<br>Matcher<br>Sensor<br>Application Device<br>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.<br>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.<br>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.<br>4. The first time an individual uses a biometric system is called | **4M**<br>***Relevant explanation with correct diagram 4M*** |

| | | | |
|---|---|---|---|
| | | 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.<br>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.<br>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)**<br>Ans. | **Describe ITIL framework.**<br>The Information Technology Infrastructure Library (ITIL) is a collection of best practices in IT service management (ITSM), and focuses on the service processes of IT and considers the central role of the user. It was developed by the United Kingdom's Office of Government Commerce (OGC). Since 2005, ITIL has evolved into ISO/IEC 20000, which is an international standard within ITSM.<br>An ITIL service management self-assessment can be conducted with the help of an online questionnaire maintained on the website of the IT Service Management Forum. The self-assessment questionnaire helps evaluate the following management areas:<br>a) Service Level Management<br>b) Financial Management<br>c) Capacity Management<br>d) Service Continuity Management | **4M**<br>***Description 2M*** |

| | | | |
|---|---|---|---|
| | | e) Availability Management<br>f) Service Desk<br>g) Incident Management<br>h) Problem Management<br>i) Configuration Management<br>j) Change Management<br>k) Release Management<br><br> Planning to Implement Service Management<br>The Business<br>The Business Perspective<br>Service Support<br>Service Delivery<br>ICT Infrastructure Management<br>Security Management<br>Application Management<br>The Technology | ***Correct diagram 2M*** |
| **4.** | **(A)**<br>**(1)**<br>Ans. | **Attempt any THREE of the following:**<br>**Explain BIBA Integrity Model.**<br><br>**Integrity Model:**<br>The BIBA Model<br>It focuses on commercial sector where, data integrity is more important than confidentiality.<br>Integrity is the protection of system data from intentional or accidental unauthorized changes.<br>Although the security program cannot improve the accuracy of data, it can help to ensure that any changes are intended and correctly applied.<br><br>Additional element of integrity is the need to protect the process and program used to manipulate the data from unauthorized modification. | **12**<br>**4M**<br><br>***Explanation 4M*** |

| | | | |
|---|---|---|---|
| | | **The BIBA model has following three properties:**<br>1. Simple Integrity Property: - Data can be read from higher integrity level.<br>2. Star Integrity property: - Data can be written to lower integrity level.<br>3. Invocation Property: - User cannot request services from higher integrity level.<br>BIBA is the opposite of BLP where BLP is a WURD model (write up, read down), BIBA is RUWD model (Read up, write down) | |
| | (2)<br>Ans. | **List any four authentication protocols for security and explain any one.**<br>**Authentication Protocols List:**<br>1) CHAP (Challenge Handshake Authentication Protocol)<br>2) EAP (Extensible Authentication Protocol)<br>3) PAP (Password Authentication Protocol)<br>4) SPAP (Shiva Password Authentication Protocol)<br>5) DES (Data Encryption Standard)<br>6) RADIUS (Remote Authentication Dial-In User Service Protocol)<br>7) S/KEY<br>8) TACACS (Terminal Access Controller Access Control System)<br>9) MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)<br>10) SKID (SKID2 and SKID3) -Secrete Key Identification Protocols.<br>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 identify by using 3-way handshaking and by using shared secrete<br>• 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.<br>• Server compares the response i.e. hash value with its own calculated hash value.<br>• If the value matches, then the authentication is acknowledged or else the connection is terminated. | **4M**<br>***List of any four protocols 2M***<br>***Explanation of any one 2M*** |

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 sis 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.

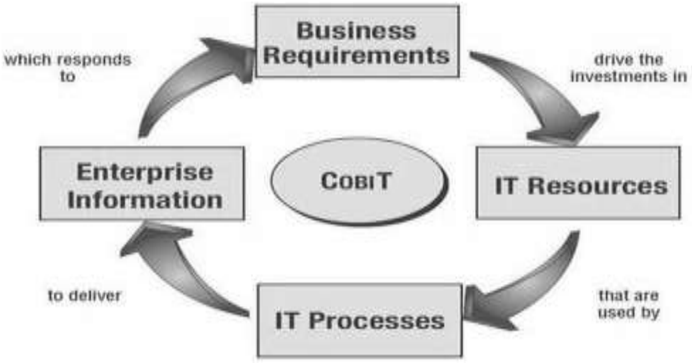
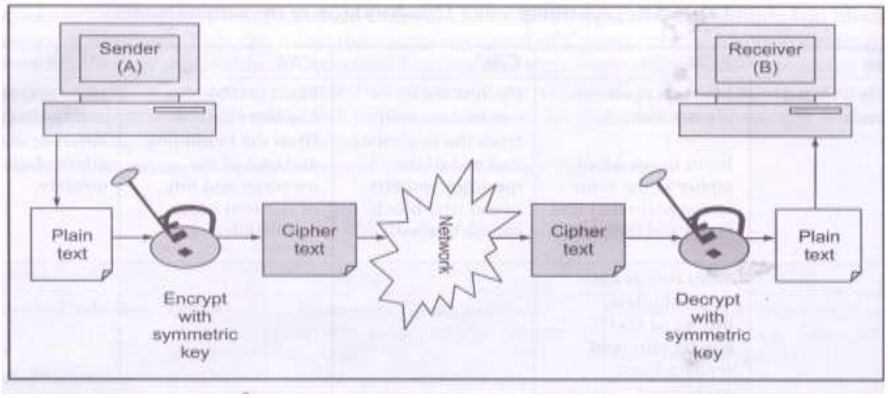
5) **DES:** It is a Data Encryption Standard (DES) is the classic among the symmetric block cipher algorithms. DES was developed in the 1970s as a US-government standard for protecting non-classified information. DES encrypts 64-bit clear-text blocks under the control of 56-bit keys. Each key is extended 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.<br>7) **S/KEY:** It is a one-time password system developed for operating systems like UNIS. 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.<br>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.<br>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.<br>10) **SKID (SKID2 and SKID3):** SKID2 and SKID3 are secrete key identification protocols. SKID2 provides unilateral entity authentication whereas SKID3 provides mutual entity authentication. | |
| | **(3)**<br><br><br>Ans. | **Explain the following with their usage:**<br>**(a) Single sign-on**<br>**(b) Kerberos**<br>**(a) Single sign-on:**<br>• Single sign-on is the ability for a user to enter the same Id and Password to Log on to multiple applications with an enterprise.<br>• Once logged in user can switch from one system to the next without logging in again.<br>• It can work between enterprise using federated authentication.<br>For example: A business partner employee may successfully log on to their enterprise system.<br>• It can work between federated authentication and employee.<br>For example: An employee who is trying to access your outsource | **4M**<br><br><br><br>***Single sign-on 2M*** |

| | | | |
|---|---|---|---|
| | | benefits supplier to update their benefits information would click on the benefits link on your intranet.<br>• To create a PIN vault, managing Id and Password.<br><br>**(b) Kerberos:**<br>• Kerberos is a network authentication protocol and it is designed to provide strong authentication for Client /Server Applications. It uses secret- key Cryptography.<br>• 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. | ***Kerberos 2M*** |
| | **(4)**<br>Ans. | **Describe COBIT framework.**<br>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.<br><br>COBIT 4.1 consists of 7 sections, which are<br>1) Executive overview,<br>2) COBIT framework,<br>3) Plan and Organize,<br>4) Acquire and Implement,<br>5) Deliver and Support,<br>6) Monitor and Evaluate, and<br>7) Appendices, including a glossary.<br><br>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. | **4M**<br><br>***Correct description 2M*** |

| | | | |
|---|---|---|---|
| | | <br> Business Requirements<br>drive the investments in<br>IT Resources<br>that are used by<br>IT Processes<br>to deliver<br>Enterprise Information<br>which responds to<br>COBIT<br><br>**Services provided by the COBIT:**<br>1. Manage operations<br>2. Manage service request and incidence<br>3. Manage problems<br>4. Manage continuity<br>5. Manage security services<br>6. Manage business process control | *Diagram 2M* |
| **4.** | **(B)**<br>**(1)**<br><br>Ans. | **Attempt any ONE of the following:**<br>**What is symmetric encryption? Explain the components of symmetric encryption.**<br>**Symmetric encryption:**<br>1. In symmetric key cryptography only one key is used and the same key is used for both encryption and decryption of messages.<br><br><br> Sender (A)<br>Receiver (B)<br>Plain text<br>Encrypt with symmetric key<br>Cipher text<br>Network<br>Cipher text<br>Decrypt with symmetric key<br>Plain text | **6**<br>**6M**<br><br>***Symmetric encryption 2M***<br><br>***Diagram 2M*** |

| | | | |
|---|---|---|---|
| | | 2. It is also referred to as Secret Key Cryptography or Private Key Cryptography<br>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.<br>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.<br>5. The most widely used symmetric ciphers are DES and AES.<br><br>**The symmetric encryption scheme has five components:**<br>**1. Plaintext:** This is the original intelligible message or data that is fed to the algorithm as input.<br>**2. Encryption algorithm:** The encryption algorithm performs various substitutions and permutations on the plaintext<br>**3. Secret Key:** The secret key is also input to the encryption algorithm. The exact substitutions and permutations performed depend on the key used, and the algorithm will produce a different output depending on the specific key being used at the time.<br>**4. Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the key. The ciphertext is an apparently random stream of data, as it stands, is unintelligible.<br>**5. Decryption Algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext | ***Components 2M*** |
| | **(2)**<br><br>Ans. | **List the different data recovery tools and explain any two data recovery tools.**<br>**Following are the data recovery tools:**<br>1. NTFS Data recovery tools<br>2. FAT data recovery tool<br>3. Digital Camera Data recovery tool<br>4. Removable media data recovery tool<br><br>**Data Recovery Tools:**<br><br>**1. NTFS Data Recovery Tools:**<br>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.<br>*Example*: - Diskinternal's NTFS Data Recovery tool. The tool | **6M**<br><br>***List of data recovery tools 2M*** |

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

***Any two data recovery tools each 2M***

**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:

- 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

| | | | |
|---|---|---|---|
| **5.** | | **Attempt any TWO of the following:** | **16** |
| | **(a)** | **Consider the plain text “COMP” and key as “Hill”, convert given plain text into cipher text using Hill Cipher. Write step-by-step procedure.** | **8M** |
| | Ans. | 1. In the above example<br>Plain text = COMP<br>key = HILL<br>Matrix = 2x2<br>2. Turn the keyword in to matrix<br>$\begin{pmatrix} H & I \\ L & L \end{pmatrix}$<br>3. Convert the keyword in to key matrix, convert each letter in to number by its position in alphabet like A = 0, B = 1, C = 2 etc.<br>$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$<br>4. Now split the plain text and write this as a column vectors.<br>$\begin{pmatrix} C \\ O \end{pmatrix} \begin{pmatrix} M \\ P \end{pmatrix}$<br>5. Next step to convert the plain text column vectors in a same way that we converted the keyword in to the key matrix. Each letter is replaced by appropriate number.<br>$\begin{pmatrix} 2 \\ 14 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix}$<br>6. Now perform matrix multiplication write key matrix with first column vector.<br>$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 2 \\ 14 \end{pmatrix} = \begin{pmatrix} 126 \\ 176 \end{pmatrix}$ | ***Procedure-4M***<br>***Correct calculated Answer 4M*** |

Matrix multiplication will be,
(7 x 2) + (8x14) = 14+ 112 = 126
(11x2) + (11x14) = 22 + 154 = 176

7. Same procedure is followed to remaining plain text.

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 204 \\ 297 \end{pmatrix}$$

Matrix multiplication will be,
(7 x 12) + (8x15) = 84+ 120 = 204
(11x12) + (11x15) = 132 + 165 = 297

8. Next take modulo 26 of each of resultant column vector.

$$\begin{pmatrix} 126 \\ 176 \end{pmatrix} \bmod 26 = \begin{pmatrix} 22 \\ 20 \end{pmatrix}$$

$$\begin{pmatrix} 204 \\ 297 \end{pmatrix} \bmod 26 = \begin{pmatrix} 22 \\ 11 \end{pmatrix}$$

9. Now, Convert 22 and 20 into letters ‘W’ and ‘U’ respectively.

$$\begin{pmatrix} 22 \\ 20 \end{pmatrix} = \begin{pmatrix} W \\ U \end{pmatrix}$$

Same procedure is for remaining plain text.

$$\begin{pmatrix} 22 \\ 11 \end{pmatrix} = \begin{pmatrix} W \\ L \end{pmatrix}$$

Hence, the plaintext ‘COMP’ and keyword ‘HILL’ then the Cipher text is “WUWL”

| | | | |
|---|---|---|---|
| | **(b)** | **Explain the following:**<br>**(1) Deleted file Recovery**<br>**(2) Formatted Partition Recovery** | **8M** |
| | Ans. | **(1) Deleted file recovery:**<br>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.<br>**Deleted file recovery**<br>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.<br>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.<br>*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.<br>Every computer file is a set of binary data i.e. in forms of ls and Os. 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.<br>*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 he 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 systems speed. Thus, it also involves a lot of over-writing on available space (where your deleted files may be). | ***Deleted file recovery 4M*** |

| | | | |
|---|---|---|---|
| | | 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 recover software.<br>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.<br>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.<br><br>**(2) Formatted Partition Recovery:**<br>If the hard drive is formatted, then people generally use a bootable CD to start the system. But if the system is booted and installed something like an operating system, on the formatted drive then there is more chances of losing the data forever. Formatting is to add deletion mark on all files or even empty FAT and system couldn't identify any content of disk partition. Formation nevertheless doesn't perform any operation upon data. Though directory is empty, data still exists. By utilizing data recovery software, user could retrieve all those data. Partition damage could probably render users considerable losses not only in terms of data, but economically also. Partition data loss is likely to bring about tens of millions of economic loss for user. Therefore, user should attach great attention on data protection while using computer. To recover files from a formatted drive through data recovery software is not a very complicated process, but it can be lengthy, and will need:<br>1. An enclosure (to convert hard drive into USB external drive).<br>2. A bootable system with preferably a high storage capacity hard drive.<br>3. A disk image creator and a virtual disk creator.<br>4. Data recovery software.<br>5. Sufficient storage space on devices other than the formatted drive. | ***Formatted Partition recovery 4M*** |
| | (c)<br><br><br><br><br>Ans. | **Explain the following w.r.t. to security:**<br>**(1) Identification**<br>**(2) Authentication**<br>**(3) Authorization**<br>**(4) Access Control** | **8M** |

| | | | |
|---|---|---|---|
| | | **(1) Identification:**<br>Identification is the first step in any access control solution. It is the process of identifying the user to verify whether he/she is what he/she claims to be. Normally, identification is done with the help of information that is known to everyone (i.e., user name or user ID) and some personal information known only to the subject (i.e. password). Faced with the threat of identity theft and increasing consequences associated with failing to secure information, enterprises are increasingly looking for stronger forms of authentication to enhance their overall security capabilities.<br><br>**(2) Authentication:**<br>Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. -To access most technology services of Indiana University, you must provide such proof of identity.<br>In private and public computer networks (including the Internet), authentication is commonly done through the use of login passwords or passphrases; knowledge of such is assumed to guarantee that the user is authentic. -Thus, when you are asked to "authenticate" to a system, it usually means that you enter your username and/or password for that system.<br>Authentication technique depending upon the nature of the business and sensitivity of the information. One has to consider various authentication methods and their pros and cons. The means of authentication are often discussed in terms of ―factors of proof, such as:<br>● Something you know to prove your identity (e.g., a PIN)<br>● Something you have to prove your identity (e.g., a smart card)<br>● Something you are to prove your identity (e.g., a fingerprint) A good authentication technique contains at least two of the above methods. In a client server environment, strong authentication is a combination of server and client authentication:<br>● Server authentication is when the server proves its identity to the client.<br>● Client authentication is when clients prove their identity to the server.<br>**(3)Authorization:**<br>In computing systems, authorization is the process of determining | ***Relevant Explanation 2M each*** |

which permissions a person or system is supposed to have. -In multi-user computing systems, a system administrator defines which users are allowed access to the system, as well as the privileges of use for which they are eligible (e.g., access to file directories, hours of access, amount of allocated storage space). -Authorization can be seen as both the preliminary setting of permissions by a system administrator, and the actual checking of the permission values when a user obtains access. -Authorization is usually preceded by authentication.

**(4) Access Control:**

Access Controls use the mechanism to identify individuals who are attempting to enter a facility, area or system. From the security audit perspective, facility access control is an element that gets stringently verified.

Access control model is a framework that dictates access control using various access- control technologies. There are standard access control models which are highly domain and implementation independent. Each access control model has its own merits and demerits, and the specific business objectives they serve depend on the organization's need, culture, nature of business, etc. these models and examine their fitness with respect to an organization's security policy and business goals.

- Discretionary Access Control (DAC).
- Mandatory Access Control (MAC).
- Role Based Access Control (RBAC)

Types:

-Identification
-Authorization
-Password
-Biometrics
-Finger print
-Handwriting/Signature
-Face Recognition
-Retina scan technique
-voice authentication Biometrics

| | | | |
|---|---|---|---|
| **6.** | | **Attempt any FOUR of the following:** | **16** |
| | **(a)** | **Describe TCSEC.** | **4M** |

| | | | |
|---|---|---|---|
| | Ans. | The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which is used to evaluate operating systems, applications, and different products. This evaluation criterion is published in a book with an orange cover, which is called appropriately the Orange Book. (We like to keep things simple in security!) Customers use the security rating that the criteria presents so they have a metric to use when comparing different systems. It also provides direction for manufactures so they know what specifications to build to, and provides a one-stop evaluation process so customers do not need to have individual components within the systems evaluated<br>TCSEC provides a graded classification of systems that is divided into hierarchical divisions of security levels:<br>A. Verified protection<br>B. Mandatory protection<br>C. Discretionary protection<br>D. Minimal security The classification A represents the highest level of security and D represents the lowest level of security.<br>Each division can have one or more numbered classes and each has a corresponding set of requirements that must be met for a system to achieve that particular rating.<br>The classes with higher numbers indicate a greater degree of trust and assurance. So B2would offer more trust than B1, and C2 would offer more trust than C1.<br>The criteria include four main topics:<br>security policy, accountability, assurance, and documentation,<br>but these actually break down into seven different areas:<br>Security policy the policy must be explicit and well defined and enforced by the mechanisms within the system.<br>Identification Individual subjects must be uniquely identified. Labels Access control labels must be associated properly with objects.<br>Documentation this includes the test, design, specification documents, user guides, and manuals.<br>Accountability Audit data must be captured and protected to enforce accountability. | ***Valid Description 4M*** |

| | | | |
|---|---|---|---|
| | | Life cycle assurance Software, hardware, and firmware must be able to be tested individually to ensure that each enforces the security policy in an effective manner throughout their lifetimes.<br>Continuous protection: The security mechanisms and the system as a whole must perform predictably and acceptably in different situations continuously.<br>These categories are evaluated independently, but the rating that is assigned at the end does not specify these different objectives individually. The rating is a sum total of these items. Each division and class incorporates the requirements of the ones below it. This means that C2 must meet its criteria requirements and all of C1 requirements, and B3has its requirements to fulfill along with those of C1, C2, B1, and B2. Each division or class ups the ante on security requirements and is expected to fulfill the requirements of all the classes and divisions below it. | |
| | **(b)**<br>Ans. | **Explain Bell Model of confidentiality with diagram.**<br>**Bell – LaPadula: -**<br>The Bell-La Padula (BLP) model is a classic mandatory access-control model for protecting confidentiality.<br>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.<br>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.<br>**How Bell LaPadula Works?**<br>The security levels in BLP form a partial order, <<br>Each object, x, is assigned to a security level, L(x).<br>Similarly, each user, ‘u’, is assigned to a security level, L(u). Access to objects by users is controlled by the following two rules:<br>Simple security property. A user ‘u’ can read an object ‘x’ only if<br>L(x) < L(x) | **4M**<br>***Explanation 2M*** |

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.

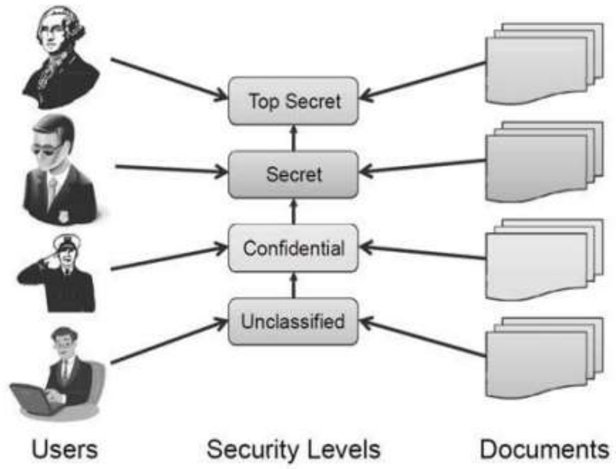


***Diagram 2M***

**(c)** Ans. **Describe IT Act, 2008.** **4M**

- 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 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.

***Suitable Explanation 4M***

| | | | |
|---|---|---|---|
| | | The modification includes<br>• Redefinition of terms like communication device which reflect the current use.<br>• Validation of electronic signatures and contracts.<br>• The owner of an IP address is responsible for content that are accessed or distributed through it.<br>• Organizations are responsible for implementation of effective data security practices.<br>**Following are the characteristics of IT ACT 2008**<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• 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. | |
| | **(d)**<br>Ans. | **Explain simple columnar transposition technique with example.**<br>**Single Columnar Transposition:** Single columnar transposition cipher is the simple cipher. Read the key, and numbered each letter of the key as per their appearance in the alphabet. The total encryption process is divided into three parts: | **4M**<br>***Explana*** |

1. Preparing the Key
2. Preparing the Plaintext
3. Encryption

***tion 2M***

**1. Preparing the Key:**

Suppose the key is “another”.

We can assign the number to each letter in this key as shown below:

***Example 2M***

a n o t h e r
1 4 5 7 3 2 6

That is, the first letter “a” is numbered 1. There are no B‘s or C‘s, so the next letter to be numbered is the ‘e‘. So e is numbered 2, followed by h, and so on. In the key if the same letter has occurred more than one time, it should be numbered 1, 2, 3, etc. from left to write.

For example, the key is ‘heaven‘. Here ‘e‘ is occurred two times. So first ‘e‘ from left hand side is numbered as 2, whereas second ‘e‘ is numbered as 3.

he a v e n
4 2 1 6 3 5

**2. Preparing the Plaintext:**

The letters from the message is written in rows under the numbered letters of the key. One letter from message is to be written under each letter of the key.

Let us say that the message is —we are the best.

We can write it as shown below:

H e a v e n

4 2 1 6 3 5

W E A R E T

H E B E S T

**3. Encryption:**

Now, arrange the above message written in rows under the numbered letters of the key as per ascending order of the numbers at the top of the plaintext letters.

a e e h n v

1 2 3 4 5 6

A E E W T R

B E S H T E

Then the letters are copied down column wise from top to bottom. The result is ciphertext, i.e.
ABEEESWHTTRE

For decryption,
First calculate the number of letters present in the ciphertext. Using the number of letters in the key, we can calculate the number of letters present in the last row.
As it can be seen above, all the columns contain only two letters and this is important. In the above example, there are 12 letters and the key having 6 letters, so there are two rows and the last row have 6 letters.
This gives us the idea about number of rows and number of letters in each column. Here there are two rows and each row having two ciphertext letters.
For decryption, the key is prepared as for encryption. Then write the first two letters below the column number ‘1‘.

he a v e n
4 2 1 6 3 5
A
B
Next two letters below column number two.

h e a v e n
4 2 1 6 3 5
E A
E B

Next two letters below column number 3 and so on. In this way write all the letters from ciphertext. It will look like this:
he a v e n
4 2 1 6 3 5
W E A R E T
H E B E S T

| | | | |
|---|---|---|---|
| | | Now, write down the letters in row wise, the result is the plaintext as below:<br>WEARETHEBEST<br>Separate the words by spaces,<br>we will get the message, i.e.,<br>WE ARE THE BEST | |
| | **(e)**<br>Ans. | **Explain any four physical access control mechanism.**<br>**Perimeter Security Controls:** Controls on the perimeter of the data center are designed to prevent unauthorized access to the facility. These types of controls, may have different “states” or behaviors based on the time of day or the day of the month. A gate may allow controlled access during the day but be locked or closed at night, for example.<br>Fences in some respects model the various levels of security in the virtual world. Turnstiles are less effective than either gates or fences. Mantraps, as the name implies, are enclosed areas with a secure door on either end that literally “trap” an individual between doors.<br><br>**Badging:**<br>Issued by a site security office, the photo identification badge is a perimeter security control mechanism that not only authenticates an individual but also continues to identify the individual while inside the facility. Most sites issuing photo identification require that the individual displays the badge where it is most visible, usually on the upper torso. The badge alone is no guarantee that unauthorized individual are denied access- badges can be stolen and photos replaced but combined with other perimeter controls, the badge offers a familiar and comfortable sense of security in most organizations.<br><br>**Keys and Combination Locks:**<br>Keys and combination locks are how most people know physical security, mainly because they are the least complicated and expensive devices. Beyond the mechanical door lock opened with a key, locks are now programmable and opened with a combination of keys (e.g., the five-key pushbutton lock once popular in IT operations), a security badge with a magnetic strip, or some other mechanism. Locks are typically unguarded and are meant to delay an intruder, not absolutely deny him access. For that reason, you rarely find these | **4M**<br><br>***Relevant explanation for each type 1M*** |

devices any more in areas where a high level of access authorization is required.

**Security Dogs:**

What some home security experts don’t tell you is that dogs are not just a man’s best friend, but they can also make great security guards! Dogs can be unflinchingly loyal and rely on all of their senses to detect intruders. They can also be trained to perform specialized services such as sniffing out drugs or explosives at airports or alerting the blind to fire before it engulfs them. The image of the German shepherd tethered to the door behind an auto junkyard may be the first thing that comes to mind when thinking about security dogs, but dogs are a highly effective and threatening perimeter security control when handled properly and humanely.

**Lighting:**

Lighting is another form of perimeter protection that discourages intruders or other unauthorized individuals from entering restricted areas. You are likely familiar with how shopping malls use streetlights to discourage parking lot break-ins, and many homeowners have motion-detector lights installed on garages and back porches. Critical buildings and installations should use some form of lighting as a deterrent, whether it be floodlights, streetlight, or searchlights. According to the National Institute of Standards and Technology, critical areas (e.g., fire escapes, emergency exits, and so forth) require safety lighting to be mounted 8 feet high and burn with a candlepower of 2 candelas (the equivalent of a strong spotlight).

**Smart Cards:**

A smart card resembles a regular payment (credit) card with the major difference that it carries a semiconductor chip with logic and nonvolatile memory. Unlike a security access card (badge with magnetic strip), the smart card has many purposes, including storing value for consumer purchases, medical identification, travel ticketing and identification, and building access control. The card may also store software that detects unauthorized tampering and intrusions to the chip itself and, if detected, can lock or destroy the contents of the chip to prevent disclosure or unauthorized uses.

| | | | |
|---|---|---|---|
| | | **Alarm Systems:**<br>The implementation of a series of the aforementioned intrusion detectors is referred to as an alarm system. A local alarm system sets off an alarm on the premises, alerting guards on the premises to respond. Private security firms manage central-station systems, such as home alarms from ADT and other well-known home security companies. They monitor a system 24 hours a day and respond to alerts from a central location. Company established, owned, and operated alarm systems (also called dedicated alarm systems) resemble a commercial central station system in that it serves many customers but differs because the focus is on the company exclusively. Dedicated systems may be more sophisticated than a local alarm system and share many of the same features as the centralized version. Additional alarms may be triggered at police or fire stations, with the permission and knowledge of the company being protected.<br>**Biometrics:**<br>The use of biometrics (Greek for “life measurements”) in conjunction with more standard forms of authentication such as fixed passwords and PINs is beginning to attract attention as the cost of the technology decreases and its sophistication increases. In fact, the traditional scheme of password-based computer security could lose stature as the use of smart card-based cryptographic credentials and biometrics authentication become commercially viable. Some companies such as the American Biometrics Corporation claim that using an individual’s unique physical characteristics along with other identification and authentication (I & A) techniques can almost unequivocally authenticate a user. Biometrics authentication uses characteristics of the human face, eyes, voice, fingerprints, hands, signature, and even body temperature, each technique having its own strengths and weaknesses. | |