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
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.

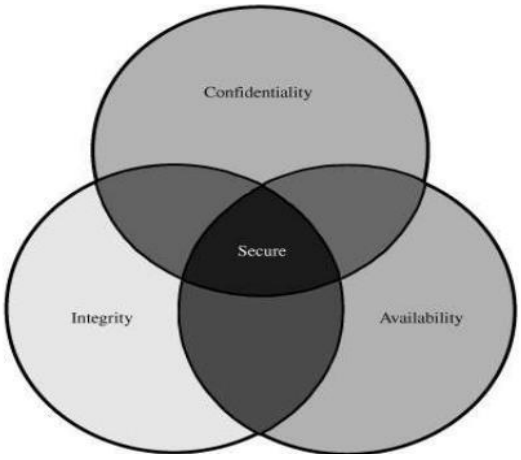
Q.1) a) Attempt any three: **12**

a) Mention basics principles of information security.
(3 principles: Each 1M, Diagram 1M)

Ans.

Basic Principles of Information Security are:

1. Confidentiality
2. Integrity
3. Availability



1. **Confidentiality:**
   The concept of confidentiality is used to prevent the intentional or unintentional unauthorized disclosure of message contents.
2. **Integrity:**
   The concept of integrity ensures that the modifications are not made to the data by unauthorized personnel or processes.
3. **Availability:**
   The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. It also guarantees that the systems are up and running when they are needed.

b) State the common criteria for information security evaluation.
(4 criteria: each 1M)

Ans.

Common criteria for information security evaluation are:

1. **Value:**
   It is the most commonly used criteria for classifying data in private sector. If the information is valuable to organization then it needs to be classified.
2. **Age:**
   The classification of the information may be lowered if the information's value decreases over the time. In the department of defense some classified documents are automatically declassified after a predetermined time period has passed.
3. **Useful life:**
   The time span or the useful life of the data or information is considered while classifying the information.
4. **Personal association:**
   If information is personally associated with specific individuals or is addressed by a privacy law then it may need to be classified.

c) What is cryptography? Mention any three application of it.
(Definition of cryptography 1M, any three applications 1M each)

Ans.

Cryptography
It is the art and science of achieving security by encoding messages to make them non-readable.

Application of cryptography:

Data Hiding: The original use of cryptography is to hide something that has been written.

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.

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.

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.

d) What are cyber crimes? List its different types.
(Definition 2M, Any four types ½ M each)

Ans.

Cybercrime (computer crime) is an illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them.
Cybercrime in a broader sense (Computer related crime) is any illegal behavior committed by means of, or in relation to a computer system or network, including such crimes as illegal possession offering or distributing information by means of a computer system or network.
For example, unauthorized access, damage to computer data or programs, computer sabotages, unauthorized interception of communications, computer espionage.

Different types of cyber crimes are:

1. Hacking
2. Cracking
3. Viruses, Virus Attacks
4. Pornography
5. Intellectual Property
6. Legal System of Information Technology

Q.1) b) Attempt any one: 6

a) What is information? Describe the need and importance of information.
(Information definition 2M, Need of information 2M, Importance of information 2M)
Note: any suitable explanation shall be considered.

Ans.

Information: It is a resource fundamental to the success of any business.

Data: It is a collection of all types of information which can be stored and used as per requirement.

Knowledge: It is based on data that is organized, synthesized or summarized and it is carried by experienced employees in the organization.

Action: It is used to pass the required information to a person who needs it with the help of information system

Need and importance of Information:

- Information is essential in organization because damage to information/data can cause disruptions in a normal process of organization like financial loss.
- Information is the most valuable resources of an organization so its management is crucial to making good business decision.
- Main objective of an information system is to monitor and document the operations of other systems.
- To satisfy the decision making capability, the information system should be call for intensive and complex interaction between different units in the organization.

b) State the security guidelines of information security.
(Guidelines 4M, security policies: 2M)

Ans.

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.

Different Information Securities Policies:-

1. Senior Management Statement of Policy
2. Regulatory Policy
3. Advisory Policy
4. Informative Policy

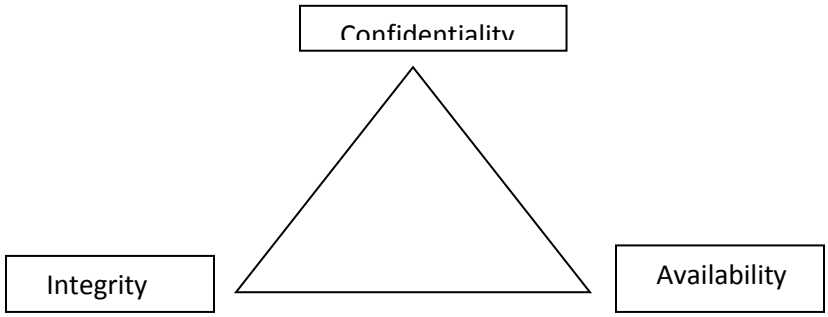
Q.2) Attempt any two: 16

a) State and describe the three pillars of information security with neat diagram.
(3 pillars with neat diagram 2M, explanation of each pillar 2M each)

Ans.

Three pillars of information security:

1. Confidentiality
2. Integrity
3. Availability



Confidentiality, Integrity and Availability i.e. CIA these three concepts are considered as three pillars of Information Security. These concepts represent the fundamental principles of Information Security. All the information security controls and safeguards, all the threats and security processes are subject to this CIA.

Confidentiality:

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

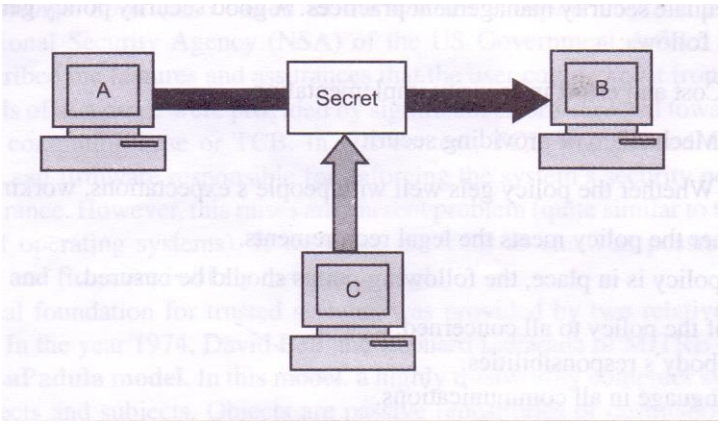


Fig: Loss of Confidentiality

Integrity:

The concept of integrity ensures that

i. Modifications are not made to data by unauthorized person or processes.
ii. Unauthorized modifications are not made to the data by authorized person or processes.
iii. The data is internally and externally consistent.

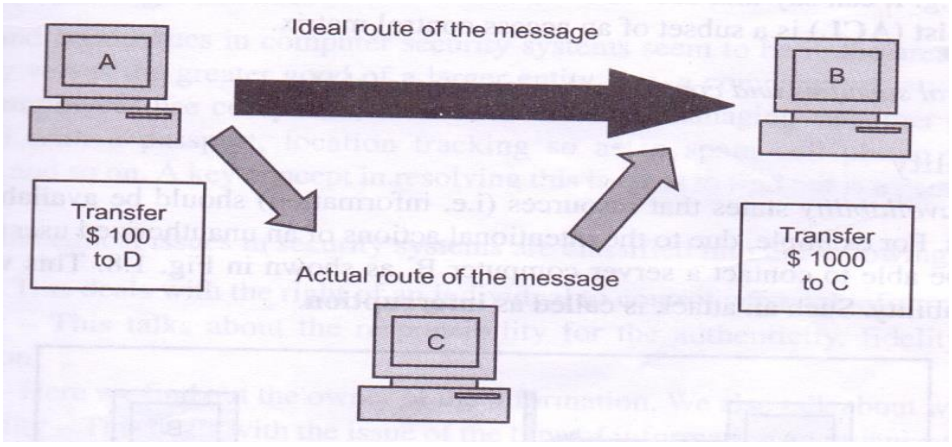


Fig: Loss of Integrity

Availability:

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

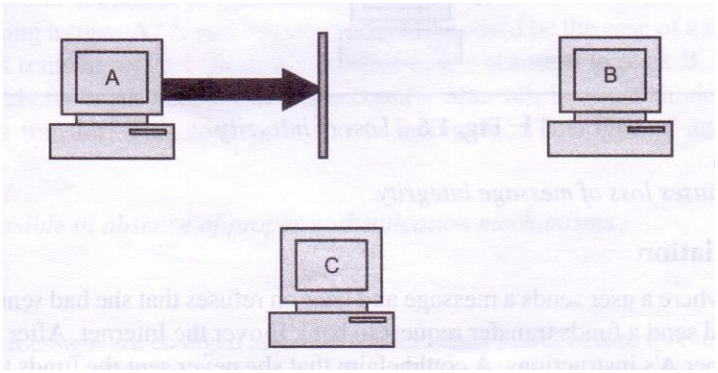


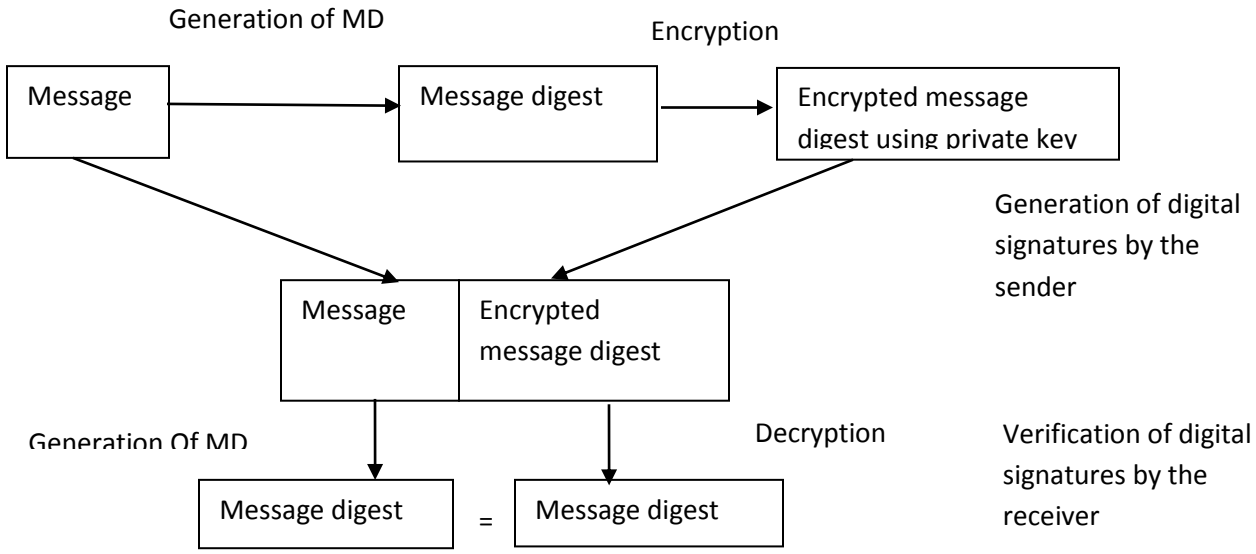
Fig: Attack on availability

b) What is digital signatures? State digital signature standards.
(Digital signature: correct explanation 2M, diagram (generation and verification) 2M, explanation of digital signature standard 4M (Diagram for DSS is optional))
Note: Any suitable explanation shall be considered

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 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:

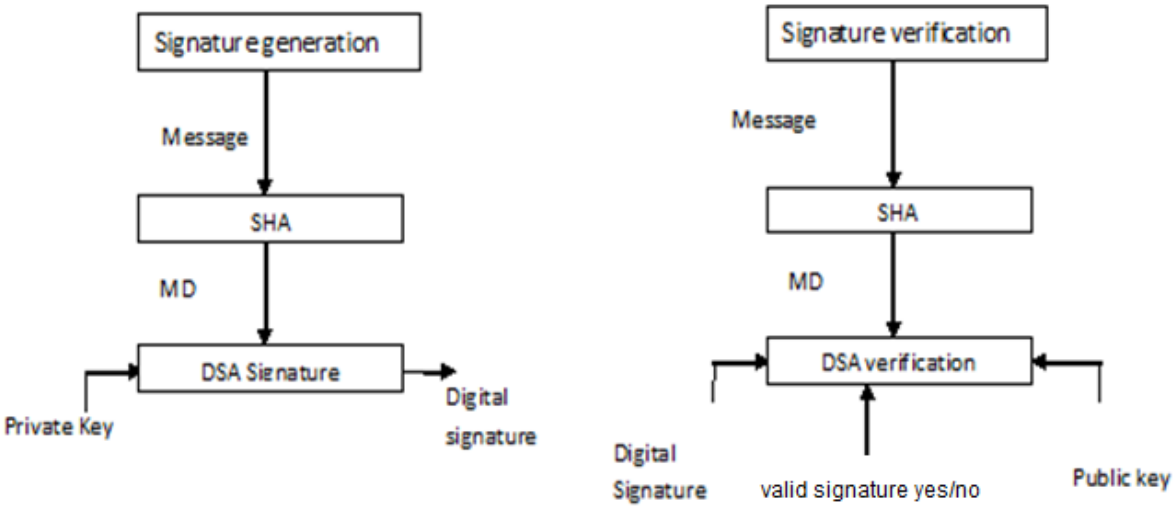


Procedure:

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.

Digital Signature Standard (DSS)

1. For performing digital signature of any message or documents, some standard is required. This standard is called Digital Signature Standard (DSS). It is published by NIST in 1991.
2. For different digital applications, this standard specifies an appropriate Digital Signature Algorithm (DSA).
3. As per this standard, the message digest of a document is calculated using secure hash algorithm-1(SHA-1).
4. Using this algorithm a signature is generated, which includes a pair of large number which is represented in the form of strings of binary digits. A set of rules and parameters are used to compute the signature.
5. The DSA algorithm has three parts-key generation, signature generation and signature verification.
6. Using user's private key, a signature is generated. Sender's public key is used for the verification of signature .Anyone can verify the signature of a sender.
7. In signature generation, the message digest of a message is computed using secure hash algorithm. Then, the signature is generated using this message digest.
8. After that, the sender sends the signature with the message to the receiver. The receiver is first intended to verify the signature using sender's public key. The recipient should use the same hash function to calculate the message digest of the received message.
9. The Hash function is specified in a separate standard, the secure Hash Standard (SHS), FIPS 180.



c) Name data recovery tools and explain data recovery procedures.
(Any four tools 1M each, explanation of 4 Data recovery procedures 1M each)

Ans.

Following are the data recovery tools:

1. NTFS Data recovery tools
2. FAT data recovery tool
3. Digital Camera Data recovery tool
4. Removable media data recovery tool
5. Recovery of deleted files
6. Recovery of formatted partition

Data Recovery Procedures:

1. **NTFS Data Recovery Tools:** NTFS Recovery is a fully automatic utility that recovers data from damaged or formatted disks. It is designed with a home user in mind. You don't need to have any special knowledge in disk recovery.
   Example: - Diskinternal's NTFS Data Recovery tool. The tool supports
   - A disk volume containing valuable info was damaged due to a system malfunction
   - A disk volume was damaged due by a dangerous virus
   - Windows cannot access a disk drive
   - Disk was damaged

- You have mistakenly formatted a disk volume
- Files or folders are not readable
- Corrupt or damaged partition table

2. FAT Data Recovery Tools:

FAT Recovery is a fully automatic utility that recovers data from damaged or formatted disks. The program scans the disk first and then restores the original structure of files and folders.
Example: - Diskinternal‘s FAT Data Recovery tool.

Works for all:

- 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. 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. If the file has been partially over written, there are some data recovery software applications which will perform better to recover the maximum of data.

It is important to save the recovered file in a separate location like a flash drive. A file can only be permanently lost if it is over written. So do not over write, do not install or create new data on the file location.

6. Procedure to recover formatted partition:

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:

1. An enclosure (to convert hard drive into USB external drive).
2. A bootable system with preferably a high storage capacity hard drive.
3. A disk image creator and a virtual disk creator.
4. Data recovery software.
5. Sufficient storage space on devices other than the formatted drive.

Q.3) Attempt any four: **16**

a) What is Risk? Describe Risk Management.

(Risk Definition 1M; Description along with Definition of Risk management 3M)

Note: Any suitable description of risk management shall be considered.

Ans.

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

(i) The adverse impacts that would arise if the circumstance or event occurs; and
(ii) The likelihood of occurrence.

Risk Management:

1. The process of identifying, assessing, and responding to risk.

OR

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.

2. Risk management involves three major undertakings:
   - Risk identification,
   - Rrisk assessment,
   - Risk control.

The various components of risk management and their relationship to each other are shown in Figure

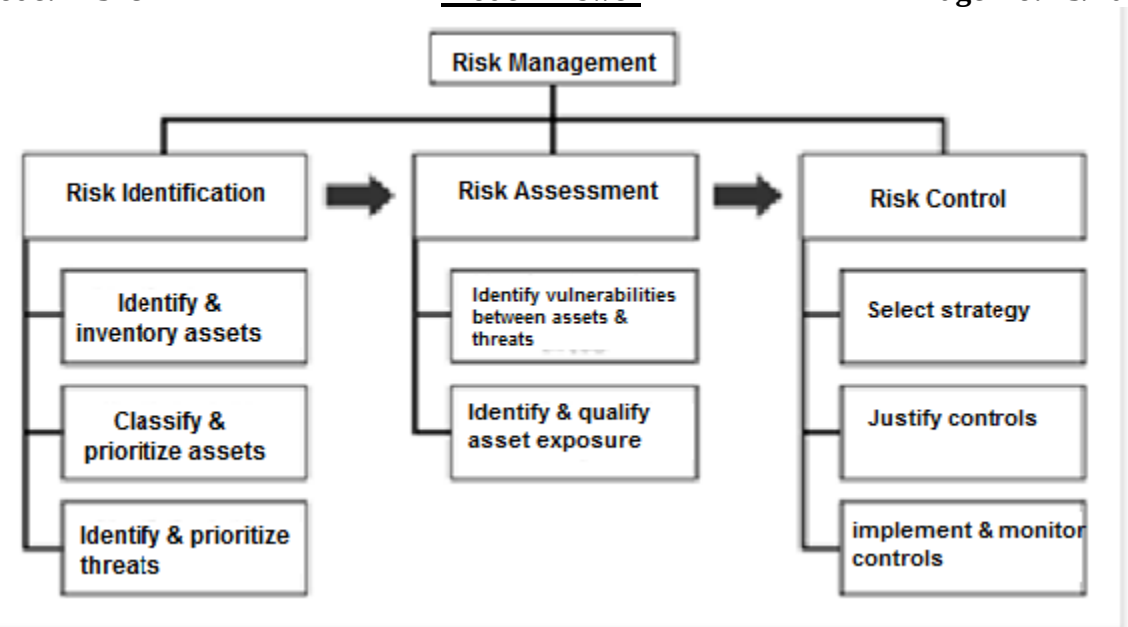


Fig: Components of Risk Management

Risk identification is the examination and documentation of the security posture of an organization's information technology and the risks it faces.

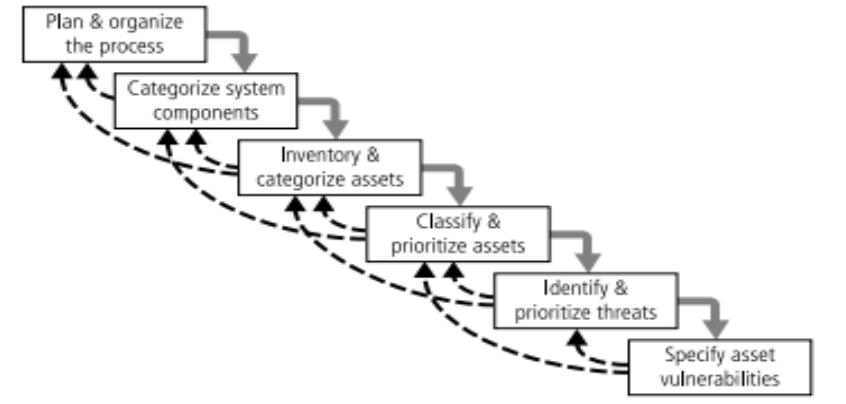


Fig: Components of Risk identification

Risk assessment is the determination of the extent to which the organization's information assets are exposed or at risk.

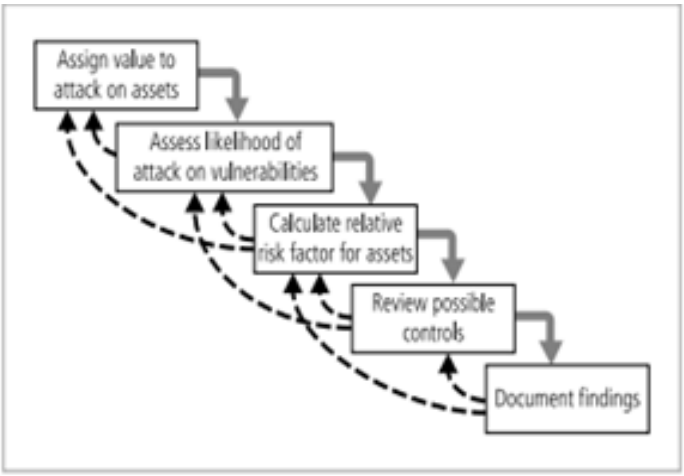


Fig: Major Stages of Risk Assessment

Risk control is the application of controls to reduce the risks to an organization's data and information systems.

It includes four strategies:

1. Defend the defend control strategy attempts to prevent the exploitation of the vulnerability. This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities from assets, limiting access to assets, and adding protective safeguards.

2 The transfer control strategy attempts to shift risk to other assets, other processes, or other organizations.

3 The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks the mitigate control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.

4. The accept control strategy is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation.

Risk can be calculated by using Risk Analysis (RA) which is of two types:

1) **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.

2) **Qualitative Risk Analysis:** A collaborative process of assigning relative values to assets, assessing their risk exposure and estimating the cost of controlling the risk.

b) Describe the need of physical security.
(Any suitable description 4M)

Ans.

Security is "the quality or state of being secure—to be free from danger."

- In other words, protection against adversaries from those who would do harm, intentionally or otherwise is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system.

- Physical security to protect physical items, objects, or areas from unauthorized access and misuse.

- Physical security encompasses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization, including the people, hardware, and supporting system elements and resources that control information in all its states (transmission, storage, and processing). Most technology-based controls can be circumvented if an attacker gains physical access to the devices being controlled. In other words, if it is easy to steal the hard drives from a computer system, then the information on those hard drives is not secure. Therefore, physical security is just as important as logical security to an information security program.

It is essential to take care of because of some following reasons:

- It will protect physical items/assets like hard disk, RAM, objects or area from unauthorized user.
- The threat of theft—the illegal taking of another's property, which can be physical, electronic, or intellectuals is a constant.
- Physical theft can be controlled quite easily by means of a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems.
- Technical hardware failures or errors occur when a manufacturer distributes equipment

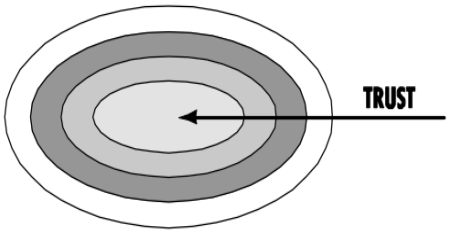
containing a known or unknown flaw. These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability. Some errors are terminal—that is, they result in the unrecoverable loss of the equipment.

- Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated, and thus, equipment can sometimes stop working, or work in unexpected ways.
- For protecting any organizations, physical layer security are important.

c) Describe the term rings of trust.
(Rings of trust in stand alone system with diagram 2M, Rings of trust in network with diagram 2M)

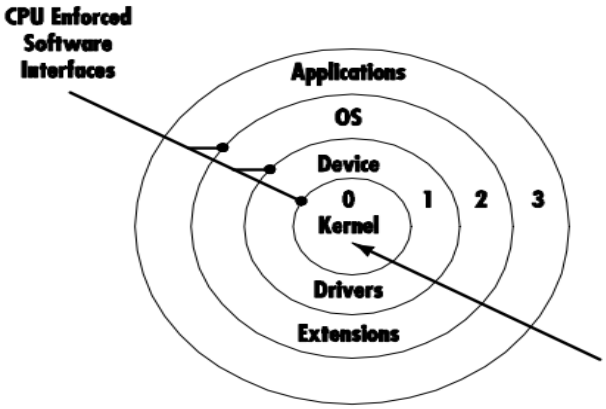
Ans.

Rings of Trust: Trust in a system moves from the outside tov the inside in a unidirectional model
As shown in the figure



The first implementation of ring model of security for a system was in MIT's Multi – shared operating system.

1. Ring of trust in standalone/single system



Here the outer most layers contain less security whereas higher level of security is implemented in inner rings.

The operating system knows who and what to trust by relying on rings of protection.

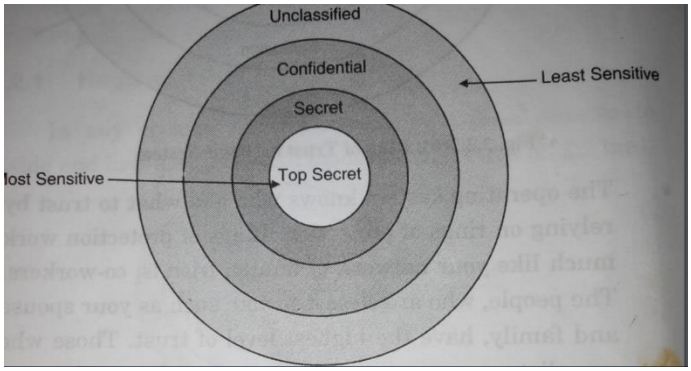


Fig : Ring of Protection

The Protection ring model the operating system provides with various level at which to execute Code or to restrict that code's access.

The rings provide much granularity.

The layer number increases and the level of trust decreases.

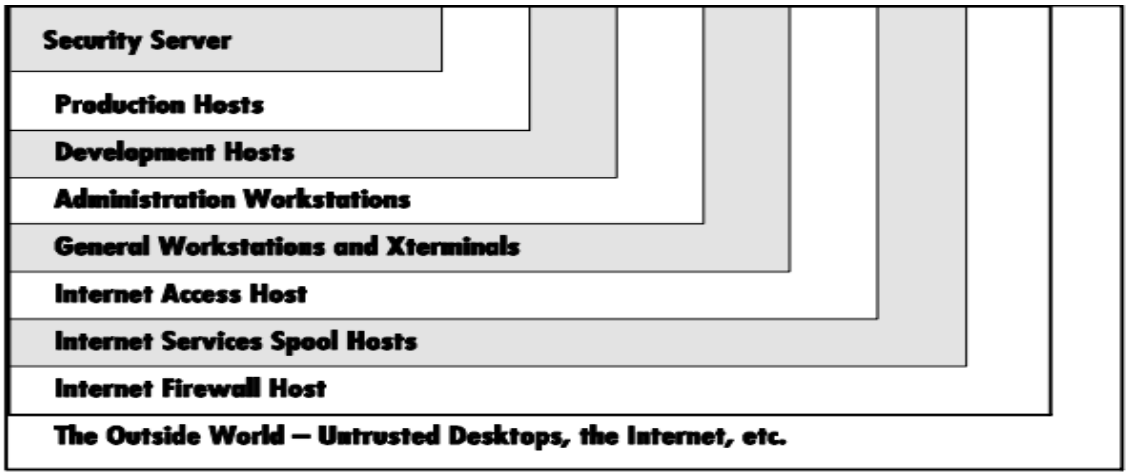
Layer 0:
The most level of trust.
The OS kernel resides at this level.
Any process running at this level is called operating in Privileged Mode.

Layer 1: It contains Non *Privileged portion* of the operating system.

Layer 2: At this level I/O drivers, low level operations and utilities reside.

Layer 3:
At this level applications and procedures operate.
Users usually interact with this level.
Operations working at this level generally called working in User Mode.

2. Ring of trust in Networked Environment



- The hosts of networks are divided into rings as per the security ratings of services provided by the host to network.
- The created ring can be treated as a trust between different host of the network.
- The hierarchy of the ring can be decided on the basis of
  - Whether the host is in the room or not i.e physically secured or not
  - Whether the hosts are having normal user accounts
  - Whether the host is at remote place or not
  - Whether the host need data from the internet
  - Whether the host provide critical services or not.
  - Whether the large amount of people affected because of downning of the host.

d) Describe play fair cipher.

(Correct description and brief example 4M)

Note: Any suitable description shall be considered

Ans.

- The Playfair cipher or Playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher.
- The technique encrypts pairs of letters (*digraphs*), instead of single letters.
- The Playfair is thus significantly harder to break.
- The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.
- To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of

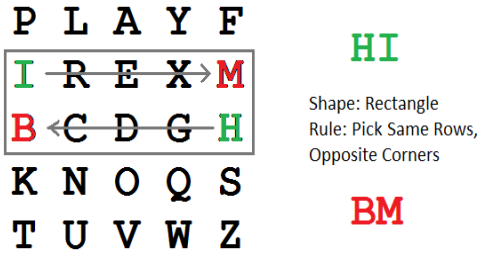
the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.

- To encrypt a message, one would break the message into digraphs (groups of 2 letters) such that, for example, "HelloWorld" becomes "HE LL OW OR LD", and map them out on the key table. If needed, append a "Z" to complete the final digraph. The two letters of the digraph are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle.

Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

1. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any uncommon monograph will do.
2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

Example: plaintext "HI" and Ciphertext "BM"



(Using rectangular Rule)

e) Describe the IT Act, 2008.
(Any 4 characteristics 1M each)
Note: Any suitable description shall be considered

Ans.

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.

The modification includes:

- Redefinition of terms like communication device which reflect the current use.
- Validation of electronic signatures and contracts.
- The owner of an IP address is responsible for content that are accessed or distributed through it.
- Organizations are responsible for implementation of effective data security practices.

Following are the characteristics of IT ACT 2008:

- This Act provides legal recognition for the transaction i.e. Electronic Data Interchange (EDI) and other electronic communications. Electronic commerce is the alternative to paper based methods of communication to store information.
- This Act also gives facilities for electronic filling of information with the Government agencies and further to change the Indian Penal Code-Indian Evidence Act 1872, Bankers code Evidence Act 1891 and Reserve Bank of India Act, 1934 and for matter connected therewith or incidental thereto.
- The General Assembly of the United Nations by resolution A/RES/51/162, dated 30 January 1997 has adopted the model law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.

- This recommends that all States give favorable consideration to the above said model law when they enact or revise their laws, in terms of need for uniformity of the law applicable to alternative to paper based methods of communication and storage of information.

- It is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

Q.4) a) Attempt any three: 12

a) Explain the protection mechanisms in a trusted computing base.
(Any 8 mechanisms ½ M each)

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 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) Mention different compliance standards for information security.
(Any accurate 04 standards with correct full forms 4M)

Ans.

1) ISMS (Implementing and Information Security Management System) is a set of policies and procedures which specifies the methods to manage the task and activities by management to achieve information security.
2) ISO 27001 (International Standard Organisation 27001) describing definition, scope, Risk assessment, control for implementation, prepare statements of applicability
3) ISO 20000 is an industry standard like ISO 9000/9001 which offers organizational certification.
4) BS 25999 (British Standard 25999) for ensuring that organization is prepared to reduce and recover quickly from potential risks which may affect their business.
5) PCI DSS (The Payment Card Industry Data Security Standard) by PCI Security Council is to decrease the payment card fraud across the internet and increase data card security.
6) ITIL Framework (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.)
7) COBIT FRAMEWORK
   (The Control Objectives for Information and related Technology (COBIT) is "a control framework that links IT initiatives to business requirements, organises 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")

c) Explain the concept of TCB.
(Suitable explanation with accurate diagram 4M)

Ans.

The trusted computing base (TCB) is the sum total of all software and hardware required to enforce security

• Typically, all of hardware, the core OS that is involved in protection, and all programs that operate with system privileges

• Desirable properties: – Small – Separable, well-defined – Independently-auditable

Reference Monitor • A reference monitor is a separable module that enforces access control decisions

• All sensitive operations are routed through the reference monitor

• The monitor then decides if the operation should proceed

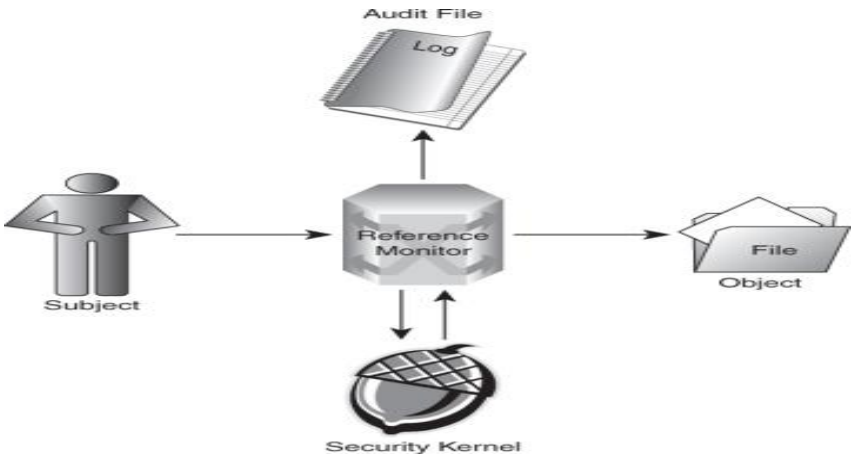


Figure: Reference Monitor

It stand s between Subjects and Objects and its role is to verify the subject, meets the minimum requirements for an access to an object as shown in figure.

The reference monitor has three properties:

1. Can not be bypassed and controls all access.
2. Can not be altered and is protected from modification or change.
3. Can be verified and tested to be correct.

In Unix/Linux security kernel acts as a Reference Monitor which will handle all user application requests for access to system resources.

In trusted system Object is something that people want to access.

These objects (data) are labeled according to their level of sensitivity.

Subjects (users) should have same level of classification while accessing object.

d) Explain classical encryption techniques of cryptography.
(Any two encryption techniques with suitable diagram 2M each)

Ans.

An original message is known as the plaintext, while the coded message is called the ciphertext.

The process of converting from plaintext to ciphertext is known as enciphering or encryption; restoring the plaintext from the ciphertext is deciphering or decryption

The many schemes used for enciphering constitute the area of study known as cryptography

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis

The areas of cryptography and cryptanalysis together are called cryptology.

There are two classifications of cryptographic algorithms.

1. Symmetric Algorithm:

Symmetric-key algorithms are algorithms for **cryptography** that use the same **cryptographic keys** for both **encryption** of plaintext and decryption of ciphertext. The **keys** may be identical or there may be a simple transformation to go between the two **keys.**

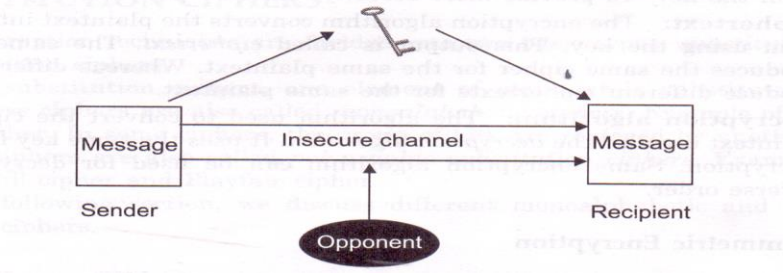


Fig: Symmetric encryption technique

Encryption algorithms are divided into two types:

i. **Block Cipher:** A block cipher encrypts 64- bit blocks of data, with a complex encryption function. Security of these ciphers totally depends on the design of the encryption function. A block cipher encrypts blocks belonging to the same document all under the same key.

ii. **Stream Cipher:** It encrypts smaller blocks of plain text data, usually bits or bytes. A stream cipher encrypts the plain text under a continuously changing key stream. Security of these ciphers depends on the design of the key stream generator.

2. Asymmetric Algorithm:

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority.

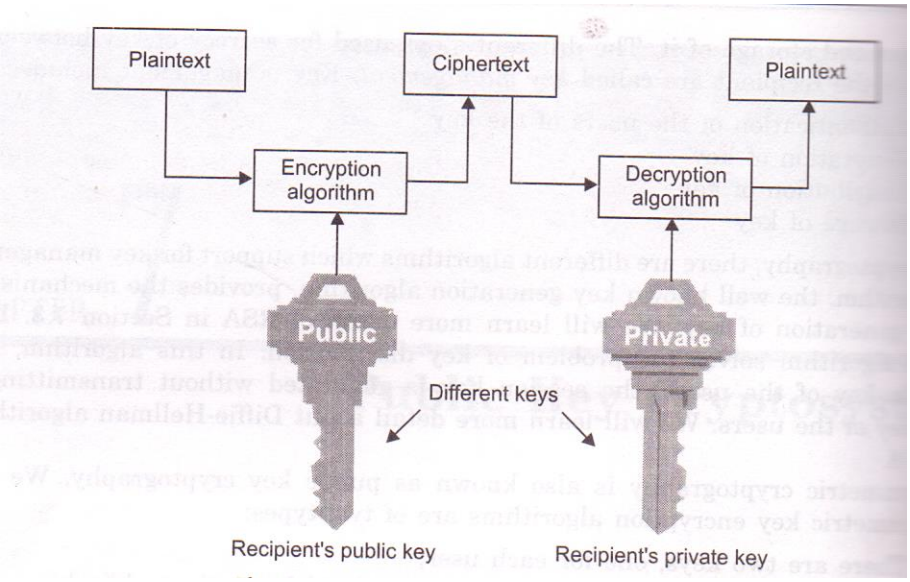


Fig: Asymmetric encryption technique

Q.4) b) Attempt any one: **6**

a) Explain how to encrypt and decrypt message using transposition method.
(Any transposition method accurate encryption with example 3M and accurate decryption with example 3M)

Ans.

In transposition Cipher method plaintext message is hidden by rearranging the order of plain text letters without altering the original letter.

In transposition cipher, the letters are written in a row under the key and then arrange the column as per alphabetical order. There are two types of transposition ciphers: single columnar and double columnar transposition ciphers.

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:

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

1. **Preparing the Key:** Suppose the key is 'another'. We can assign the number to each letter in this key as shown below:

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.

h	e	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'.

h	e	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:

h	e	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:

WEARETHEBEST

Separate the words by spaces, we will get the message,i.e.,

WE ARE THE BEST

Double Columnar Transposition:

The singular columnar transposition cipher is not much secure. To provide stronger transposition cipher, double columnar transposition is used. The working of double columnar cipher is similar to the single columnar transposition, but the process is repeated twice. Here we can use either the same key both times or two different keys. Suppose the plaintext is "we are the best" and the keys are "heaven" and "another".

h	e	a	v	e	n
4	2	1	6	3	5
W	E	A	R	E	T
H	E	B	E	S	T

The first encryption gives: ABEEESWHTTRE. These letters are written under the second key, thus we get:

a	n	o	t	h	e	r
1	4	5	7	3	2	6
A	B	E	E	E	S	W
H	T	T	R	E		

If the last row is having fewer letters than the first row, then we can add some more letters to complete the row. But this reduces the security of the cipher. So, one can encrypt the plaintext by not adding any dummy letters in the last row. The ciphertext is as below:

AHSEEBTETWER

The double columnar transposition cipher uses two keys so it is stronger than the single columnar transposition. The cryptanalysis of double columnar is difficult as compared to that of single columnar cipher.

b) What is stegnography? Describe authentication protocols.
(Explanation of stegnography 3M, any six authentication protocols ½ M each)

Ans.

Stegnography: Stegnography is a technique of hiding a large amount of secret message within an ordinary message and the extraction of it at its destination.

In modern digital stegnography 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 following formula shows the stegnographic process.

Cover Media + Hidden Data + Stego –Key = StegoMedium

Cover Media : It 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.

Describe Authentication Protocols:

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.

Various authentication protocols are listed and described below.

1. **CHAP** - Challenge Handshake Authentication Protocol is a three way handshake protocol which is considered more secure than PAP. Authentication Protocol.
2. **EAP** - Extensible Authentication Protocol is used between a dial-in client and server to determine what authentication protocol will be used.
3. **PAP** - Password Authentication Protocol is a two way handshake protocol designed for use with PPP. Authentication Protocol Password Authentication Protocol is a plain text password used on older SLIP systems. It is not secure.
4. **SPAP** - Shiva PAP. Only NT RAS server supports this for clients dialing in.

5. **DES** - Data Encryption Standard for older clients and servers.
6. **RADIUS** - Remote Authentication Dial-In User Service used to authenticate users dialing in remotely to servers in a organization's network.
7. **S/Key** - A onetime password system, secure against replays. RFC 2289. Authentication Protocol.
8. **TACACS** - Offers authentication, accounting, and authorization. Authentication Protocol.
9. **MS-CHAP (MD4)** - Uses a Microsoft version of RSA message digest 4 challenge and reply protocol. It only works on Microsoft systems and enables data encryption. Selecting this authentication method causes all data to be encrypted.
10. **SKID** - SKID2 and SKID3 are vulnerable to a man in the middle attack.

Q.5) Attempt any two: **16**

a) Describe the following terms:

i) Mail Bombs

ii) Hacking

iii) Pornography

iv) Cracking.

(2M for Each term)

Ans.

i) Mail Bombs:

Email ―bombing" is characterized by abusers repeatedly sending an identical email message to a particular address. A mail bomb is the sending of a massive amount of email to a specific person or system. A huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop functioning. Mail bombs not only inconvenience the intended target but they are also likely to inconvenience everybody using the server. Senders of mail bombs should be wary of exposing themselves to reciprocal mail bombs or to legal actions.

ii) Hacking:

Every act committed towards breaking into a computer and/or network is hacking and it is an offence. Hackers write or use readymade computer programs to attack the target computer. They possess the desire to destruct and they get enjoyment out of such destruction. Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are hot on hackers target lists and attacks on government websites receive wide press coverage.

iii) Pornography

Child Pornography is a very inhuman and serious cybercrime offence. It includes the following:

- Any photograph that can be considered obscene and/or unsuitable for the age of child viewer.
- Film, video, picture.
- Computer generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

Internet is the most frequently used tool for such criminals to reach children and practice child sex abuse. The spreading use internet and its easy accessibility to children has made them viable victim to cybercrime. There is a type of humans called Pedophiles who usually allure the children by obscene Pornographic contents and then they approach them for sex. Then they take their naked photographs while having sex. Such people sometime misguide children telling them that they are of the same age and win their confidence. Then they exploit the children either by forcing them to have sex or selling their pictures over internet.

iv) Cracking:

A cracker is someone who breaks into someone else's computer system, often on a network by passing passwords or licenses in computer programs or in other ways intentionally breaches computer security. A cracker can be doing this for Profit maliciously, for some altruistic purpose or cause, or because the challenge is there. The term "cracker" is not to be confused with "hacker". Hackers generally deplore cracking.

b) Write a short note on ITIL and COBIT framework.
(ITIL: - Description 3M, Diagram 1M; COBIT: - Description 3M; Diagram 1M)

Ans.

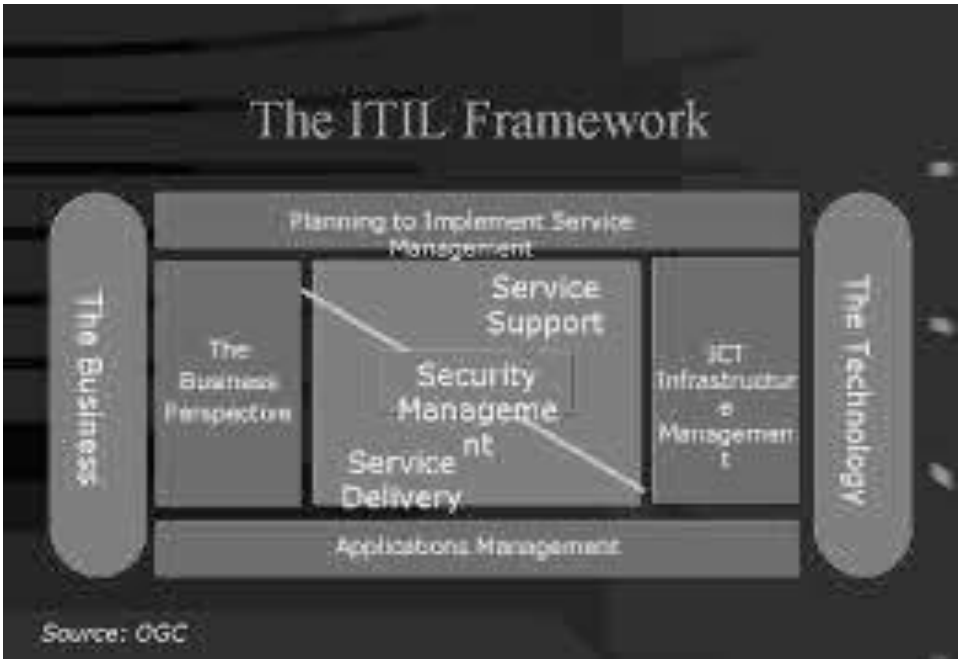
ITIL:

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.

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:

a) Service Level Management,

b) Financial Management,
c) Capacity Management,
d) Service Continuity Management,
e) Availability Management,
f) Service Desk,
g) Incident Management,
h) Problem Management,
i) Configuration Management,
j) Change Management, and
k) Release Management.



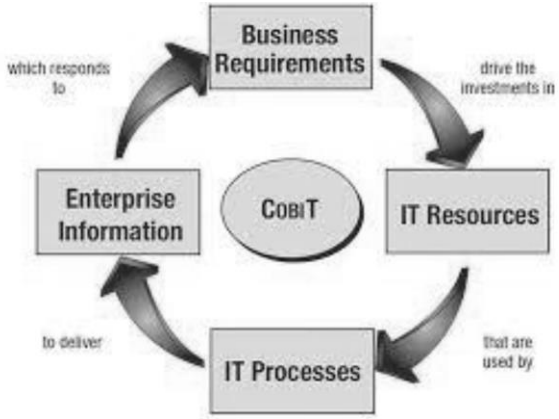
COBIT:

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.



c) Describe different authorization and authentication mechanism.
(Explanation of authorization 4M, Explanation of authentication 4M)
Note: Any suitable explanation or mechanism shall be considered.

Ans.

Authorization:

Authorization is the matching of an authenticated entity to a list of information assets and corresponding access levels. This list is usually an ACL or access control matrix. 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.
4. **System administrator** or **sysadmin**: He is a person who is responsible for the configuration, and reliable operation of computer systems; especially multi-user computers, such as servers. The system administrator seeks to ensure that the uptime, performance, resources, and security of the computers he or she manages meet the needs of the users, without exceeding the budget.
5. **Access control list** (**ACL**): With respect to a computer file system, it is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.
6. **Principle of least privilege:** It requires that in a particular abstraction layer of a computing environment, every module must be able to access only the information and resources that are necessary for its legitimate purpose.

Authentication:

Authentication is the process of validating a supplicant's purported identity. 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 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.

   A **passphrase** is a series of characters, typically longer than a password, from which a **virtual password** is derived. For example, while a typical password might be "23skedoo," a typical passphrase might be "MayTheForceBeWithYouAlways," represented as "MTFBWYA."

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.

Asynchronous tokens, which don't require that the server and tokens all maintain the same time setting, use a challenge/response system, in which the server challenges the supplicant during login with a numerical sequence. The supplicant places this sequence into the token and receives a response. The prospective user then enters the response into the system to gain access.

3. **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.

Q.6) Attempt any four: 16

a) Explain about viruses and viruses attacks.
(Virus: 2M; any two Virus attacks 1M each; any relevant description shall be considered)

Ans.

Virus: It is a malicious code which perform specific task to harm intended user or groups of users.

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files. A computer virus is one kind of threat to the security and integrity of computer systems. A Computer virus can cause the loss or alteration of programs or data, and can compromise their confidentiality .A computer virus can spread from program to program, and from system to system, without direct human intervention.

Viruses attacks:

A virus attack is when your computer's security is penetrated, and someone tries to steal your computer information and documents.

Types of viruses attack:

- **DOS:** A Denial of Service attack is a type of cyber crime where an internet site is made unavailable by using multiple computers which make repeated requests to the server.

- **SPAM:** It is an irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.
- **Malicious insider:** An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.
- **Phishing:** It is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.
- **Botnet:** It is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.

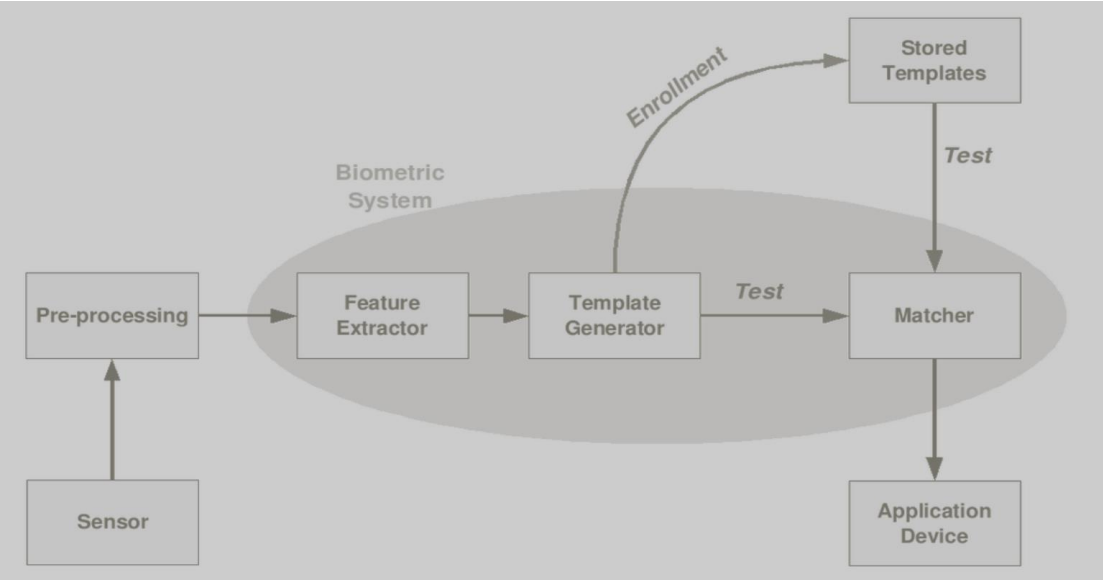
b) Write a note on biometrics.

(Description 3M; Diagram 1M; any relevant description shall be considered)

Ans..

Biometrics:

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.



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 a 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.

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.

Second, in identification mode the system performs a one-to-many comparison against a 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.

The first time an individual uses a biometric system is called enrolment. During the enrolment, 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 enrolment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust.

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 artifact 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.

During the enrolment 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.

Some common biometric techniques in use today include

- Fingerprint recognition
- Signature dynamics
- Iris scanning
- Retina scanning
- Voice prints
- Face recognition

c) Describe BIBA model of integrity.
(Description 1M; Properties 3M; any relevant description shall be considered)

Ans:

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.

Hence ken BIBA developed a model 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: - Data can be read from higher integrity level.
2. Star Integrity property: - Data can be written to lower integrity level.
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)

d) Describe ITSEC with its classes.
(Description of ITSEC 2M; Classes 2M; any relevant description shall be considered)

Ans.

Information Technology security equation criteria (ITSEC):
ITSEC is developed by European country for security equation criteria. ITSEC focuses more on integrity and availability. It tries to provide a uniform approach to product and system. ITSEC will also provide security targets like.

- Policy for system security.

- Required mechanism for security.
- Required rating to claim for minimum strength.
- Level for evaluating targets –functional as well as evaluation.

ITSEC classes contain hierarchical structure where every class will be added to the class above it. This class contains some particular function.

- F-IN Provides high integrity.
- F-AV Provides high availability.
- F-DI Provides high data integrity.
- F-DX It is used for networks to provide high integrity while exchanging data in networking.

ITSEC uses following 7 classes from E0 to E6 to evaluate the security:

- E0 – Minimal protection.
- E1 – Security target and informal architecture design must be produced.
- E2 – An informal detail design and test document must be produced.
- E3 – Source code or hardware drawing to be produced. Correspondence must be shown between source codes of detailed design.
- E4 – Formal model of Security and Semi – formal specification of Security function architecture and detailed design to be produced.
- E5 – Architecture design explain the inter relationship between security component.
- 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.

e) Explain ceasor cipher with example.
(Description 2M; Example 2M)

Ans:

Caesar Cipher:

The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Example:-

Plain: MEET ME AFTER THE TOGA PARTY

Cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

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

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

Let us assign a numerical equivalent to each letter:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows. For each plaintext letter, substitute the cipher text letter

$$C = E(3, P) = (P + 3) mod\ 26$$

A shift may be of any amount, so that the general Caesar algorithm.

$$C = E(K, P) = (K + P) mod\ 26$$

Where takes on a value in the range 1 to 25.The decryption algorithm is simply

$$P = D(K, C) = (C - K)\ mod\ 26$$

If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys. The results of applying this strategy to the example cipher text. In this case, the plaintext leaps out as occupying the third line.

Three important characteristics of this problem enabled us to use a brute force cryptanalysis:

- The encryption and decryption algorithms are known.
- There are only 25 keys to try.
- The language of the plaintext is known and easily recognizable.