Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more importance. (Not applicable for subject English and Communication Skills)
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgment 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.1) A) Attempt any three: 12M

a) Define the following terms:

1) Plain text
2) Cipher text
3) Cryptography
4) Cryptanalysis
(Correct definition, each 1M)

Ans.

1) **Plain text**
   Plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to the message.
2) **Cipher text**
   When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.
3) **Cryptography**
   Cryptography is the art and science of achieving security by encoding messages to make them non-readable.
4) **Cryptanalysis**
   Cryptanalysis is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

b) Define the following terms:

1) Interruption
2) Interception
3) Fabrication
4) Modification

(Correct definition, each 1M)

Ans.

1) Interruption

Interruption is when a file is corrupted or lost. In general, interruption refers to the situation in which services or data become unavailable, unusable, destroyed, and so on. In this sense, denial of service attacks by which someone maliciously attempts to make a service inaccessible to other parties is a security threat that classifies as interruption

2) Interception

Interception refers to the situation that an unauthorized party has gained access to a service or data. A typical example of interception is where communication between two parties has been overheard by someone else. Interception also happens when data are illegally copied, for example, after breaking into a person‘s private directory in a file system.

3) Fabrication

Fabrication refers to the situation in which additional data or activities are generated that would normally not exist. For example, an intruder may attempt to add an entry into a password file or database. Likewise, it is sometimes possible to break into a system by replaying previously sent messages.

4) Modification

Modifications involve unauthorized changing of data or tampering with a service so that it no longer adheres to its original specifications. Examples of modifications include intercepting and subsequently changing transmitted data, tampering with database entries, and changing a program so that it secretly logs the activities of its user.

c) List down three pillars of information security. Describe any one in detail with neat labeled diagram.

(List 2M, Description of any one pillar with diagram 2M)

Ans.

Three pillars of information security:

1) Confidentiality
2) Integrity
3) Availability

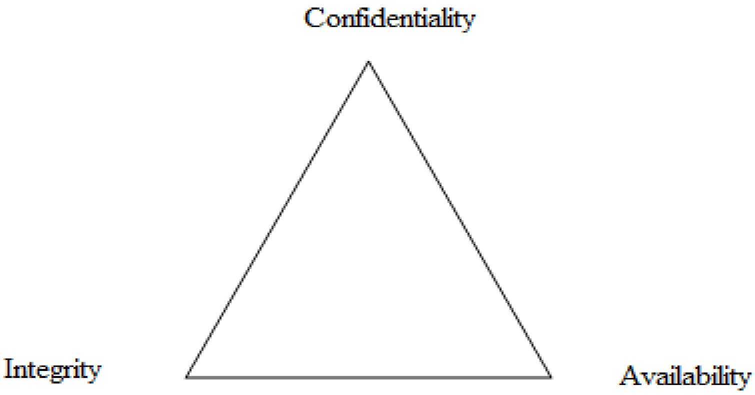


Fig: Three pillars of Information Security

1) Confidentiality:

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

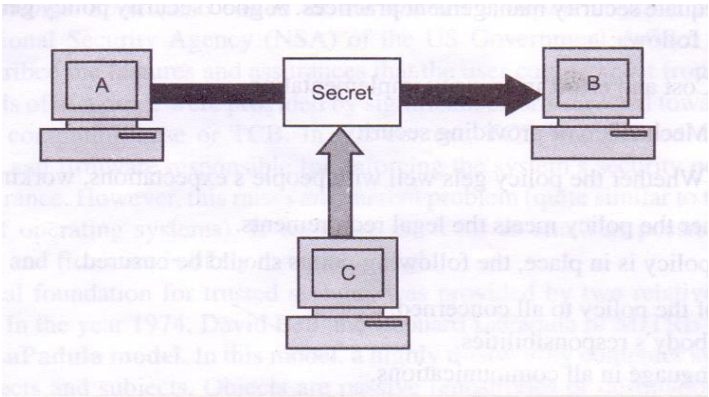


Fig: Loss of Confidentiality

2) Integrity:

The concept of integrity ensures that

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

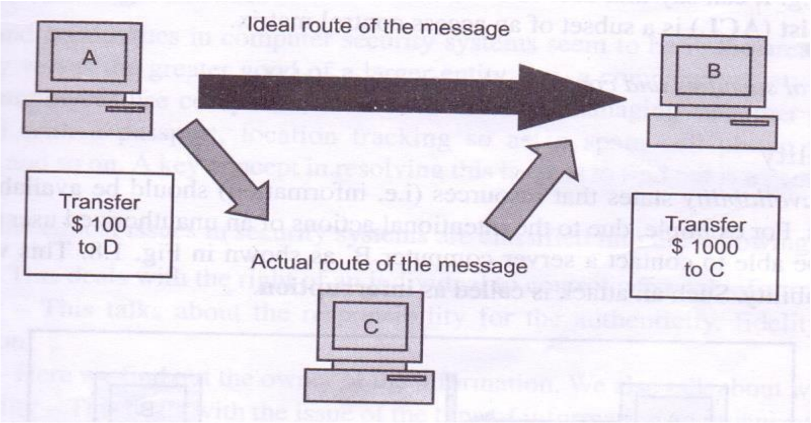


Fig: Loss of Integrity

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

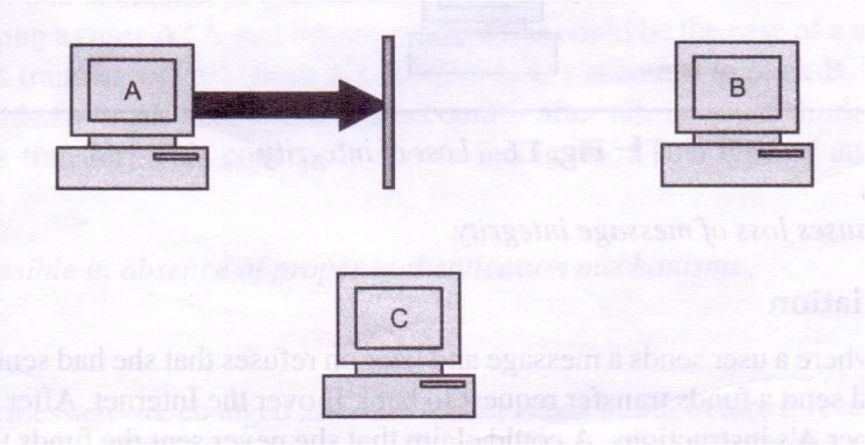


Fig: Attack on availability

d) Define following terms with example:

1) Hacking

2) Cracking

(Definition of each 1M, any one relevant example of each 1M)

Ans.

1) 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.

Example:

Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are hot on hacker’s target lists and attacks on government websites receive wide press coverage.

2) Cracking

Cracking is the act of breaking into a computer system, often on a network. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Some breaking-and-entering has been done apparently to point out weaknesses in a site's security system.

Example:

1. Editing a program’s source code.
2. Creating a program, like a key generator or some sort of application that tricks an application in to thinking that a particular process has occurred.

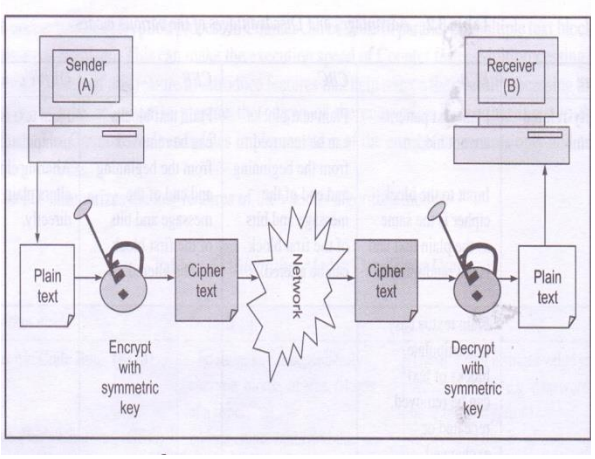
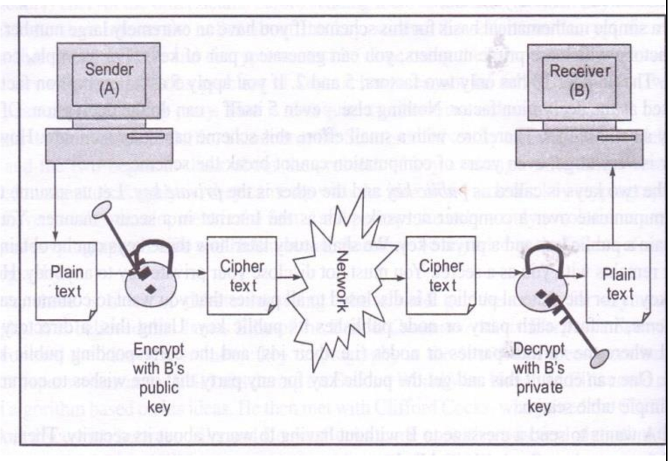
Q.1) B) Attempt any one: 6M

a) Differentiate between symmetric and asymmetric key cryptography.

(Any 6 relevant points each 1M)

Ans.

Symmetric Key Cryptography	Asymmetric Key Cryptography
1. In symmetric key cryptography only one key is used and the same key is used for both encryption and decryption of messages.	1. In asymmetric key cryptography two different keys are used. One key is used for encryption and other key is used for decryption.

2. Symmetric key cryptography:  Sender (A) Receiver (B) Plain text Cipher text Network Cipher text Plain text Encrypt with symmetric key Decrypt with symmetric key	2. Asymmetric key cryptography:  Sender (A) Receiver (B) Plain text Cipher text Network Cipher text Plain text Encrypt with B's public key Decrypt with B's private key
3. It is also referred to as Secret Key Cryptography or Private Key Cryptography	3. It is also referred to as Public Key Cryptography.
4. 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.	4. In this method the two keys are mathematically interrelated, but it's impossible to derive one key from the other.
5. 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.	5. Asymmetric-key confirms the sender's identity by double the encryption.
6. The most widely used symmetric ciphers are DES and AES.	6. Well-known asymmetric ciphers are the Diffie-Hellman algorithm, RSA, and DSA.

b) Describe IT Act 2000.

(Any 6 relevant points each 1M)

Ans. The IT Act 2000 gives very good solution to the cyber crimes these solutions are provided in the following ways. In this Act several sections and Chapters are there which are defined in the following manner:

1. Chapter 1 the preliminary chapter of IT Act 2000 gives all of the information about the short title, territory up to which it is extendable, and the basic application of related laws.
2. Chapter 2 to 7 of this Act defines 'access', 'addressee', 'adjudicating officer', 'affixing digital signature', 'Asymmetric Cryptography', 'cyber', 'computer', 'digital signature', 'Digital Signature Certificate' and other numerous basic terms, which are defined in its

appendix.

3. Other chapters of this Act define those crimes which can be considered as cognizable offences, i.e. for which the police can arrest the wrongdoer immediately.
4. Section 80 of this Act gives a freedom to the police officer to search, arrest the offender who is indulged in that crime or going to commit it.
5. Section 65 to 70 covers all of the cognizable offences, namely, 'tampering of documents', 'hacking of the personal computer', 'obscene information transmission or publication', 'failure of compliance by certifying authority or its employees, of orders of the Controller of certifying authorities', 'Access or attempt to access by any unauthorized person, a protected system notified by Govt. in the Official Gazette' in which non-bailable warrant is issued or no warrant is required as shown in table below.
6. Section 71 indicates the offence 'Misrepresentation of material fact from the controller or Certifying Authority for obtaining any license or Digital Signature Certificate'. In which bailable warrant may be issued covered in the table below.

Q.2) Attempt any two: 16M

a) Explain TCB (Trusted Computing Base) with respect to Information Security.
(Relevant Explanation with neat diagram 8M)

Ans.

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

1. Typically, all of hardware, the core OS that is involved in protection, and all programs that operate with system privileges
2. Desirable properties: – Small – Separable, well-defined – Independently-auditable Reference Monitor.
3. A reference monitor is a separable module that enforces access control decisions
4. All sensitive operations are routed through the reference monitor
5. The monitor then decides if the operation should proceed.

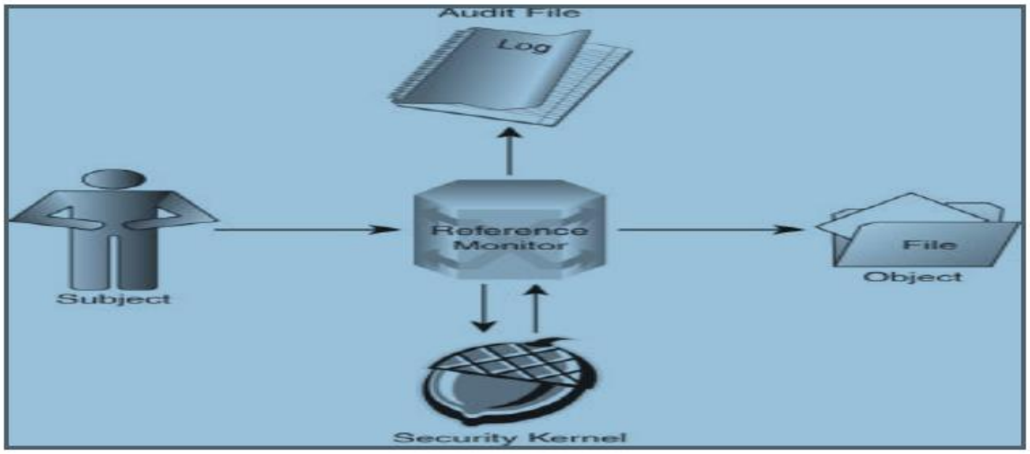


Fig: Reference Monitor

6. 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.
7. In Unix/Linux security kernel acts as a Reference Monitor which will handle all user application requests for access to system resources.
8. In trusted system Object is something that people want to access.
9. These objects (data) are labeled according to their level of sensitivity.
10. Subjects (users) should have same level of classification while accessing object.

The reference monitor has three properties:

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

b) Discuss Access Control? List types of access control and describe any two in brief.

(Access control 2M, Types of access control list (any 4) 2M, Description of any two types 2M each)

Ans.

Access control is a collection of mechanisms that work together to create security architecture to protect the assets of an information system. One of the goals of access control is personal accountability, which is the mechanism that proves someone performed a computer activity at a specific point in time.

Types of Access Controls:

1. Identification
2. Authentication
3. Least Privilege
4. Information Owner
5. Discretionary Access Control
6. Access Control Lists
7. Mandatory Access Control
8. Role Based Access Control

1. Identification:

Identification uniquely identifies the users of an information system. Identification equates to a user’s offline identity through his or her name, initials, e-mail address or a meaningless string of characters.

2. Authentication:

Authentication permits the system to verify one’s identification credential. Authenticating yourself to a system tells it the information you have established to prove that you are who you say you are.

Password, Signature, Photo are some examples which are used to identify a person.

3. Least Privilege:

The principle of least privilege is the predominant strategy to assure confidentiality. The objective is to give people the least amount of access to a system that is needed to perform the job they are doing. The need to know dictates the privilege to perform a transaction or access a resource.

4. Information Owner:

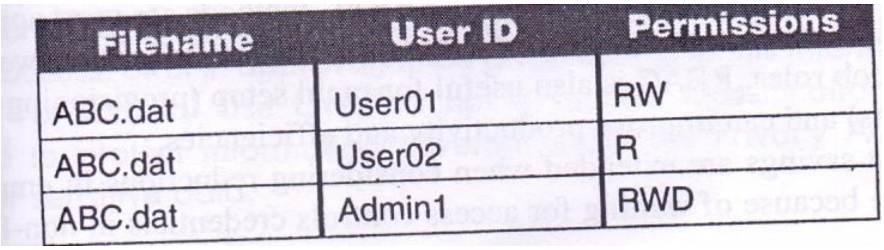
An information owner is one who maintains overall responsibility for the information within an information system. The information owner must be the one to make the decisions about who uses the system and how to recover the system in the event of disaster. e.g. Department head, Division executive.

5. Discretionary Access Control:

The principle of discretionary access control (DAC) dictates that the information owner is the one who decides who gets the access the system. DAC authority may be delegated to others who then are responsible for user setup, revocation and changes. Most of the common operating systems on the market today such as Windows, Macintosh, Unix rely on DAC principles for access and operation.

6. Access Control Lists:

An access control list (ACL) is simply a list of file of users who are given the privilege of access to a system or a resource. The privileges are Read, Write, Update, Execute, Delete or Rename. A system using ACL’s to protect data files might encode the permissions as shown in Table.



Filename	User ID	Permissions
ABC.dat	User01	RW
ABC.dat	User02	R
ABC.dat	Admin1	RWD

Table: Example users and permissions

7. Mandatory Access Control:

In a system that uses mandatory access control, the system decides who gains access to information based on the concepts of subjects, objects and labels. In a MAC environment, objects are labeled with a classification such as Secret, Top Secret and subjects or users are cleared to that class of object.

Subjects: The people or other systems that are granted a clearance to access an object within the information system.

Objects: The elements within the information system that are being protected from use or access.

Labels: The mechanism that binds objects to subjects. A subject's clearance permits access to an object based on the labeled security protection assigned to that object.

8. Role Based Access Control:

Role-based access control (RBAC) groups' users with a common access need. A role for a group of users who perform the same job functions and require similar access to resources. Role based controls simplify the job of granting and revoking access by simply assigning rights to the group for access control purposes. This is especially helpful where there is a high rate of employee turnover or frequent changes in employee roles.

c) Consider a Plain Text "INFORMATION SECURITY" convert given plain text into cipher text using single columnar transposition cryptography using following data:
No. of columns = 6
Encryption Key = 326154
(Preparing key 2M, Preparing Plain Text 2M, Encryption 2M, Ciphertext 2M)

Ans.

Given information is:

Plain Text: "INFORMATION SECURITY"

Encryption Key=326154

No of columns= 6

Preparing the key:

Divide the key given into no of columns given.

As per the given data key will be

3	2	6	1	5	4

Preparing the Plain Text:

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

As per the given data:

3	2	6	1	5	4
I	N	F	O	R	M
A	T	I	O	N	S
E	C	U	R	I	T
Y					

key

PlainText

Encryption:

Arrange the above message written in rows under the numbers of the key as per ascending order of the numbers at the top of the plaintext letters.

1	2	3	4	5	6
O	N	I	M	R	F
O	T	A	S	N	I
R	C	E	T	I	U
		Y			

Then letters are copied down column wise from top to bottom. The result is ciphertext.

CipherText is: OORNTCIAEYMSTRNIFIU

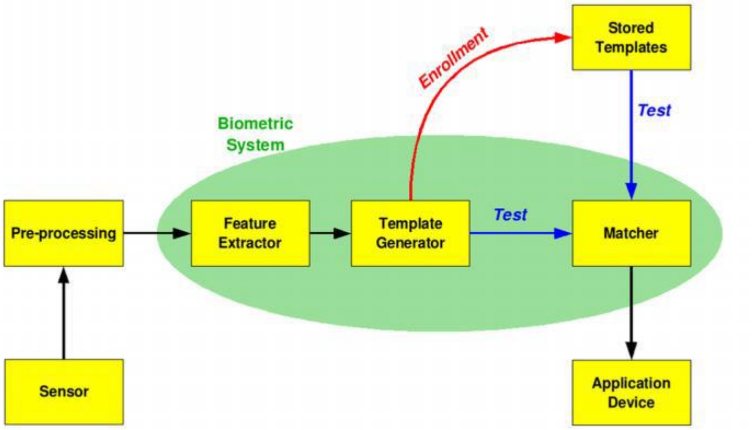
Q.3) Attempt any four: 16M

a) Explain in detail biometric authentication.

(Relevant explanation with correct diagram 4M)

Ans.

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.



1. The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of

a person. In the first step, reference models for all the users are generated and stored in the model database.

2. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison.
3. Second, in identification mode the system performs a one-to-many comparison against biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.
4. The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust.
5. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way.
6. During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements.

b) Explain one time PAD cryptography for encryption.
(Relevant explanation with example 4M)

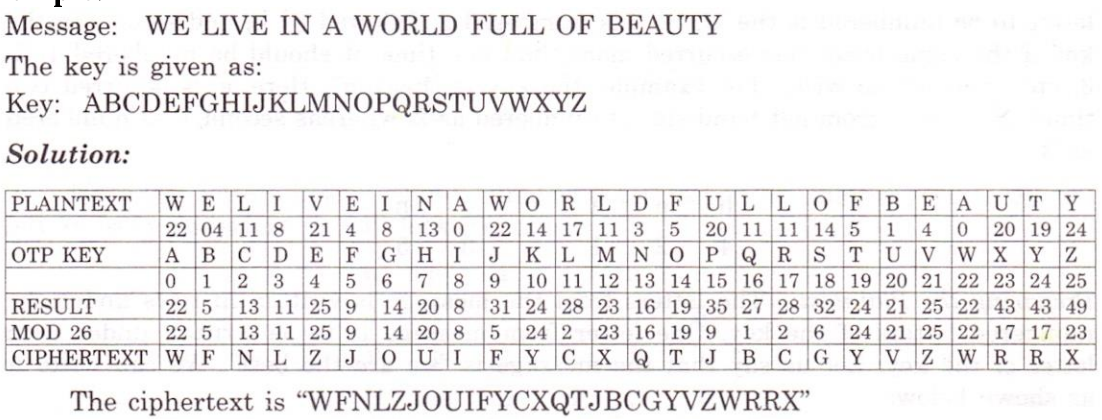
Ans.

One time pad also known as Vernam Cipher, is implemented using random set of non-repeating characters as the input cipher text. The most significant point here is that once an input cipher text for transposition is used, it is never used again for any other messages hence the name one time pad. The length of the input cipher text is equal to the length of the original plain text.

The algorithm used in the Vernam cipher / one time pad is described as follows:

1. Treat each plain text alphabet as a number in an increasing sequence i.e. A = 0, B = 1, …Z =25.
2. Do the same for each character of the input cipher text.
3. Add each number corresponding to the plain text alphabet to the corresponding input cipher text alphabet number.
4. If the sum thus produced is greater than 26, then subtract 26 from it.
5. Translate each number of the sum back to the corresponding alphabet. This gives the output cipher text.

Example:



Message: WE LIVE IN A WORLD FULL OF BEAUTY

The key is given as:

Key: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Solution:

PLAINTEXT	W	E	L	I	V	E	I	N	A	W	O	R	L	D	F	U	L	L	O	F	B	E	A	U	T	Y
	22	04	11	8	21	4	8	13	0	22	14	17	11	3	5	20	11	11	14	5	1	4	0	20	19	24
OTP KEY	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
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
RESULT	22	5	13	11	25	9	14	20	8	31	24	28	23	16	19	35	27	28	32	24	21	25	22	43	43	49
MOD 26	22	5	13	11	25	9	14	20	8	5	24	2	23	16	19	9	1	2	6	24	21	25	22	17	17	23
CIPHERTEXT	W	F	N	L	Z	J	O	U	I	F	Y	C	X	Q	T	J	B	C	G	Y	V	Z	W	R	R	X

The ciphertext is “WFNLZJOUIFYCXQTJBCGYVZWRRX”

c) **Define information. State need and importance of information.**
(Definition - 1M, Need and importance - 1M each (any 3 points))

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:

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

d) How to evaluate information security? Write down any two criterias to evaluate information security.
(Relevant explanation 4M)
Note: Any suitable explanation related to information security evaluation shall be considered.

Ans.

Information Technology security evaluation criteria (ITSEC):

ITSEC is developed by European country for security equation criteria.

1. ITSEC focuses more on integrity and availability. It tries to provide a uniform approach to product and system.
2. ITSEC will also provide security targets like:
    i. Policy for system security
    ii. Required mechanism for security
    iii. Required rating to claim for minimum strength
    iv. Level for evaluating targets –functional as well as evaluation

ITSEC classes contain hierarchical structure where every class will be added to the class above it. This class contains some particular function.
F-IN This class will provide high integrity.
F-AV This class will provide high availability.
F-DI This class will provide high data integrity.
F-DX This class is used for networks. Of provide high integrity while exchanging data in networking.
ITSEC uses following I 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.

- **BLP Model**

BLP is confidentiality models and it is used to describe what action must be taken to ensure the confidentiality of information.

BLP model defines the relationship between objects (the files, program, data) and subject (the person, process or device) relationship describe which level of access privilege applied to the subject on which object‘s.

BLP is a hierarchical State Machine model it has many layers.
BLP is a formal model of security policy which defines set of rules for access control.

- **BIBA Model**
  The Biba model has a similar structure to the BLP model, but it addresses integrity rather than confidentiality. Objects and users are assigned integrity levels that form a partial order, similar to the BLP model. The integrity levels in the Biba model indicate degrees of trust worthiness, or accuracy, for objects and users, rather than levels for determining confidentiality.
  - Clark and Wilson Model
  - Non-interference Model
  - State machine Model
  - Access Matrix Model
  - Information flow Model

e) Explain the following terms: -
1) Authorization
2) Authentication.
(Authorization 2M, Authentication 2M)

Ans.

Authorization:

It is a process of verifying that the known person has the authority to perform certain operation.
It cannot occur without authentication.
It is nothing but granting permissions and rights to individual so that he can use these rights to access computer resources or information.

Authentication:

Authentication is the process of determining identity of a user or other entity.
It is performed during log on process where user has to submit his/her username and password. There are three methods used in it.

1. Something you know
User knows user id and password.
2. Something you have
Valid user has lock and key.
3. Something about you
User's unique identity like fingerprints, DNA etc.

Q.4) A) Attempt any three: 12M

a) How to recover the data if the file is deleted?
(Relevant explanation 4M)

Ans.

There is no such thing as a permanently deleted file. If a recycle bin is empty, or a file is deleted with Shift + Delete button, it will simply kill the path that directs to the exact physical location where the file is stored. In hard drives, tracks are concentric circles and sectors are on the tracks like wedges. The disk rotates When want to access a file and the head reads the file from that sector. The same head also writes new data on sectors marked as available space. 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. Every computer file is a set of binary data i.e. in forms of l’s and 0’s. 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. 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 system‘s speed. Thus, it also involves a lot of over-writing on available space (where your deleted files may be). 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. 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.

b) Define term integrity. Explain integrity model with example.
(Definition of Integrity 1M, Integrity model with example 3M)

Ans.

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.

Integrity Model:

The BIBA Model

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)

c) Explain term "Kerberos" with an example.
(Relevant explanation 2M, example 2M)

Ans.

Kerberos

- Kerberos is a network authentication protocol and it is designed to provide strong authentication for Client /Server Applications. It uses secret- key Cryptography.
- Kerberos is a protocol which was created by MIT as a solution to network security problems. It uses strong cryptography hence a client can prove its identity to a server and vice versa over an in secure network connection.

Basics of Kerberos

- The basic Kerberos Model has the following participants:
- A Client
- A Server
- An Authentication Server (AS)
- A Ticket granting Server (TGS)

Example:

Suppose client (Samiksha) wants to communicate with server (Archana)
Using Kerberos protocol, Archana will verify the identity of samiksha and a session key will be established between Samiksha and Archana.

1. The Client (Samiksha) requests a ticket for ticket granting service from the authentication server. The authentication server has a strong database of password information for the entire clients.
2. AS returns an encrypted ticket i.e encrypted using Smaiksha's secret password information.
3. Samiksha wants to use the service that Archana (Server) provides. So Samiksha submits her ticket to the ticket granting server.

4. The ticket granting server verifies the ticket for identifying Samiksha and after verification gives a new ticket to Samiksha that will allow her to make use of Archana's Service.
5. Samiksha now has a service ticket which she can submit to Archana. She sends Archana the service ticket as well as authentication credential. Archana checks the ticket with the authentication credential to make sure whether it is a valid client or not. After verification, Archana will provide the service to Samiksha (the client).

d) Define security. State the needs of security.
(Definition 1M, need of security (any 3 points) 3M)

Ans.

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.

Need of Security:

1. **Security protecting the Functionality of an Organization.**
   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.
   For e.g. Managing payroll has more to do with management then Calculating wages, other things etc.
2. **Enabling the safe operation of application.**
   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.
3. **Protecting data that organization use and collect.**
   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.
4. **Safeguarding technology assets in organization.**
   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.

Q.4) B) Answer any one: 6M

a) Describe following with respect to cyber crime.

1) Intellectual property theft
2) Mail Bombs
3) Bug exploits.

(Description of Intellectual property theft 2M, Mail Bombs 2M, Bug exploits 2M)

Ans,

1. Intellectual property theft

Intellectual property is any innovation, commercial or artistic; any new method or formula with economic value; or any unique name, symbol, or logo that is used commercially. Intellectual property is protected by patents on inventions; trademarks on branded devices; copyrights on music, videos, patterns, and other forms of expression; and state and federal laws. Stealing intellectual property is cheap and easy. All a thief has to do is copy someone else's ideas or product. The other person or company—the victim—has done all the work, but thieves can reap huge profits. Intellectual property theft can cost people their jobs, damage the reputation of the original maker of the counterfeited product, cause sickness and bodily harm, deprive governments of desperately needed tax revenue, and even result in the spread of organized crime and gangs—which in turn can damage more lives and destroy neighborhoods.

2. Mail Bombs

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

3. Bug Exploits

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system.

b) Tell what is COBIT framework? List any four services provided by COBIT. What are the benefits after implementing COBIT framework?

(What is COBIT-2M, Any four Services 2M, Any two benefits 2M)

Ans.

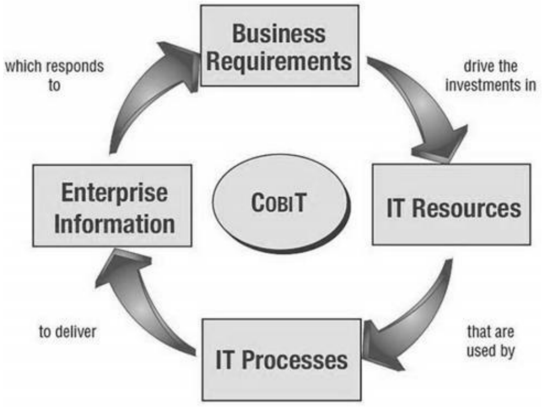
COBIT:

The Control Objectives for Information and related Technology (COBIT) is ―a control framework that links IT initiatives to business requirements, organizes IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered. The IT GOVERNANCE INSTITUTE (ITGI) first released it in 1995, and the latest update is version 4.1, published in 2007.

COBIT 4.1 consists of 7 sections, which are

1) Executive overview,
2) COBIT framework,
3) Plan and Organize,
4) Acquire and Implement,
5) Deliver and Support,
6) Monitor and Evaluate, and
7) Appendices, including a glossary.

Its core content can be divided according to the 34 IT processes. COBIT is increasingly accepted internationally as a set of guidance materials for IT governance that allows managers to bridge the gap between control requirements, technical issues and business risks. Based on COBIT 4.1, the COBIT Security Baseline focuses on the specific risks around IT security in a way that is simple to follow and implement for small and large organizations. COBIT can be found at ITGI or the Information Systems Audit and Control Association (ISACA) websites.



Services provided by the COBIT:

1. Manage operations
2. Manage service request and incidence
3. Manage problems
4. Manage continuity
5. Manage security services
6. Manage business process control

Benefits after implementing COBIT framework:

1. Maintaining high-quality information to support business decisions
2. Achieving strategic goals and realize business benefits through the effective and innovative use of IT

3. Achieving operational excellence through reliable, efficient application of technology
4. Maintaining IT-related risk at an acceptable level
5. Optimizing the cost of IT services and technology
6. Supporting compliance with relevant laws, regulations, contractual agreements and policies.

Q.5) Attempt any two: 16M

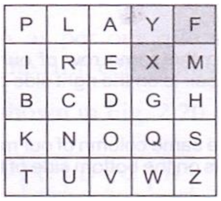
a) Consider a plain text "My name is Atul" convert given plain text into cipher text using "Playfair" cipher cryptography using Key-Playfair cipher example.
(Construction of Polybius square 1M, total 7 correct steps each 1M)

Ans.

1. First we break the original text into pairs of two alphabets each. This means that our original text would now look like this:

MY NAME IS ATUL

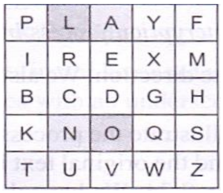
2. Now, we apply our Playfair Cipher algorithm to this text. The first pair of alphabets is MY. Looking at the matrix, we see the alphabets M and Y do not occur in the same row or column. Therefore, we need to apply step #5 of our Playfair cipher encryption process. This means that we need to replace this text with the text diagonally opposite to it. In this case, this text is XF, which is our first cipher text block. This is shown Fig .1



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

Fig. 1: Alphabet pair 1

3. Our next text block to be encrypted in NA. Again, step #5 will apply as depicted in Fig: 2

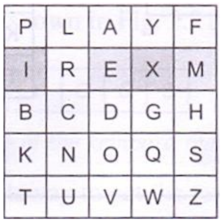


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Fig. 2: Alphabet pair 2

As we can see, our second block of cipher text is OL.

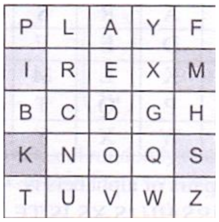
4. We will now take a look at the third block of plain text, which is ME. This is shown in Fig 3. We can see that the alphabets E and M making up this block are in the same (second) row. Therefore, based on our logic of step #3, the cipher text block would be IX.



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

Fig. 3: Alphabet pair 3

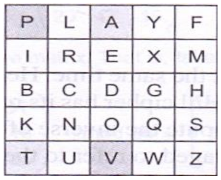
5. We will now take a look at the fourth block of plain text, which is IS. This is shown in Fig.4. We can see that we need to apply the logic of step #5 to get the diagonal alphabets. Based on this, the cipher text block would be MK.



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

Fig. 4: Alphabet pair 4

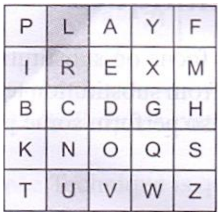
6. We will now take a look at the fifth block of plain text, which is AT. This is shown in Fig.5. We can see that we need to apply the logic of step#5 to get the diagonal alphabets. Based on this, the cipher text block would be PV.



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

Fig. 5: Alphabet pair 5

7. We will now take a look at the sixth and last block of plain text, which is UL. This is shown in Fig.6. We can see that the two alphabets U and L are in the same columns. Therefore, we need to apply the logic of step #4 to get the alphabets LR.



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

Fig. 6: Alphabet pair 6

Thus our plain text blocks MY NAME IS ATUL becomes XF OLIX MK PVLR

b) Describe following with respect to information security.

1) Risk Management

2) Security and Policies

3) Standards and guidelines

(Description of Risk Management with diagram 4M; Security and Policies: 2M; Standards and Guidelines: 1M each)

Ans.

1) 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,
- Risk assessment,
- Risk control.

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

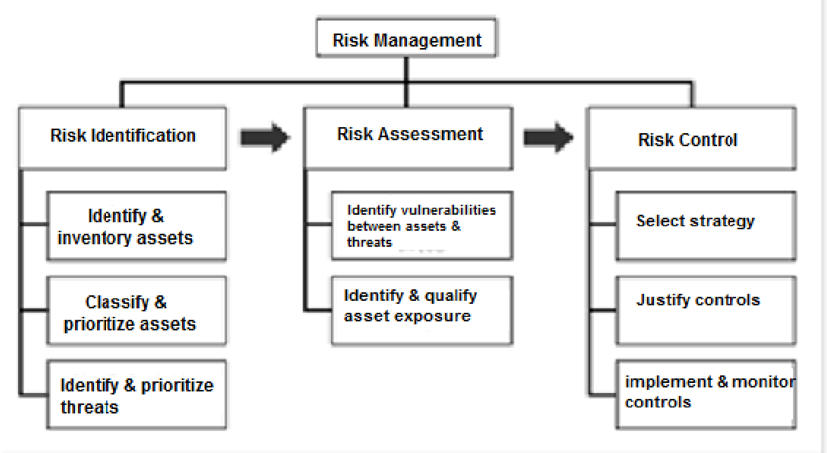

Risk Management
Risk Identification
Risk Assessment
Risk Control
Identify & inventory assets
Classify & prioritize assets
Identify & prioritize threats
Identify vulnerabilities between assets & threats
Identify & qualify asset exposure
Select strategy
Justify controls
implement & monitor controls

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.

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

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:

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.

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.

2) Security and Policies:-

Protection of information and the system that store and process this information is very much essential in this IT world.

It is required to implement rules and controls around the protection of information and the systems that store and process this information.

An information security policy consists of higher level statements relating to the protection of information across the business and should be by senior management.

Businesses may have a single encompassing policy or several specific policies that target different areas like

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

3) Standards And Guidelines:-

Standards:

Standard consists of specific low level mandatory controls that help enforce and support the information security policy. Standard helps to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or software. For example, a password standard may set out rules for password complexity and a Windows standard may set out the rules for hardening Windows clients

Guidelines:

1. It should consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.

2. It should view as best practices that neither are nor usually requirements, but are strongly recommended.

3. It can be consisting of additional recommended controls that support a standard or help to fill in the gaps where no specific standard applies.

4. A standard may require specific technical controls for accessing the internet securely and separate guidelines may be outline the best practices for using it.

c) Define virus. List four phases of viruses and how to deal with viruses.
(Definition of virus 2M, four phases 2M, dealing with virus 4M)

Ans. A **virus** is a computer program that attaches itself to another legitimate program and causes damage to the computer system or to the network.

During its lifetime, a virus goes through **four phases**:

(a) **Dormant phase**: Here, the virus is idle. It gets activated based on certain action or event (e.g. the user typing a certain key or certain date or time is reached, etc). This is an optional phase.

(b) **Propagation phase**: In this phase, a virus copies itself and each copy starts creating more copies of self, thus propagating the virus.

(c) **Triggering phase**: A dormant virus moves into this phase when the action/ event for which it was waiting is initiated.

(d) **Execution phase**: This is the actual work of the virus, which could be harmless (display some message on the screen) or destructive (delete a file on the disk).

Dealing with Viruses:

Preventing viruses is the best option. However, it is almost impossible to prevent them altogether with the world connected to the Internet all the time. We have to accept that viruses will attack and would need to find ways to deal with them. Hence, we can attempt to detect, identify and remove viruses.

Detection of viruses involves locating the virus, having known that a virus has attacked. Then we need to identify the specific virus that has attacked. Finally, we need to remove it. For this, we need to remove all traces of the virus and restore the affected programs/ files to their original states. This is done by anti-virus software.

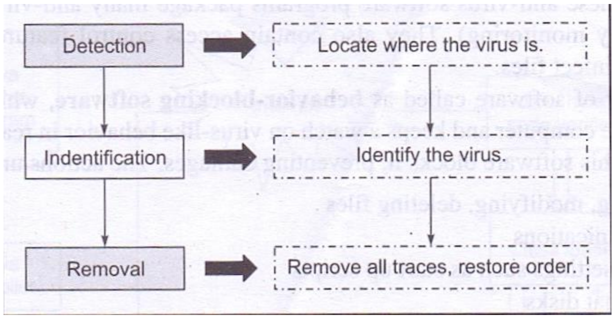


Fig: Virus elimination steps diagram

Generations of anti-virus software:

There are four generations of anti-virus software inclusive are first generation simple scanners, second generation heuristic scanners, third generation activity traps and fourth generation full featured protection. A first-generation scanner requires a virus signature to identify a virus which may contain wildcards but has essentially the same structure and bit pattern in all copies. Such signature-specific scanners are limited to the detection of known viruses. A second-generation scanner uses heuristic rules to search for probable virus infection, for example looking for fragments of code that are often associated with viruses. Another second-generation approach is integrity checking, using a hash function rather than a simpler checksum. Third-generation programs are memory-resident programs that identify a virus by its actions rather than structure in an infected program. These activity traps have the advantage that it is not necessary to develop signatures but only to identify the small set of actions indicating an infection is attempted and then intervene. Finally there is Fourth-generation products which are packages consisting of a variety of antivirus techniques used in conjunction by making use of scanning and activity traps. In addition, such a package includes access control capability, which limits the ability of viruses to penetrate a system and then limits the ability of a virus to update files in order to pass on the infection.

Q.6) Attempt any four: **16M**

a) List the various steps to create digital certificates.

(4 Steps: 1M each)

Ans.

Step1: Key generation:

Subject generates its own pair of keys. Registration Authority (RA) generating a key pair on behalf of the Subject.

Step 2: Registration:

Subject sends public key and evidences to the Registration Authority (RA).

Step 3: Verification:
After the registration process is complete the Registration Authority (RA) has to verify the user's credentials.

Step 4: Certificate Creation:
Assuming that all the steps so far have been successful the Registration Authority (RA) passes on all the details of the user to the CA (Certification Authority)

b) Explain the concepts of system security assurance.
(Relevant explanation 4M)

Ans. System Security Assurance Concepts:

In IT security system, there are two types of requirements:

- **Functional requirement:** It tells what system should do according to design.
- **Assurance requirement:** It tells in what way the functional requirement should be implemented and tested.

Both the above mentioned requirements should be able to answer- whether system do the right things in right way or not.

1. Goals of security Testing
2. Formal Security Testing Models

1. Goals of security Testing:

- Security testing will show the flaws in security mechanisms of an information system which protect the data/information and functionality as expected.
- This will verify the functions which are designed to achieve security and also validate the implementation of these functions - they are not faulty or random.
- Such type of testing will be done by expert users not by causal users.
- Security assurance and testing are ties together with many different concepts as well as principals and it is unfamiliar to many employees who are involved in IT development.

2. Formal Security Testing Models:

1) TCSEC: Trusted computer system evaluation criteria
2) ITSEC: Information Technology Security Evaluation Criteria
3) CTCPEC: Canadian Trusted Computer Product Evaluation
4) FC: Federal Criteria
5) Common Criteria:
    - TCSEC, CTCPEC and ITSEC are joint to support international separate criteria into a single set of IT security criteria and the name given as Common Criteria (CC).

c) Describe confidentiality model of information security.
(Relevant explanation: 4M)

Ans. Confidentiality Model of Information Security:

It is used to describe what actions must be taken to ensure the confidentiality of information.

It can specify how security tools are used to achieve the desired level of confidentiality.

Bell – LaPadula: -

The Bell-La Padula (BLP) model is a classic mandatory access-control model for protecting confidentiality.

The BLP model is derived from the military multilevel security paradigm, which has been traditionally used in military organizations for document classification and personnel clearance.

The BLP model has a strict, linear ordering on the security of levels of documents, so that each document has a specific security level in this ordering and each user is assigned a strict level of access that allows them to view all documents with the corresponding level of security or below.

How Bell LaPadula Works?

The security levels in BLP form a partial order,

Each object, x, is assigned to a security level, L(x). Similarly, each user, u, is assigned to a security level, L(u). Access to objects by users is controlled by the following two rules:

o Simple security property. A user u can read an object x only if

L(x) <L(u)

o 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.

d) Elaborate what is information classification? Describe any two criterias for the information classification.
(Elaboration with the any four terms: 2M, Any Two criteria: 2M)

Ans.

Classification of information is used to prevent the unauthorized disclosure and the resultant failure of confidentiality

Terms for information classification:

1. Unclassified

Information that is neither sensitive nor classified. The public release of this information does not violet confidentiality.

2. Sensitive but Unclassified (SBU)
Information that has been designated as a minor secret but may not create serious damage if disclosed.

3. Confidential
The unauthorized disclosure of confidential information could cause some damage to the country‘s national security.

4. Secret
The unauthorized disclosure of this information could cause serious damage to the countries national security.

5. Top secret
This is the highest level of information classification. Any unauthorized disclosure of top secret information will cause grave damage to the country‘s national security.

Criteria for information Classification:
1. Value
It is the most commonly used criteria for classifying data in private sector. If the information is valuable to an organization it needs to be classified.
2. Age
The classification of the information may be lowered if the information value decreases over the time.
3. Useful Life
If the information has been made available to new information, important changes to the information can be often considered.
4. Personal association
If the information is personally associated with specific individual or is addressed by a privacy law then it may need to be classified.

e) List any four authentication protocols. Explain any one authentication protocol.
(List of any four protocols 2M, explanation of any one 2M)

Ans.

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
   - After establishment of link, the server sends a challenge message to the client. Then client responds with a value obtained by using a one-way hash function.
   - Server compares the response i.e. hash value with its own calculated hash value.

- If the value matches, then the authentication is acknowledged or else the connection is terminated.

2) **EAP:** It is Extensible Authentication Protocol and mainly used for wireless networks and point to point connections. It may support various authentication mechanisms like tokens, certificate, one-time password, smart cards etc. In EAP protocol
   - A user requests connection to WLAN through an access point.
   - Then the access point requests identification (ID) data from the user and transmits that data to an authentication server.
   - The authentication server then request the access point for proof of the validity of the ID.
   - After the verification from the user, access point sends it back to the authentication server and the user is connected to the network.
3) **PAP:** It is Password Authentication Protocol. It is used by Point to Point Protocol to validate users before allowing them access to server resources. In this protocol, a user's name and password are transmitted over a network and compared to a table of name-password pairs. It is a two way handshaking protocol.
   - Client sends username and password.
   - Server sends "authentication-ack", if credentials are OK or "authentication-nak".
4) **SPAP:** It 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.
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.
8) **TACACS:** It is a Terminal Access Controller Access Control System. It is an older authentication protocol used mainly in UNIX networks. It allows a remote access server to pass a user's login password to an authentication server to check whether access can

be allowed to a given system or not. TACACS is an encryption protocol and therefore less secure.

9) **MS-CHAP(MD4):** It is a Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). It is based on CHAP and was developed to authenticate remote Windows-based workstations. It uses the Message Digest 4 (MD4) hashing algorithm and the Data Encryption Standard (DES) encryption algorithm to generate the challenge and response. It also provides mechanisms for reporting connection errors and for changing the user's password. It only works on Microsoft Systems.

10) **SKID (SKID2 and SKID3):** SKID2 and SKID3 are secrete key identification protocols. SKID2 provides unilateral entity authentication whereas SKID3 provides mutual entity authentication.