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.

1. a) Attempt any THREE of the following : Marks 12

(i) Define information. State need and importance of information.

(Definition - 1 Mark, Need and importance - 1 Mark each (any 3))

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.

(ii) State the meaning of information security and risk management with example.

(Meaning of Information Security - 1 Mark, Meaning of risk management - 1 Mark, Example - 1 Mark each)

Ans: **Information security:** sometimes shortened to Info Sec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Example of Information Security

- Unauthorized disclosure of sensitive information
- Theft or loss of equipment that contains private or potentially sensitive information
- Extensive virus or malware outbreak and/or traffic
- Attempts (either failed or successful) to gain unauthorized access to a system or it's data
- Compromised user account
  - Responding to a phishing email
- Extensive disruption of information services

Risk Management:-

Risk management is the keystone to an effective performance as well as for targeted, proactive solutions to potentials threats and incidents. Risk management is the ongoing process of identifying risk and implementing plans to address them.

Examples of Risk Management

- **Fire:** Damage cause to a system due to fire in the premises where information is preserve.
- **Flood:** Datacenter/ Information hub gets affected due to flood.

- **Loss of access:** Loss of account access due to loss of authenticity/ or loss of access credentials.
- **Cyber-attack:** Machines containing sensitive data are hijacked via the network.

(iii) Define cryptography. Explain application of cryptography. (Any three points)

(Definition-1 Mark, Application-1 Mark each (any 3))

Ans: **Cryptography**: it is the art 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.

(iv) Define cyber crime. How it is different from other crimes.

(Definition -1 Mark, Difference- 3 Marks (Any three distinguished points are expected))

Ans: **Definition of Cybercrime:**

Cybercrime is any illegal behavior, directed by means of electronic operations, that targets the security of computer system and the data processed by them.

- Since most of the cybercrime are an attack on data or information about individuals, organization, community, government. Generally the attacks do not take place on a physical body but it will be on the personal or corporate virtual body that means a set of informational attributes which define people and institutions etc. on the internet.
- There are transaction-based crimes like fraud, pornography digital piracy, money laundering, and counterfeiting.

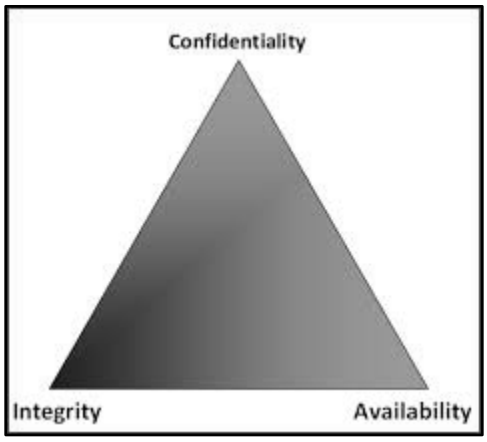
- Some crimes are specific crimes with specific victims; still the criminal hides it in the relative anonymity which is provided by the internet.
- With cybercrime integrity of information can be changed which results into repudiation of message origination.

b) Attempt any ONE of the following: Marks 06

(i) Explain importance of pillars of information security.

(Pillars - 2 Marks each)

Ans:



Confidentiality:

The concept of confidentiality is used as an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many mays, such as through the intentional release of private company information or through a misapplication of network rights.

Integrity:

This is yet another very important concept in information security. The concept of integrity ensures that:

1. Modifications are not made to data by authorized personnel or processes.
2. Unauthorized modifications are not made to data by authorized personnel or process.

3. The date are internally and externally consistent, this is internal information is consistent among all subentries and the internal information is consistent with the real world, external situation.

Availability:

This is the last of the important triad in information security. The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. In other words 'availability' guarantees that the systems are up and running when they are need. In addition, this concept guarantees that the security services needed by the security practitioner are in working order.

(ii) Explain different information security policies and guidelines.

(Security Policies - 4 Marks (one policy -1 Mark), Guidelines - 2 Marks)

Ans: Different Information Securities Policies:-

1. **Senior Management Statement of Policy:**

   This is the first step in the policy creation process. This is a general, high level statement of policy that contains the following elements:

   - An acknowledgement of the importance of computing and networking resources, that are part of the information system, to the organization's business model;
   - A statement of support for Information security throughout the business enterprises;
   - A commitment to authorize and manage the definition of the lower level standards, procedures and guidelines.

2. **Regulatory Policy:**

   These are security policies that an organization must implement owing to compliance, regulation or other legal requirements as prevalent in the organization's operating environment, both internal and external. The various entities with which the business organization interacts can be financial institutions, public utilities or some other types of organizations that operate in the public interest. Regulatory policies are usually very detailed and specific to the industry in which the business organization operates. The two main purposes of the regulatory policies are:

   - Ensuring that an organization follows the standard procedures or base practices of an operation in its specific industry.

- Giving an organization the confidence that it is following the standard and accepted industry policy.

3. Advisory Policy:

These are security policies that may not be mandated but are strongly recommended. Normally, the consequences of not following them are defined. An organization with such polies wants its employees to consider these polices mandatory. Most polices fall under this broad category.

4. Informative Policy:

These are polices that exist simply to inform the reader. There are no implied or specified requirements, and the audience for this information could be certain internal entities or external parties.

Guidelines:

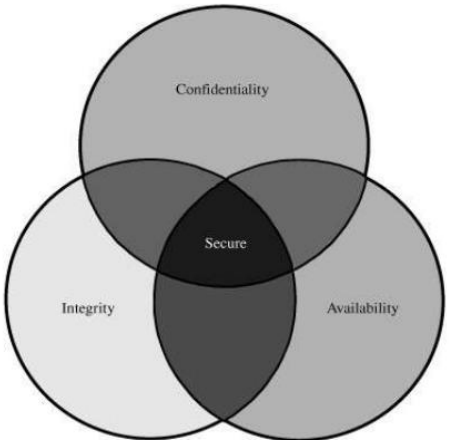
- It should consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.
- It should view as best practices that neither are nor usually requirements, but are strongly recommended.
- It can be consisting of additional recommended controls that support a standard or help to fill in the gaps where no specific standard applies.
- A standard may require specific technical controls for accessing the internet securely and separate guidelines may be outline the best practices for using it.

2. Attempt any TWO of the following: Marks 16

a) Explain basic principles of information security.

(Diagram - 2 Marks, Each principles - 2 Marks)

Ans:



Confidentiality:

The concept of confidentiality is used as an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many mays, such as through the intentional release of private company information or through a misapplication of network rights.

Integrity:

This is yet another very important concept in information security. The concept of integrity ensures that:

- Modifications are not made to data by authorized personnel or processes.
- Unauthorized modifications are not made to data by authorized personnel or process.
- The date are internally and externally consistent, this is internal information is consistent among all subentries and the internal information is consistent with the real world, external situation.

Availability:

This is the last of the important triad in information security. The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. In

other words 'availability' guarantees that the systems are up and running when they are need. In addition, this concept guarantees that the security services needed by the security practitioner are in working order

b) Explain any two substitution cipher you have studied.

(Any 2 Techniques are expected - 4 Marks each, for Description - 2 Marks, for example - 2 Marks (any relevant example shall be consider))

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 is

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

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.

In most networking situations, we can assume that the algorithms are known. What generally makes brute-force cryptanalysis impractical is the use of an algorithm that employs a large number of keys. For example, the triple DES algorithm makes use of a 168-bit key, giving a key space of or greater than 3.7 X 10^{50} possible keys.

Mono-alphabetic Ciphers:-

Major drawback of the Caesar cipher is its predictability. Once we decide to replace an alphabet in a plain-text message with an alphabet that is k positions up or down the order, one replace all other alphabets with same technique.

In mono alphabetic ciphers instead of using uniform scheme for all the alphabets in a given plain text messages, we decide to use random substitution. This means that in a given plain text message, each A can replace by any other alphabet (B through Z). The crucial difference being there is no relation between replacement of B and replacement of A.

Example:-

PLAIN	A	B	C	D	E	F	G	H	I	J	K	L	M
CIPHER	E	L	X	N	A	K	R	V	F	Z	O	Y	H

PLAIN	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CIPHER	C	M	Q	D	U	W	B	S	J	T	G	P	I

PLAIN TEXT: INFORMATION SECURITY

CIPHER TEXT: FCKMUHEBFMC WAXSUFBP

Homophonic Substitution Cipher:-

It is similar to mono alphabetic cipher. The only difference in homophonic substitution cipher is that the replacement alphabet set in case of simple substitution technique is fixed, in the case of homophonic substitution cipher, one plain text alphabet can map to more than one cipher text alphabet.

Example:-

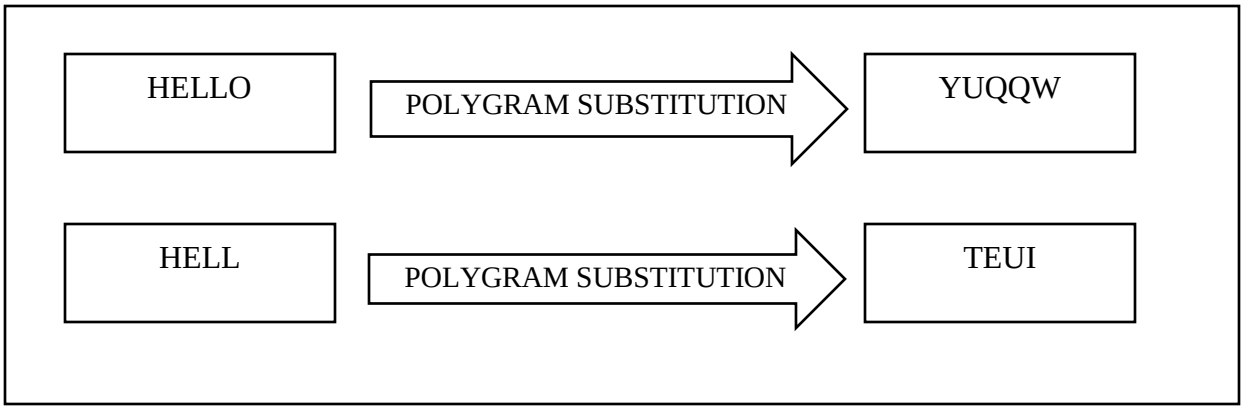
For example A can be replaced by any character.

PLAIN	I	N	F	O	R	M	A	T	I	O	N	S	E	C	U	R	I	T	Y
CIPHER	S	L	O	C	K	D	E	H	Z	J	N	B	A	Q	U	I	Y	W	F

Polygram Substitution Cipher:

In Polygram Substitution cipher instead of replacing one plain text alphabet with one cipher text alphabet at a time, a block of alphabets are replaced with another block. This is done by replacing a block with completely different cipher text block. This is true spite of the block that even though sub string among two blocks will be replaced by different strings of alphabets.

Example:-



Hill Cipher:-

Each letter is represented by a number modulo 26. (Often the simple scheme A = 0, B = 1, ..., Z = 25 is used, but this is not an essential feature of the cipher.) To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, again modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26). The cipher can, of course, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead of modulo 26.

Example:-

Consider the message 'ACT', and the key below (or GYBNQKURP in letters):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

Which corresponds to a cipher text of 'POH'. Now, suppose that our message is instead 'CAT', or:

$$\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$$

This time, the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

Which corresponds to a cipher text of 'FIN'. Every letter has changed. The Hill cipher has achieved Shannon's diffusion, and an n-dimensional Hill cipher can diffuse fully across n symbols at once.

Decryption

In order to decrypt, we turn the cipher text back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters). (There are standard methods to calculate the inverse matrix; see matrix inversion for details.) We find that, modulo 26, the inverse of the matrix used in the previous example is:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \pmod{26}$$

Taking the previous example cipher text of 'POH', we get:

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

which gets us back to 'ACT', just as we hoped.

The matrix will have an inverse if and only if its determinant is not zero. Also, in the case of the Hill Cipher, the determinant of the encrypting matrix must not have any common factors with the modular base. Thus, if we work modulo 26 as above, the determinant must be nonzero, and must not be divisible by 2 or 13. If the determinant is 0, or has common factors with the modular base, then the matrix cannot be used in the Hill cipher, and another matrix must be chosen (otherwise it will not be possible to decrypt). Fortunately, matrices which satisfy the conditions to be used in the Hill cipher are fairly common.

For our example key matrix:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} \equiv 6(16\cdot 15 - 10\cdot 17) - 24(13\cdot 15 - 10\cdot 20) + 1(13\cdot 17 - 16\cdot 20) \equiv 441 \equiv 25 \pmod{26}$$

So, modulo 26, the determinant is 25. Since this has no common factors with 26, this matrix can be used for the Hill cipher. The risk of the determinant having common factors with the modulus can be eliminated by making the modulus prime. Consequently a useful variant of the Hill cipher adds 3 extra symbols (such as a space, a period and a question mark) to increase the modulus to 29.

c) List and explain different data recovery tools with example.

(List - 2 Marks, Description of any 3 tools is expected - 2 Marks each)

Ans: Following are the data recovery tools:

- NTFS Data recovery tools
- FAT data recovery tool
- Digital Camera Data recovery tool
- Removable media data recovery tool

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

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 "overlooks" or 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, VFAT. Files up to 64 KB are recovered by FAT Recovery.

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

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:-

- CardRecovery
- PhotoRec
- Recover My Files
- Recuva

3. Attempt any FOUR of the following: Marks 16

a) Define the term confidentiality. Explain with example.

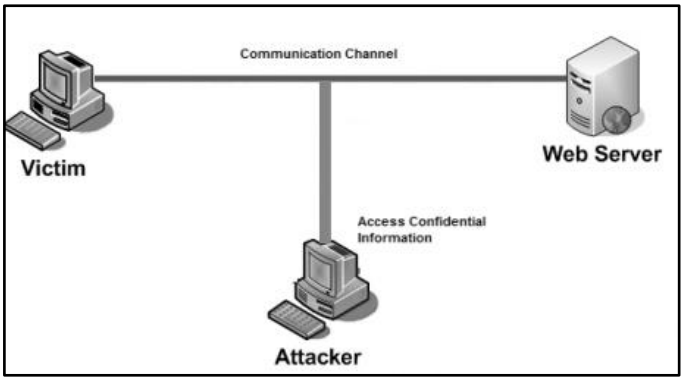
(Definition - 2 Marks, Description - 2 Marks)

Ans: Confidentiality:

The concept of confidentiality is used as an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many Mays, such as through the intentional release of private company information or through a misapplication of network rights.

The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of message. Confidentiality gets compromised if an unauthorized

person is able to access a message. An example of comprising the confidentiality of messages is shown in figure. Here the user of Victim computer sends a message to the user of computer Web Server. And another user Attacker gets access to this message which is not desired and therefore defeats the purpose of confidentiality. Interception can causes loss of message confidentiality.



b) Mention and explain any two classical encryption techniques.

(List - 2 Marks, Explanation - 1 Mark each (Any technique shall be considered)

Ans: Following are the Classical Encryption Techniques

- Substitution Ciphers
  - Caesar cipher
  - Monoalphabetic ciphers
  - Playfair cipher
  - Polyalphabetic ciphers
- Transposition (permutation) Ciphers
  - Rail Fence Cipher
  - Columnar Transposition Cipher
  - Row Transposition Cipher

Examples:-

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.

For 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

$$C = E(3, P) = (P + 3) mod 2$$

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

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

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.

In most networking situations, we can assume that the algorithms are known. What generally makes brute-force cryptanalysis impractical is the use of an algorithm that employs a large

number of keys. For example, the triple DES algorithm makes use of a 168-bit key, giving a key space of or greater than 3.7 X 10^{50} possible keys.

Mono-alphabetic Ciphers:-

Major drawback of the Caesar cipher is its predictability. Once we decide to replace an alphabet in a plain-text message with an alphabet that is k positions up or down the order, one replace all other alphabets with same technique.

In mono alphabetic ciphers instead of using uniform scheme for all the alphabets in a given plain text messages, we decide to use random substitution. This means that in a given plain text message, each A can replace by any other alphabet (B through Z). The crucial difference being there is no relation between replacement of B and replacement of A.

Example:-

PLAIN	A	B	C	D	E	F	G	H	I	J	K	L	M
CIPHER	E	L	X	N	A	K	R	V	F	Z	O	Y	H

PLAIN	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CIPHER	C	M	Q	D	U	W	B	S	J	T	G	P	I

PLAIN TEXT: INFORMATION SECURITY

CIPHER TEXT: FCKMUHEBFMC WAXSUFBP

Homophonic Substitution Cipher:-

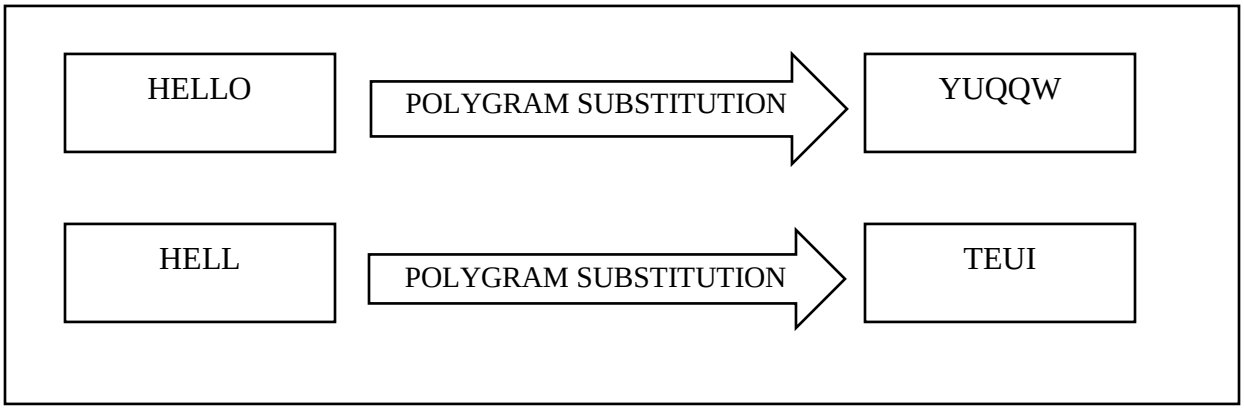
It is similar to mono alphabetic cipher. The only difference in homophonic substitution cipher is that the replacement alphabet set in case of simple substitution technique is fixed, in the case of homophonic substitution cipher, one plain text alphabet can map to more than one cipher text alphabet. For example A can be replaced by any character.

PLAIN	I	N	F	O	R	M	A	T	I	O	N	S	E	C	U	R	I	T	Y
CIPHER	S	L	O	C	K	D	E	H	Z	J	N	B	A	Q	U	I	Y	W	F

Polygram Substitution Cipher:

In Polygram Substitution cipher instead of replacing one plain text alphabet with one cipher text alphabet at a time, a block of alphabets are replaced with another block. This is done by replacing

a block with completely different cipher text block. This is true spite of the block that even though sub string among two blocks will be replaced by different strings of alphabets.



Hill Cipher:-

Each letter is represented by a number modulo 26. (Often the simple scheme A = 0, B = 1, ..., Z = 25 is used, but this is not an essential feature of the cipher.) To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, again modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26). The cipher can, of course, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead of modulo 26.

Consider the message 'ACT', and the key below (or GYBNQKURP in letters):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

Which corresponds to a cipher text of 'POH'. Now, suppose that our message is instead 'CAT', or:

$$\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$$

This time, the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

This corresponds to a cipher text of 'FIN'. Every letter has changed. The Hill cipher has achieved Shannon's diffusion, and an n-dimensional Hill cipher can diffuse fully across n symbols at once.

Decryption

In order to decrypt, we turn the cipher text back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters). (There are standard methods to calculate the inverse matrix; see matrix inversion for details.) We find that, modulo 26, the inverse of the matrix used in the previous example is:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \pmod{26}$$

Taking the previous example cipher text of 'POH', we get:

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

which gets us back to 'ACT', just as we hoped.

The matrix will have an inverse if and only if its determinant is not zero. Also, in the case of the Hill Cipher, the determinant of the encrypting matrix must not have any common factors with the modular base. Thus, if we work modulo 26 as above, the determinant must be nonzero, and must not be divisible by 2 or 13. If the determinant is 0, or has common factors with the modular base, then the matrix cannot be used in the Hill cipher, and another matrix must be chosen (otherwise it will not be possible to decrypt). Fortunately, matrices which satisfy the conditions to be used in the Hill cipher are fairly common.

For our example key matrix:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} \equiv 6(16 \cdot 15 - 10 \cdot 17) - 24(13 \cdot 15 - 10 \cdot 20) + 1(13 \cdot 17 - 16 \cdot 20) \equiv 441 \equiv 25 \pmod{26}$$

So, modulo 26, the determinant is 25. Since this has no common factors with 26, this matrix can be used for the Hill cipher. The risk of the determinant having common factors with the modulus can be eliminated by making the modulus prime. Consequently a useful variant of the Hill cipher adds 3 extra symbols (such as a space, a period and a question mark) to increase the modulus to 29.

Row Transposition:-

Variations of the basic transposition techniques such as rail fence technique exist. Such a scheme is given below which is known as Simple columnar Transposition technique or Row Transposition technique.

Algorithm/Steps:-

1. Write the plain text message row by row in a rectangle of a predefined size.
2. Read the message column by column, however, it need not be in the order of columns, it can be any random order.
3. The message thus obtained is the cipher text message.

Example:

Plain Text: "**Come Home Tomorrow"**

1. Consider a rectangle with six column and. Therefore, when the message is written in the rectangle row by row it will look as follow

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

2. Now, decide the order of columns as some random order, say, 4, 6, 1, 2, 5, 3 Then read the text in the order of these columns.
3. The cipher text obtained from it would be : **EOW OO CMR OER HM MTO**

While Decryption phase the cipher is written back in same rectangle with same size and all ciphers are placed as per the key.

c) Mention and explain integrity model.

(Description - 2 Marks; Rules - 2 Marks)

Ans: The 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.

For example, a file stored on a machine in a closely monitored data center would be assigned a higher integrity level than a file stored on a laptop. In general, a data-center computer is less likely to be compromised than a random laptop computer. Likewise, when it comes to users, a senior employee with years of experience would have a higher integrity level than an intern.

The Biba Model Rules

The access-control rules for Biba are the reverse of those for BLP. That is, Biba does not allow reading from lower levels and writing to upper levels.

If we let I (u) denote the integrity level of a user u and I(x) denote the integrity level for an object, x, we have the following rules in the Biba model:

A user u can read an object x only if $I(u) \leq I(x)$.

A user u can write (create, edit or append to) an object x only if $I(x) \leq I(u)$.

Thus, the Biba rules express the principle that information can only flow down, going from higher integrity levels to lower integrity levels.

d) Explain row transposition cipher with example.

(Description - 2 Marks, Example - 2 Marks)

Ans: Variations of the basic transposition techniques such as rail fence technique exist. Such a scheme is given below which is known as Simple columnar Transposition technique or Row Transposition technique.

Algorithm/Steps:-

1. Write the plain text message row by row in a rectangle of a predefined size.
2. Read the message column by column, however, it need not be in the order of columns, it can be any random order.
3. The message thus obtained is the cipher text message.

Example:

Plain Text: "**Come Home Tomorrow"**

4. Consider a rectangle with six column and. Therefore, when the message is written in the rectangle row by row it will look as follow

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

5. Now, decide the order of columns as some random order, say, 4, 6, 1, 2, 5, 3 Then read the text in the order of these columns.
6. The cipher text obtained from it would be : **EOW OO CMR OER HM MTO**

While Decryption phase the cipher is written back in same rectangle with same size and all ciphers are placed as per the key.

e) Explain the importance of Intellectual property laws.

(Any four importance - 4 Marks (1 Mark for each importance))

Ans: Intellectual proper is a generic term for legal entitlements attached to certain names, written and recorded media and inventions. The holders of these legal entitlements may exercise various exclusive rights in relation to the subject matter of the intellectual property. The word intellectual indicates the fact that this term concerns a process of the mind. The property implies that ideation is analogous to the construction of tangible objects. Intellectual property law and enforcement vary widely from jurisdiction to jurisdiction. Intellectual property laws confer a bundle of exclusive rights in relation to the particular form or manner in which ideas or information are expressed or manifested, and not in relation to the ideas or concepts themselves. The term intellectual property denotes the specific legal rights that authors, inventors and other intellectual property holders may hold and exercise and not the intellectual work itself.

Intellectual property laws are designed to protect different forms of subject matter, although in some cases there is a degree of overlap:

1. Copyrights
2. Patents
3. Trademark
4. Trade Secret
5. Trade Name
6. Domain Name.

Traditionally, businesses have thought of their physical assets, such as land, buildings, and equipment as the most important.

Increasingly, however, a company's intellectual assets are the most important.

4. a) Attempt any THREE of the following: Marks 12

(i) Explain different security standards.

(Any two standards are expected- 2 Marks for each)

Ans: ISO/IEC 27001:2005 (Information Security Management System - Requirements)

The international standard ISO/IEC 27001:2005 has its roots in the technical content derived from BSI standard BS7799 Part 2:2002. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within an organization. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets. This standard is usually applicable to all types of organizations, including business enterprises, government agencies, and so on. The standard introduces a cyclic model known as the "Plan-Do-Check-Act" (PDCA) model that aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS. The PDCA cycle has these four phases:

a) "Plan" phase – establishing the ISMS

b) "Do" phase – implementing and operating the ISMS

c) "Check" phase – monitoring and reviewing the ISMS

d) "Act" phase – maintaining and improving the ISMS

Often, ISO/IEC 27001:2005 is implemented together with ISO/IEC 27002:2005. ISO/IEC 27001 defines the requirements for ISMS, and uses ISO/IEC 27002 to outline the most suitable information security controls within the ISMS.

ISO/IEC 27002 is a code of practice that provides suggested controls that an organization can adopt to address information security risks. These controls are not mandatory. There is therefore no certification for ISO/IEC 27002, but a company can be certified compliant with ISO/IEC 27001 if the management process follows the ISMS standard. There is a list of accredited certification bodies that can certify an organization against the ISMS standard, which is maintained on the UK Accreditation Service website.

CARD INDUSTRY DATA SECURITY STANDARD

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by a number of major credit card companies (including American Express, Discover Financial Services, JCB,

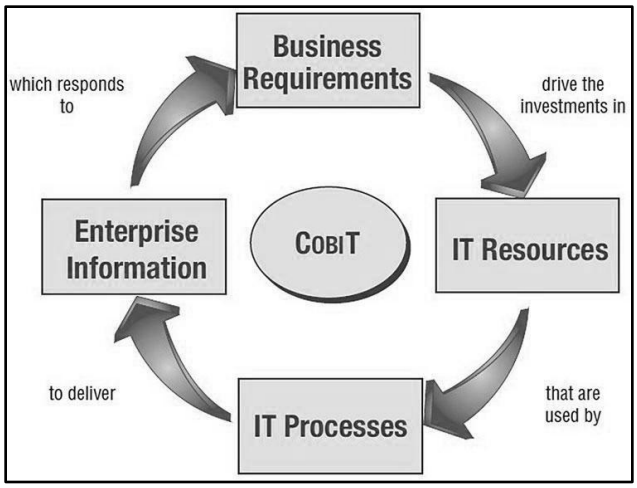
MasterCard Worldwide and Visa International) as members of the PCI Standards Council to enhance payment account data security. The standard consists of 12 core requirements, which include security management, policies, procedures, network architecture, software design and other critical measures. These requirements are organized into the following areas:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

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.

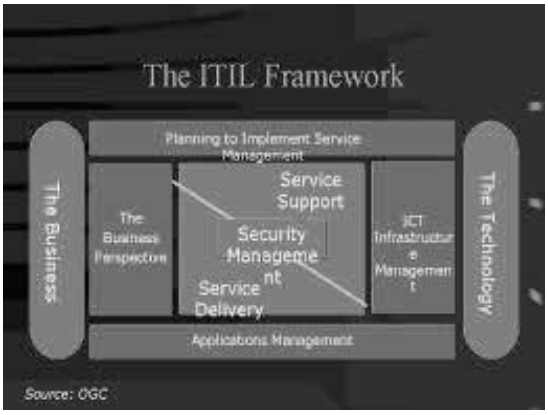
COBIT is increasingly accepted internationally as a set of guidance materials for IT governance that allows managers to bridge the gap between control requirements, technical issues and business risks. Based on COBIT 4.1, the COBIT Security Baseline focuses on the specific risks around IT security in 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.



ITIL (OR ISO/IEC 20000 SERIES)

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.



(ii) Describe TCSEC.

(Any relevant description shall be consider; Description - 1 Mark, Policy - 1 Mark, Accountability - 1 Mark, Classes - 1 Mark)

Ans: Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DOD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information.

Policy: The security policy must be explicit, well-defined and enforced by the computer system. There are three basic security policies:

Mandatory Security Policy - Enforces access control rules based directly on an individual's clearance, authorization for the information and the confidentiality level of the information being sought. Other indirect factors are physical and environmental. This policy must also accurately reflect the laws, general policies and other relevant guidance from which the rules are derived.

Marking - Systems designed to enforce a mandatory security policy must store and preserve the integrity of access control labels and retain the labels if the object is exported.

Discretionary Security Policy - Enforces a consistent set of rules for controlling and limiting access based on identified individuals who have been determined to have a need-to-know for the information.

Accountability

Individual accountability regardless of policy must be enforced. A secure means must exist to ensure the access of an authorized and competent agent which can then evaluate the accountability information within a reasonable amount of time and without undue difficulty. There are three requirements under the accountability objective:

Identification - The process used to recognize an individual user.

Authentication - The verification of an individual user's authorization to specific categories of information.

Auditing - Audit information must be selectively kept and protected so that actions affecting security can be traced to the authenticated individual.

Divisions and classes

The TCSEC defines four divisions: D, C, B and A where division A has the highest security. Each division represents a significant difference in the trust an individual or organization can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1.

Each division and class expands or modifies as indicated the requirements of the immediately prior division or class.

- **D — Minimal protection**

  Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division
- **C — Discretionary protection**
  - C1 — Discretionary Security Protection
  - C2 — Controlled Access Protection
- **B — Mandatory protection**
  - B1 — Labeled Security Protection
  - B2 — Structured Protection
  - B3 — Security Domains
- A — Verified protection
  - A1 — Verified Design
  - Beyond A1

(iii) Define physical access control and mention physical access threats.

(Definition - 2 Marks, Physical access threats - 2 Marks (any 4))

Ans: Definition:-

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

Physical Access Threats

- Weather
  - Temperature, humidity, water, flood, wind snow, lightening, etc.
- Fire and Chemical
  - Explosion, smoke, toxic, material. Industrial pollutions, etc.
- Earth Movement
  - Earthquake, volcano, slide, etc.
- Object Movement
  - Building collapse, falling object, car, truck, plane, etc.
- Energy
  - Electricity, magnetism, radio wave anomalies, etc.
- Organism
  - Virus, bacteria, animal, insect, etc.
- Equipment
  - Mechanical or electronic component failure, etc
- Human
  - Strike, war, sabotage, etc.

(iv) Explain the meaning of Stegnography and Digital signature. Give example.

(Stegnography - 2 Marks, Digital Signature - 2 Marks, Any relevant example shall be consider)

Ans: Steganography:-

The art and science of hiding information by embedding messages within other, seemingly harmless messages. Stegnography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

Stegnography sometimes is used when encryption is not permitted. Or, more commonly, Stegnography is used to supplement encryption. An encrypted file may still hide information using Stegnography, so even if the encrypted file is deciphered, the hidden message is not seen.

Digital Certificate:-

A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may also be referred to as a public key certificate.

Just like a passport, a digital certificate provides identifying information is forgery resistant and can be verified because it was issued by an official, trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real.

To provide evidence that a certificate is genuine and valid, it is digitally signed by a root certificate belonging to a trusted certificate authority. Operating systems and browsers maintain lists of trusted CA root certificates so they can easily verify certificates that the CAs have issued and signed. When PKI is deployed internally, digital certificates can be self-signed.

b) Attempt any ONE of the following: Marks 06

(i) List different authentication protocols and explain any two in detail.

(List - 2 Marks, description of any two protocols - 2 Marks)

Ans:

- Direct authentication
  - Based on a shared secret master key
  - Based on a public-key system
  - Diffie-Hellman
- Mediated authentication
  - Based on key distribution centers
  - Otway-Rees
  - Kerberos

Based on a shared secret master key:-

Assume here that A and B already share a secret key – this is called sometimes the master key MK because the two will only use this rarely, whenever they need to authenticate each other and establish a session key

- Master keys will only be used to establish session keys
- Concentrate here on how to establish session keys

Protocol: A issues a requests to B for a session key and includes a nonce N_1

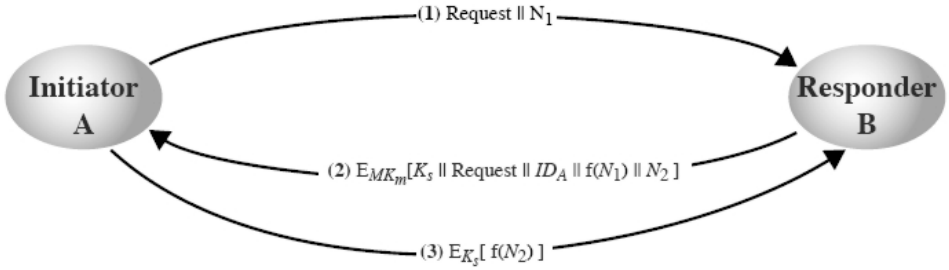
B responds with a message encrypted using the shared master key – include there the session key he selects, A's id, a value f(N_1) (say the successor of N_1) and another nonce N_2

- At this point, A is sure of B's identity: only he knows the master key; B is not sure of anything yet
- A knows that the message is fresh: B sends a transformation on N_1

Using the new session key, A return f(N_2) to B

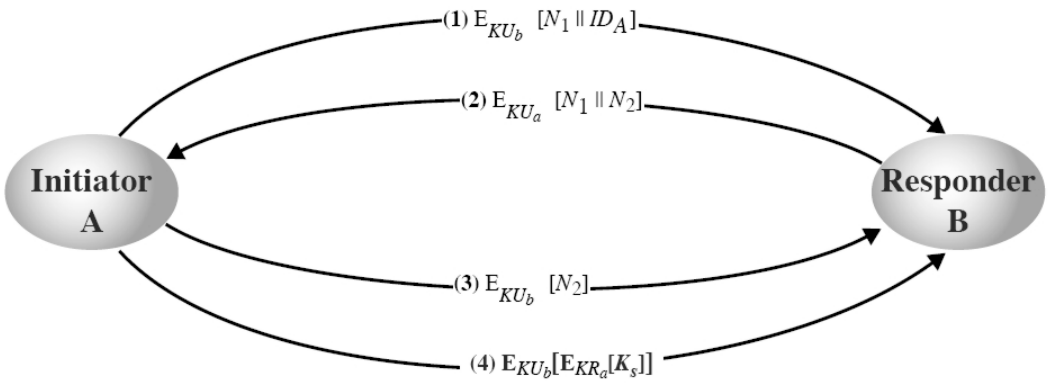
B is sure of A's identity: only A can read the message he sent, including the session key

B knows that the message is fresh: A sends a transformation on N_2



A general scheme of public-key authentication (and distribution of secret keys)

- Assume here that A and B know each other's public key N_1 and N_2 in the scheme are random numbers – they ensure the authenticity of A and B (because only they can decrypt the messages and read N_1 and N_2)
- After Step 2, A is sure of B's identity: right response to its challenge.
- After Step 3, B is sure of A's identity: right response to its challenge.



Diffie-Hellman key exchange

This is the first ever published public-key algorithm – used in a number of commercial products elegant idea: establish a secret key based on each other's public keys

Protocol Alice and Bob need to agree on two large numbers n,g, where n is prime, (n-1)/2 is also prime and some extra conditions are satisfied by g (to defeat math attacks) – these numbers may be public so Alice could generate this on her own

Alice picks a large (say, 512-bit) number x and B picks another one, say y

Alice initiates the key exchange protocol by sending Bob a message containing $(n,g,g^x \bmod n)$

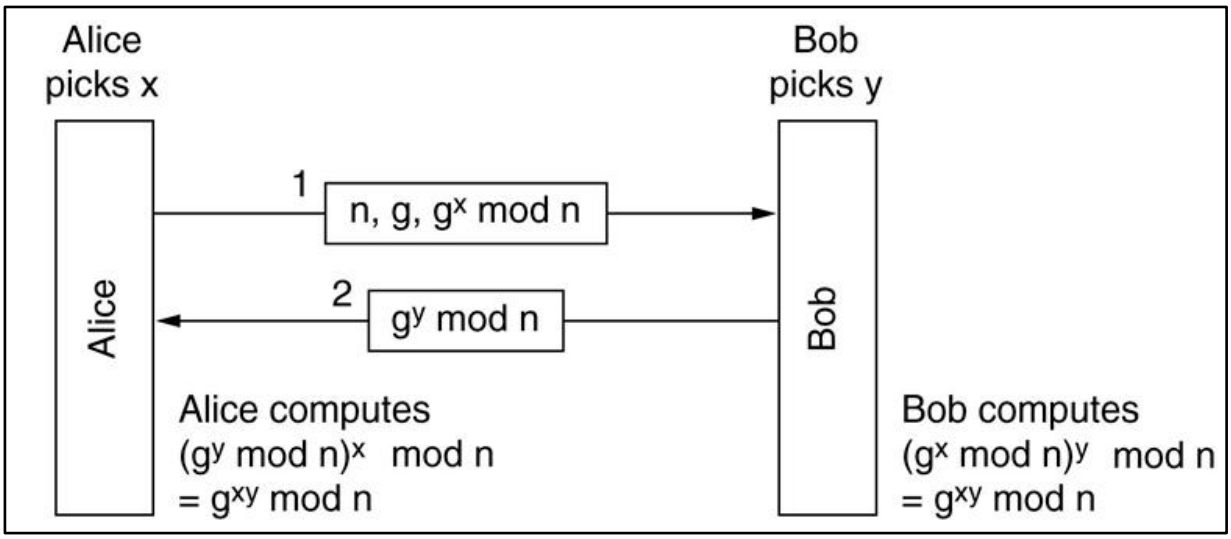
Bob sends Alice a message containing $g^y \bmod n$

Alice raises the number Bob sent her to the x-th power mod n to get the secret key:

$$(g^y \bmod n)^x \bmod n = g^{xy} \bmod n$$

Bob raises the number Alice sent to the y-th power modulo n to get the secret key:

$$(g^x \bmod n)^y \bmod n = g^{xy} \bmod n$$



Based on key distribution centers:-

Setting up a shared key was fairly involved with the previous approaches and perhaps not quite worth doing ("sour grape attack") Each user has to maintain a secret key (perhaps on some plastic card) for each of his friends – this may be a problem for popular people

Different approach: have a trusted key distribution center (KDC)

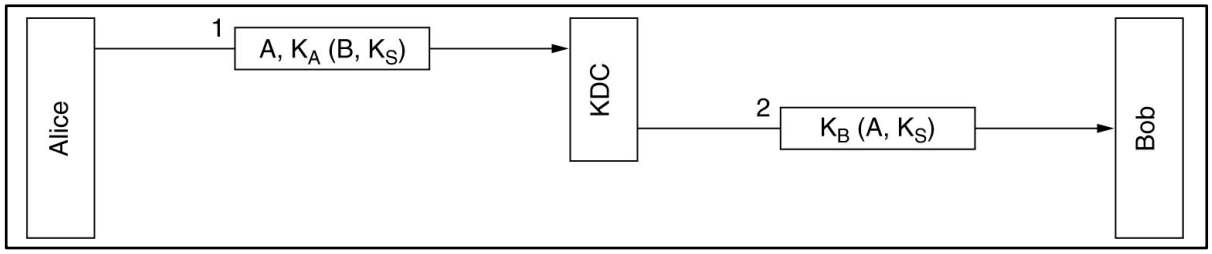
Each user maintains one single secret key – the one to communicate with KDC

Authentication and all communications go through KDC

Alice picks K_s and tells KDC that she wants to talk to Bob using K_s – A uses secret key K_A used only to communicate with KDC

KDC decrypts the message and sends K_s to Bob together with Alice's id – KDC uses key K_B used only to communicate with B

Authentication here is for free – key K_A is only known to A and KDC



Kerberos Terminology

The following glossary defines some Kerberos terminology.

Credential: Users or clients need to present some kind of credentials that authorize them to request services. Kerberos knows two kinds of credentials—tickets and authenticators.

Ticket: A ticket is a per-server credential used by a client to authenticate at a server from which it is requesting a service. It contains the name of the server, the client's name, the client's Internet address, a time stamp, a lifetime, and a random session key. All this data is encrypted using the server's key.

Authenticator: Combined with the ticket, an authenticator is used to prove that the client presenting a ticket is really the one it claims to be. An authenticator is built using the client's name, the workstation's IP address, and the current workstation's time, all encrypted with the session key known only to the client and the relevant server. An authenticator can only be used once, unlike a ticket. A client can build an authenticator itself.

Principal: A Kerberos principal is a unique entity (a user or service) to which it can assign a ticket. A principal consists of the following components:

- **Primary**—the first part of the principal, which can be the same as your username in the case of a user.
- **Instance**—some optional information characterizing the primary. This string is separated from the primary by a /.
- **Realm**—this specifies your Kerberos realm. Normally, your realm is your domain name in uppercase letters.

Mutual authentication: Kerberos ensures that both client and server can be sure of each other's identity. They share a session key, which they can use to communicate securely.

Session key: Session keys are temporary private keys generated by Kerberos. They are known to the client and used to encrypt the communication between the client and the server for which it requested and received a ticket.

Replay: Almost all messages sent in a network can be eavesdropped, stolen, and resent. In the Kerberos context, this would be most dangerous if an attacker manages to obtain your request for a service containing your ticket and authenticator. The attacker could then try to resend it (*replay*) to impersonate you. However, Kerberos implements several mechanisms to deal with this problem.

Server or service: *Service* is used to refer to a specific action to perform. The process behind this action is referred to as a *server*.

How Kerberos Works?

Kerberos is often called a third party trusted authentication service, which means all its clients trust Kerberos's judgment of another client's identity. Kerberos keeps a database of all its users and their private keys.

To ensure Kerberos is working correctly, run both the authentication and ticket-granting server on a dedicated machine. Make sure that only the administrator can access this machine physically and over the network. Reduce the (networking) services running on it to the absolute minimum—do not even run sshd.

(ii) Explain one time Pad cipher and Hill cipher with example.

(One time pad -2 Marks, Hill cipher - 2 Marks, 1 Mark for each example)

Ans: One Time Pad:-

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 message 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: - Plain Text = ***"BEING HUMAN"***

1 PLAIN TEXT	B	E	I	N	G	H	U	M	A	N
	1	4	8	13	6	7	20	12	0	13
+										
2 ONE TIME PAD	O	R	D	I	N	A	R	I	L	Y
	14	17	3	8	13	0	17	8	11	25
3. INITIAL TOTAL	15	21	11	21	19	7	**37**	20	11	**38**
4. SUBTRACT 26, IF >26	15	21	11	21	19	7	11	20	11	12
5. CIPHER TEXT	Q	V	L	V	T	H	L	V	L	M

It should be clear that since the one time pad is discarded after a single use, this technique is a highly secure and for small plain text message, but is clearly impractical for large messages. The vermin cipher was first implemented at AT & T with the help of a device called the vermin machine.

One time pad is discarded after single use and therefore is suitable only for short messages.

Hill Cipher:-

Each letter is represented by a number modulo 26. (Often the simple scheme A = 0, B = 1, ..., Z = 25 is used, but this is not an essential feature of the cipher.) To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, again modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26). The cipher can, of course, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead of modulo 26.

Consider the message 'ACT', and the key below (or GYBNQKURP in letters):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

This corresponds to a cipher text of 'POH'. Now, suppose that our message is instead 'CAT', or:

$$\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$$

This time, the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

This corresponds to a cipher text of 'FIN'. Every letter has changed. The Hill cipher has achieved Shannon's diffusion, and an n-dimensional Hill cipher can diffuse fully across n symbols at once.

Decryption

In order to decrypt, we turn the cipher text back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters). (There are standard methods to calculate the inverse matrix; see matrix inversion for details.) We find that, modulo 26, the inverse of the matrix used in the previous example is:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \pmod{26}$$

Taking the previous example cipher text of 'POH', we get:

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

which gets us back to 'ACT', just as we hoped.

The matrix will have an inverse if and only if its determinant is not zero. Also, in the case of the Hill Cipher, the determinant of the encrypting matrix must not have any common factors with the modular base. Thus, if we work modulo 26 as above, the determinant must be nonzero, and must not be divisible by 2 or 13. If the determinant is 0, or has common factors with the modular base, then the matrix cannot be used in the Hill cipher, and another matrix must be chosen (otherwise it will not be possible to decrypt). Fortunately, matrices which satisfy the conditions to be used in the Hill cipher are fairly common.

For our example key matrix:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} \equiv 6(16 \cdot 15 - 10 \cdot 17) - 24(13 \cdot 15 - 10 \cdot 20) + 1(13 \cdot 17 - 16 \cdot 20) \equiv 441 \equiv 25 \pmod{26}$$

So, modulo 26, the determinant is 25. Since this has no common factors with 26, this matrix can be used for the Hill cipher. The risk of the determinant having common factors with the modulus can be eliminated by making the modulus prime. Consequently a useful variant of the Hill cipher adds 3 extra symbols (such as a space, a period and a question mark) to increase the modulus to 29.

5. Attempt any <u>TWO</u> of the following: Marks 16

a) How do you recover the data in below situations

(i) Deleted file recovery

(ii) Formatted partition recovery

(Situation- 4 Marks for each)

Ans:

(i) Deleted file recovery

- There is no such thing as a permanently deleted file. If a recycle bin is empty, or a file is deleted with Shift + Delete button, it will simply kill the path that directs to the exact physical location where the file is stored.
- In hard drives, tracks are concentric circles and sectors are on the tracks like wedges. The disk rotates When want to access a file and the head reads the file from that sector. The same head also writes new data on sectors marked as available space.
- 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 ls and Os. The physical space is declared as available space for new data to be written when a file is deleted. So if anyone performs any new activity on a disk after deleting a file, then there is a chance that the file would be replaced partially or completely by new data.
- 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.

(iii) Formatted partition recovery

- 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 tiles 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. Causes for partition damage generally include following types
  (i) Improper operation
  (ii) Virus attack
  (iii) Installation of defective software
- 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 U3 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.
- It is necessary to understand that nothing is erased from a disk, it's just made inaccessible after deletion, and the space is made available as free space to all other programs. This means, nothing is truly deleted until it's over written with a new file. Now the recommendation is to take the disk out of the system, and get one of the enclosures that power up, the hard drive and

come with a USB interface. By a hard-drive-to-USB enclosure, one can be able to connect the hard drive as an external USB to a working system.

- As if the hard drive is formatted, then the new system will not show any data on it. Do not write anything on the hard drive. Keep in mind that the hard drive is to be recovered from, not to be written on. Install data recovery software on the working system's hard drive.
- It is also possible to install an image creating tool to create a disk image. By running the image creation tool, anyone can create an image of the formatted drive and save it on a separate drive. Mount that image on a virtual disk creator, and run data recovery software on it. When the scan is complete and the software gives the list of recoverable files, make sure that the recovered files are needed to save to another destination.
- The disk image creation requires a lot of disk space because it may be of the same size as the formatted disk, hence the primary drive should have enough capacity.
- So, the safest Way to recover files from a formatted drive is to create an image, recover data from it, and save the recovered files in a separate place. Once all important files are recovered, it is possible to take the hard drive out of the enclosure and put it back into the system.

b) Explain following with their usage

(i) Karberos

(ii) Biometrics

(For each Diagram- 2 Marks, For each Explanation - 2 Marks)

Ans:

(i) Karberos

Kerberos is a computer network authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

Usage:

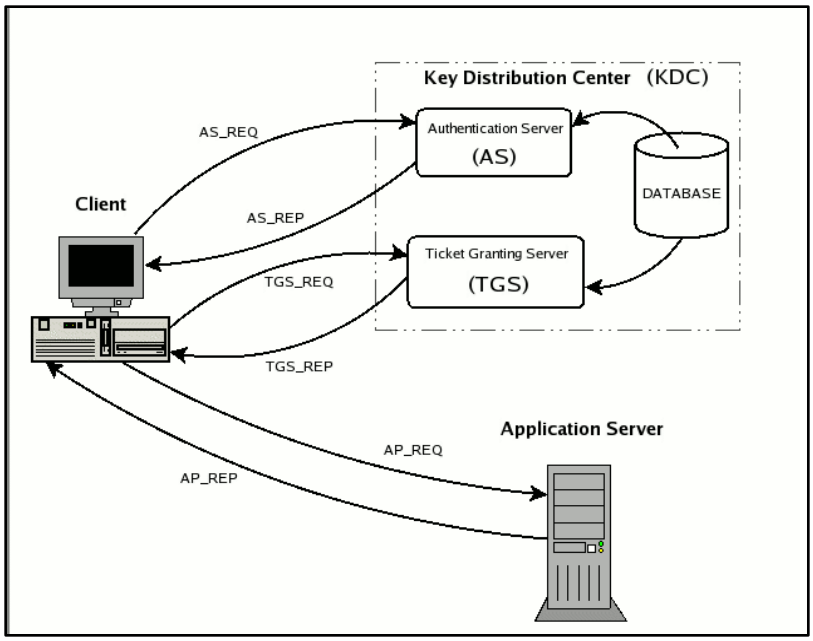
- It provides mutual authentication - both the user and the server verify each other's identity.
- Kerberos protocol messages are protected against eavesdropping and replay attacks.
- Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public key cryptography by utilizing asymmetric key cryptography during certain phases of authentication.

- It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise.

Working:

- In a Kerberos system, there is a designated site on the network, called the Kerberos server, which performs centralized key management and administrative functions. The server maintains a database containing the secret keys of all users, generates session keys whenever two users wish to communicate securely, and authenticates the identity of a user who requests certain network services.
- The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure

The process is as follows



The Kerberos authentication process

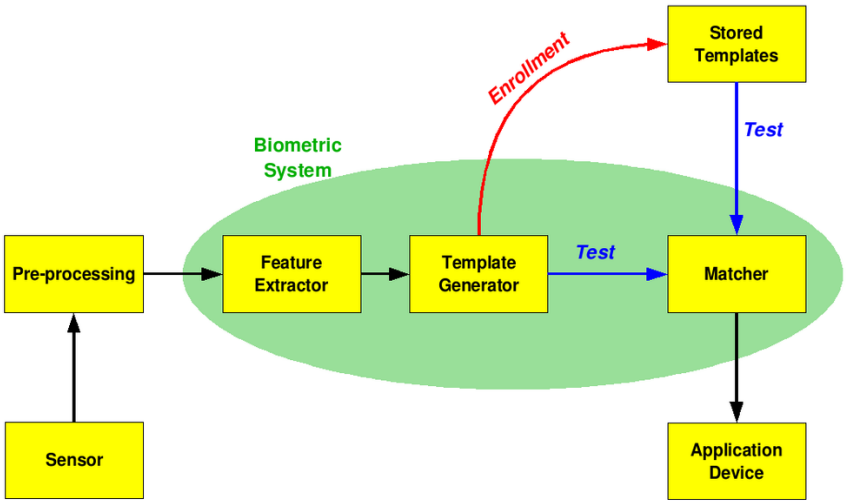
The same key is used at both ends of each exchange:

- AS_REQ is the initial user authentication request (i.e. made with kinit) This message is directed to the KDC component known as Authentication Server (AS);

- AS_REP is the reply of the Authentication Server to the previous request. Basically it contains the TGT (encrypted using the TGS secret key) and the session key (encrypted using the secret key of the requesting user);
- TGS_REQ is the request from the client to the Ticket Granting Server (TGS) for a service ticket. This packet includes the TGT obtained from the previous message and an authenticator generated by the client and encrypted with the session key;
- TGS_REP is the reply of the Ticket Granting Server to the previous request. Located inside is the requested service ticket (encrypted with the secret key of the service) and a service session key generated by TGS and encrypted using the previous session key generated by the AS;
- AP_REQ is the request that the client sends to an application server to access a service. The components are the service ticket obtained from TGS with the previous reply and an authenticator again generated by the client, but this time encrypted using the service session key (generated by TGS);
- AP_REP is the reply that the application server gives to the client to prove it really is the server the client is expecting. This packet is not always requested. The client requests the server for it only when mutual authentication is necessary.

(iii) Biometrics

Biometrics refers to metrics related to human characteristics and traits. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control.



- 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 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.
- 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.

- 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.

Types of Biometrics

- **Eyes - Iris Recognition**

  Visual Biometric the use of the features found in the iris to identify an individual.

- **Eyes - Retina Recognition**

  Visual Biometric The use of patterns of veins in the back of the eye to accomplish recognition.

- **Face Recognition**

  Visual Biometric The analysis of facial features or patterns for the authentication or recognition of an individual's identity. Most face recognition systems either use Eigen faces or local feature analysis.

- **Fingerprint Recognition**

  Visual Biometric The use of the ridges and valleys (minutiae) found on the surface tips of a human finger to identify an individual.

- **Hand Geometry Recognition**

  Visual/Spatial Biometric The use of the geometric features of the hand such as the lengths of fingers and the width of the hand to identify an individual.

- **Signature Recognition**

  Visual/Behavioral Biometric The authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication, Static and Dynamic. Static is most often a visual comparison between one scanned signature and another scanned signature, or a scanned signature against an ink signature. Technology is available to check two scanned signatures using advances

algorithms. Dynamic is becoming more popular as ceremony data is captured along with the X,Y,T and P Coordinates of the signor from the signing device. This data can be utilized in a court of law using digital forensic examination tools, and to create a biometric template from which dynamic signatures can be authenticated either at time of signing or post signing, and as triggers in workflow processes.

- **Typing Recognition**
  - Behavioral Biometric The use of the unique characteristics of a person's typing for establishing identity.
- **Vein Recognition**

  Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger or palm.
- **Voice / Speaker Recognition**

  There are two major applications of speaker recognition:
- **Voice - Speaker Verification / Authentication**

  Auditory Biometric The use of the voice as a method of determining the identity of a speaker for access control.

  If the speaker claims to be of a certain identity and the voice is used to verify this claim. Speaker verification is a 1:1 match where one speaker's voice is matched to one template (also called a "voice print" or "voice model"). Speaker verification is usually employed as a "gatekeeper" in order to provide access to a secure system (e.g.: telephone banking).
- **Voice - Speaker Identification**

  Auditory Biometric Identification is the task of determining an unknown speaker's identity. Speaker identification is a 1: N (many) match where the voice is compared against N templates. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc.

c) List different compliance standards used in information security. Explain any two standards in detail.

(List -2 Marks, Each component -3 Marks)

Ans:

1. Implementing and Information security Management System
2. ISO 27001
3. ISO 20000
4. BS 25999
5. PCI DSS
6. ITIL Framework
7. COBIT Framework

1. Implementing and Information security Management System

When the part of the management system dealing with information security it is referred to as the information security management system (ISMS).

An information security management system (ISMS) is a set of policies and procedures which specifies the instruments and methods that the management should use to clearly manage (plan, adopt, implement, supervise and improve) the tasks and activities aimed at achieving information security.

The main objective of ISMS is to provide systematic approach for managing an organization's sensitive information in order to protect it.

ISMS involves the following essential components

- Personal
- Processes
- Information

The goal of ISMS is to minimize risk and make sure business continuity by pro-actively limiting the impact of a security breach.

It addresses employee behavior and processes as well as information and technology. It can be targeted towards a particular type of data, such as customer data or it can be implemented in a comprehensive way that becomes part of the company's culture.

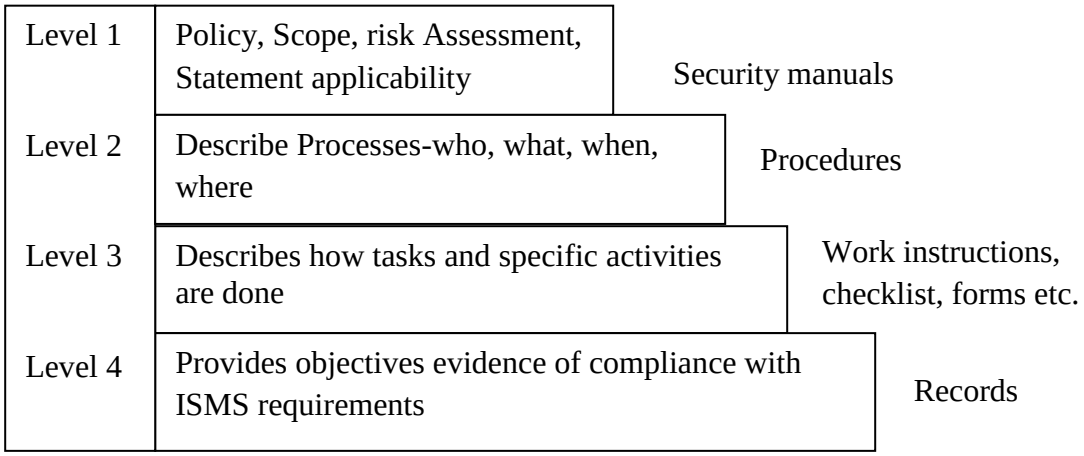


Fig. Four levels of documentation in ISMS

Above figure shows some basic measures that can be applied to achieve security of information system and threats to security should be controlled and managed by using broad security policy with the help of management.

Organizations should identify the nature of possible threats to information system hence controls are used to ensure security of Information System. In organization, it is also necessary to ensure privacy, confidentiality of data stored in system; hence it is necessary to continually evaluate the controls by auditing process.

2. ISO 27001

The international organization for standard (ISO) is established in year 1997. It is nongovernmental international body that collaborates with the International Electro technical commission (IEC) and the International Telecommunication Union (ITU) on information and communication technology (ICT) standards.

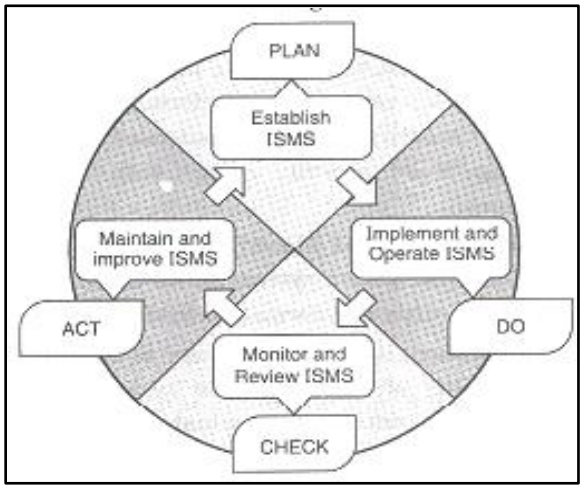
ISO 27001 describes following processes:

- Definition of Information Security Policy
- Definition of Scope of ISMS
- Security Risk Assessment
- Manage the identified risk
- Select controls for implementation

- Prepare SoA (Statement of Applicability)

ISO 27 001 uses PDCA (Plan-Do-Check-Act) approach and this is used to improve the effectiveness of an organization:

Plan : This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls



PDCA Model

- Do : This phase includes carrying out everything that was planned during the previous phase
- Check : The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check Whether the results meet the set objectives
- Act: The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

ISO 27001 allows selection of objectives and controls of security which shows the unique security risks and requirements. This information is used to prepare SoA and then SoA is used to prepare Risk Treatment Plan.

3. ISO 20000

- ISO 20000 is an industry standard like ISO 9000/9001, and like ISO 9000/9001, ISO 20000 offers organizational certification.
- ISO 20000 standards show IT how to manage improve IT while establishing audit criteria. It also provides auditors with a documented standard to use for measuring IT compliance.

- The ITIL offers certifications for individuals but ISO 20000 is an organizational certification with international recognition.
- ISO 20000 Was basically developed to use best practice guidance provided in ITIL framework. This standard was developed/ published in December 2005.
- ISO 20000 have two specifications

➢ ISO .20000-1. is the specification for Service Management. .It defines the processes and provides assessment criteria and recommendations for those who are responsible for IT Service Management. Organizational certification uses this section. It includes following sections :

- Scope
- Terms and Definitions
- Requirements for a Management System
- Planning and Implementing Service Management
- Planning and Implementing New or Changed Services
- The Service Delivery Process
- Relationship Processes
- Resolution Processes
- Release Process
- Control Processes

➢ ISO 20000-2 documents a "code of practice" that explains how to manage IT with regard to ISO 20000-1 audits. It includes all the sections from part 1 except requirements for a management system.

Both ISO 20000-1 and ISO 20000-2 derive directly from the ITIL best practice.

- Already, several governments have stated that ISO 20000 is a requirement for outsourced IT services. As the industry recognizes the value of ISO 20000, more and more companies will require their partners and vendors to reach ISO 20000 certification.
- ISO 20000 also includes more than Service Delivery and Service Support. It includes sections on managing suppliers and the business; as Well as Security Management.

- ISO 20000 can assist the organization in benchmarking its IT service management, improving its services, demonstrating an ability to meet customer requirements and create a framework for an independent assessment.
- Some of the most common benefits of ISO 20000 certification for service providers are as follows:

  (1) It offers competitive differentiation by demonstrating reliability and high quality of service.

  (2) It gives access to key markets, as many organizations in the public sector mandate that their IT service providers demonstrate compliance With ISO/IEC 20000.

4. BS 25999

- Business Continuity Management (BCM), the subject of British Standard BS 25999, is of real importance to organizations of all sizes, types, industry and location and to all staff members from Board directors, corporate executives and IT managers through to facilitate managers and business continuity professionals.
- Service disruptions, delays in responding to customer requests, the inability to process transactions in a timely manner, or being unable to resume business in the face of a disaster can all have significant impacts on an organization's effective operation.
- Natural disasters as well as terrorist activities have shown that an organization's resilience to disaster its ability to resume business quickly and efficiently were directly related to its preparedness to respond to unforeseen events.
- The BS 25999 standard is formed of two parts.
  - BS 25999-1 is a Code of Practice for Business Continuity Management (BCM), took the form of general guidance on the processes, principles and terminology recommended for BCM. It was published by the British Standards Institution in December 2006.
  - BS 25999-2 is a Specification for a Management Scheme, specified a set of requirements for implementing, operating and improving a BCM System (BCMS). It was published in November 2007.
- Because of Part 2, organization can have their business continuity management arrangements independently certified by external auditors, thereby providing stakeholders, customers with a real degree of comfort.

- Both parts of the standard contributed significantly to the international standards that succeeded then and to the development of other national and international standards.
- Following are the benefits of implementation of a BCM in the organization
- Increased flexibility when faced with organizational threat
  - Improved competence to maintain critical business services through action plan rehearsal
  - Enhanced capability to handle disruption and protect brand reputation when integrated with business planning.

For consumers it provides:

- Confidence and trust in the organization's brand because organization is using a consistent, standardized and robust method to assess, monitor and reduce the business risks
- BS 25999 can be used by any organization that wants to ensure they are prepared to reduce and recover quickly from potential risks which may affect their business.

5. PCI DSS

- The Payment Card Industry Data Security Standard (PCI DSS) is administered by the PCI Security Standards Council.
- The purpose of the Standard is to decrease payment card fraud across the internet and increase credit card data security.
- Organizations that store transmit or process card holder data must comply with PCI DSS. Compliance is regulated and enforced by the 'acquiring bank with which every organization must have a merchant account.
- The PCI DSS applies to any organization that processes, transmits or stores cardholder data.
  - For Merchant: The PCI DSS applies to Merchant. Even if merchant have subcontracted all PCI DSS activities to a third party, merchant have the responsibility for ensuring all the contracted parties are compliant with the standard.
  - For Service Provider : Including a software developer, the PCI DSS applies to service provider if he process, transmit or store cardholder data, or his activities affect the security of the cardholder data as it is being processed, transmitted or stored.
- IT Governance can advise on the applicability of the PCI DSS to the organization.

- The PCI DSS can apply across the whole of organization, or to a subset of the organization that transmits or stores the cardholder data away from the rest of the organization.
- It can apply to all people, processes and technologies that are involved in the processing, transmission or storage of cardholder data.
- It is not just the electronic systems but includes all systems including paper records such as receipts, mail order forms etc., and recordings of phone conversations if they capture cardholder data being read out to call centre operators.
- The Standard basically requires all applicable merchants and member service providers (MSPs) who are involved with the storage, processing or transmitting of cardholder data to -

  (1) Build the secure network using firewall etc and maintain it

  (2) Protect the stored data of cardholder and transmission encryption to and from the data center across public networks

  (3) Maintain a program for management of vulnerability using anti-virus software and using patches to secure system or application.

  (4) Implement strong access control by restricting the data access of cardholder, by using unique IDs and by Physical access restrictions to the data center and the managed servers.

  (5) Monitoring and testing networks on regular basis by logging and monitoring access to network resources / cardholder data and regular testing of security systems and processes.

6. ITIL Framework:

- In the early 1980s, the evolution of computing technology moved from mainframe-centric infrastructure and centralized IT organizations to distributed computing and geographically dispersed resources.
- While the ability to distribute technology provides more flexibility to the organizations, the side-effect was inconsistent application of processes for technology delivery and support.
- The UK government recognized that utilizing consistent practices for all aspects of an IT service lifecycle could assist in driving organizational effectiveness and efficiency, as Well as achieving predictable service levels.
- It was this recognition that gave rise to ITIL, which has become a successful mechanism to drive consistency, efficiency and excellence into the business of managing IT services.
- ITIL is an approach to IT Service Management

- A service is something that provides value to customers. Services that customers can directly utilize or consume are known as Business services.
- Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services.

Example - Payroll is an IT service that is used to consolidate information, calculate compensation and generate pay cheque on a regular basis.

- In order for Payroll to run, it is supported by a number of technology or infrastructure' services. An infrastructure service does its Work in the background, so that the business does not directly interact with it, but nevertheless this service is necessary as part of the overall value chain to the business service. 'Server administration', 'database administration' and 'storage administration' are all examples of infrastructure services required for the successful delivery of the Payroll business service.
- ITIL can be adapted and used in conjunction with other good practices such as
  - COBIT (a framework for IT Governance and Controls)
  - Six Sigma (a quality methodology)
  - TOGAF (a framework for IT architecture)
  - ISO 27000 (a standard for IT security)
  - ISO/IEC 20000 (a standard for IT service management)
- IT organizations have traditionally focused on managing the infrastructure services and technology silos. ITIL suggests _a more holistic approach to managing services from end to end.
- Managing the entire business service along with its underlying components in a cohesive manner ensures that every aspect of a service is considered so that the required functionality and service levels are delivered to the business customer.

Following are the benefits to organization with ITIL framework:

- improve resource utilization
- be more competitive
- reduce re-work
- eliminate redundant work
- improve availability, reliability and security of business critical IT services
- improve project deliverables and time-scales

- justify the cost of service quality
- provide services that meet or exceed business demands

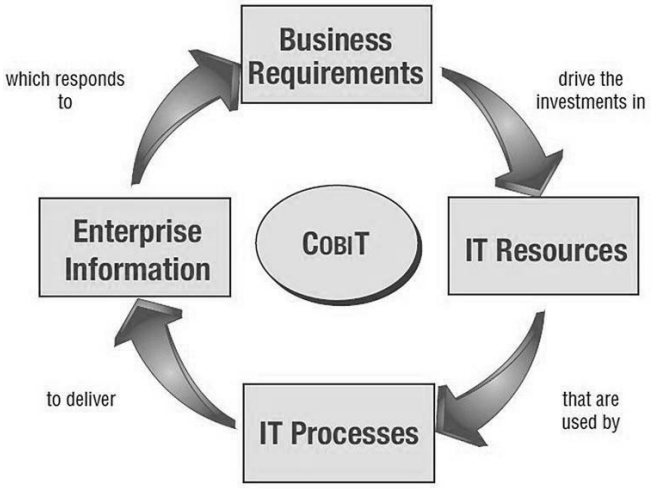
ITIL framework can be adopted by many types of companies like:

- Large technological companies
- Retailers
- Financial Services Organizations
- Entertainment
- Manufacturing
- Life Sciences companies etc.

7. COBIT Framework

- The Control Objectives for Information and related Technology COBIT) is "a control framework that links IT initiatives to business requirements, organizes IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered".
- COBIT is a framework developed by ISACA (Information System Audit and Control Association) in year 1996 for IT management and IT overnance.
- COBIT is a set of guidance materials for IT governance that allows managers to bridge the gap between control requirements, technical issues and business risks.
- The main aim of COBIT is to research, develop, publicize and promote an authoritative, up to date, international set of generally accepted information technology control objectives for day to day use by business managers, IT professionals and assurance.
- In COBIT, a control is the policy, procedure, practices and organizational structures, which are designed to achieve reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.
- Control objective is a statement of desired result or purpose to be achieved by implementing control procedures in a particular activity.

The COBIT framework is based on the following principle: To provide the information that the organization requires to achieve its objectives, the organization requires investing in and managing and controlling IT resources using a structured set of processes to provide the services which deliver the required enterprise information.



COBIT Framework

Managing and controlling information are at the heart of the COBIT framework and help to ensure alignment to business requirements.

Following are certain criteria that COBIT refers to as business requirements for information:

(1) Effectiveness: It means that the information is relevant, timely, correct, consistent and applicable to the business process.

(2) Efficiency: It means that-» the information is optimal for productive as Well as economical – use of resources.

(3) Confidentiality: It means that the information is protected from unauthorized use.

(4) Integrity: It means that the information is accurate and complete and valid for business.

(5) Availability: It means that the information will be available whenever required by the business process.

(6) Compliance: It means the information has fulfilled all laws, regulations and contractual arrangements, externally imposed business criteria as well as internal policies.

(7) Reliability: It means that the information is appropriate for management to operate the entity and apply governance responsibilities.

- COBIT defines IT activities in a generic process model within four domains. These domains are 'Plan and 0rganize', 'Acquire and Implement', 'Deliver and Support', and 'Monitor and Evaluate'.
- The COBIT framework provides a reference process model and common language for everyone in an enterprise to view and manage IT activities.
- The most necessary and early step towards good governance is use of an operational model and a common language for all different parts of the business in IT.
- COBIT will provide a structure to measure and monitor the performance of IT, communication with service providers and incorporation of best management practices.
- A process model encourages process ownership, enabling responsibilities and accountability to be defined.

6. Attempt any FOUR of the following: Marks 16

a) List different types cybercrimes. Explain any two in detail.
(List -2 Marks, for explanation-2 Marks)

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 spans not only state but national boundaries as well. Cybercrime was broken into two categories and defined as

Cybercrime in a narrow sense (Computer Crime) : any illegal behavior directed by means of electronic operations that target the security of computer stems and the data processed by them.

Cybercrime in a broader sense (Computer related crime) : 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.

1. Hacking
2. Cracking
3. Viruses, Virus Attacks
4. Pornography
5. Intellectual Property

6. Legal System of Information Technology

l. Hacking

Every act committed towards breaking into a computer and/or network is hacking and it is an offence. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get enjoyment out of such destruction. Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

Government websites are hot on hacker's target lists and attacks on government websites receive wide press coverage.

2. Cracking

A cracker is someone who breaks into someone else's computer system, often on a network; bypasses 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.

3. Viruses, Virus Attacks

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.

4. 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.

5. Software Piracy

Cybercrime Investigation Cell of India defines "software piracy" as theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. Software piracy can be defined as "copying and using commercial software purchased by someone else". Software piracy is illegal. Each pirated piece of software takes away from company profits, reducing funds for further software development initiatives. Making duplication of software is an act of copyright infringement, and it's illegal. Providing unauthorized access to software or to serial numbers used to register software can also be illegal ways to Deal With/Minimize Software Piracy : "

- Have a central location for software programs. Know which applications are being added, modified or deleted.
- Secure master copies of software and associate documentation, while providing faculty access to those programs when needed.
- Never lend or give commercial software to unlicensed users.
- Permit only authorized users to install software.
- Train and make staff aware of software use and security procedures which reduce likelihood of software piracy.

6. Intellectual Property

Intellectual property (IP) rights are the legally recognized exclusive rights to creations of the mind. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs.

Intellectual Property Rights (IPR), are rights granted to creators and owner of works that are results of human intellectual creativity. These works can be in the industrial, scientific, literary and artistic domains, which can be in form of an invention, a manuscript, a suite of software or a business name.

The agreement provides norms and standards for protection and enforcement of IPRS in member countries, in respect to following areas patents, copyrights, trademarks, industrial designs, layout designs of integrated circuits etc. IPR is an important consideration in issues concerning licensed software.

7. Legal System of Information Technology

Computer technology has revolutionized the world. It has removed restrictions of geographical proximity in communication and business. However, with every great invention, also come its follies. That is the reason why Security plays a big part in today's world of computers, e-commerce and the Internet.

With this development of security for computers, came the need for a legal system to prosecute perpetrators. Also, with the recent boom in E-commerce, it has become pertinent to have legal systems and laws in place, to protect and uphold contracts, business transactions, data processing and development over the Internet. Legal system plays a vital part in the upholding a secure information technology infrastructure. .

Jurisdiction is a major stumbling block for the legal system when it comes to dealing with computers, networks and their security, across the globe.

It is important that security administrators understand the support they have from the legal system in order to adequately protect their computer systems. At the same time, it is important that companies develop healthy computer ethics to minimize intrusions from within. It is a well-

known fact that most instances of computer crime occur from the inside, and thus creating a culture of ethical computer behavior is vital deterrent to underhand computer related activities.

8. 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.

9. 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.

10. Cyber Crime Investigation

Computer crimes will always involve some type of computer-security breach. Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; using the property or services of another without authorization; or committing theft commits computer crime.

Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

Computer Forensics is as important element in Cyber Crime Investigation which deals in examination of digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

b) Explain remote user access and authentication with example.

(Explanation-2 Marks, For example - 2 Marks)

Ans: When a person is working at remote location, there is a problem of security because the user is using insecure network i.e. internet.

User uses internet to access the LAN of corporate office. Hence the additional security like access control mechanisms is requires protecting user as well as LAN of corporate office.

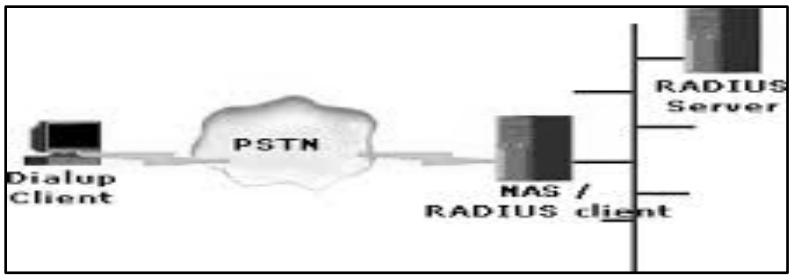
Example:

Remote Access Dial-In Service (RADIUS):

RADIUS is a protocol which provides authentication, authorization, and accounting (AAA protocol) management for users and network services. It configures the information between a Network Access Server (NAS) which desires to authenticate its links and a shared Authentication Server.

- Works in both situations (a) Local (b) Mobile.
- Uses PAP, CHAP or EAP protocols to authenticate users.
- Look in text file, LDAP Servers, Database for authentication.
- After authentication services parameters passed back to NAS.
- Be notified when the session starts and stop. This data will be used for Billing or Statistics purposes.
- SNMP is used for remote monitoring
- It can be used as a proxy.

It allows company to maintain profile of users in central database so that remote server can share it. With the help of RADIUS, company can set up a policy which can be applied at a single administered network point.



RADIUS

Operation of RADIUS:

Before Client starts communicating with RADIUS Server, it is required that shared secret must be shared between Client and Server and Client must be configured to use RADIUS server to get service.

Once Client is configured properly then,

Client starts with Access-Request: it includes access credentials like username and password.

Server sends either Access-Accept, Access-Reject or Access-Challenge: The RADIUS server checks the information send by client using authentication schemes (PAP, CHAP or EAP). The user's proof of identification is verified along with, optional other information like the user's network address or phone number, account status, and specific network service access privileges etc. The RADIUS server then returns one of the above three responses.

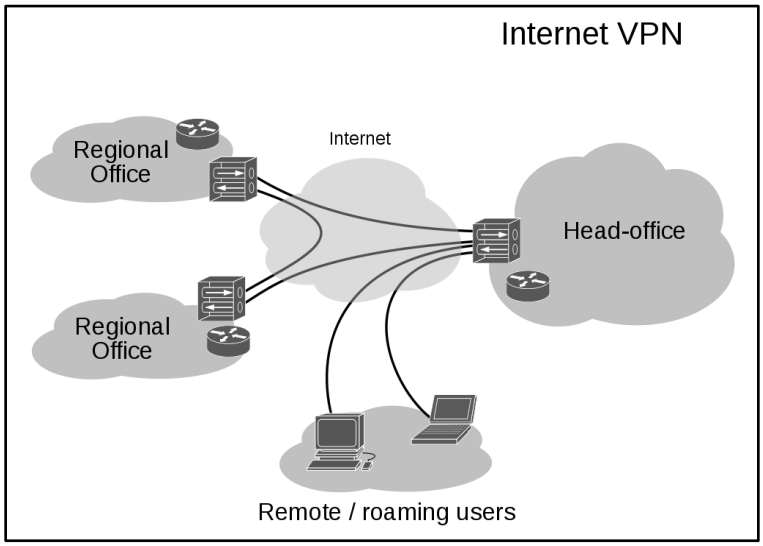
Example 2: Virtual Private Network

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or Wi-Fi-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions.

A VPN connection across the Internet is similar to a wide area network (WAN) link between websites. From a user perspective, the extended network resources are accessed in the same way as resources available within the private network.

VPNs allow employees to securely access their company's intranet while traveling outside the office. Similarly, VPNs securely connect geographically separated offices of an organization, creating one cohesive network. VPN technology is also used by individual Internet users to secure their wireless transactions, to circumvent geo restrictions and censorship, and to connect to proxy servers for the purpose of protecting personal identity and location.



c) Describe BIBA model of security.

(For Explanation- 4 Marks)

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 can not 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 can not 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.

(For Explanation- 4 Marks)

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 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 code 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 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,

1) Dominance Relation :-

User with particular clearance level will only be able to access file of particular classification and below.

2) Discretionary Security:-

Specific subject (users) are granted specific mode of access.

e) Describe Symmetric and Asymmetric Cipher: Give example.

(Symmetric Cipher - 1 Mark, Asymmetric Cipher - 1 Mark, Example - 1 Mark each)

Ans: Symmetric cipher:

Symmetric ciphers are the oldest and most used **cryptographic ciphers**. In a symmetric cipher, the key that deciphers the cipher text is the same as (or can be easily derived from) the key enciphers the clear text. This key is often referred to as the secret key.

Example:

The most widely used symmetric ciphers are DES and AES.

Asymmetric cipher:

An asymmetric cipher uses two keys: one key that is kept secret and known to only one person (the private key) and another key that is public and available to everyone (the public key). The two keys are mathematically interrelated, but it's impossible to derive one key from the other.

Example:

Well-known asymmetric ciphers are the Diffie-Hellman algorithm, RSA, and DSA.