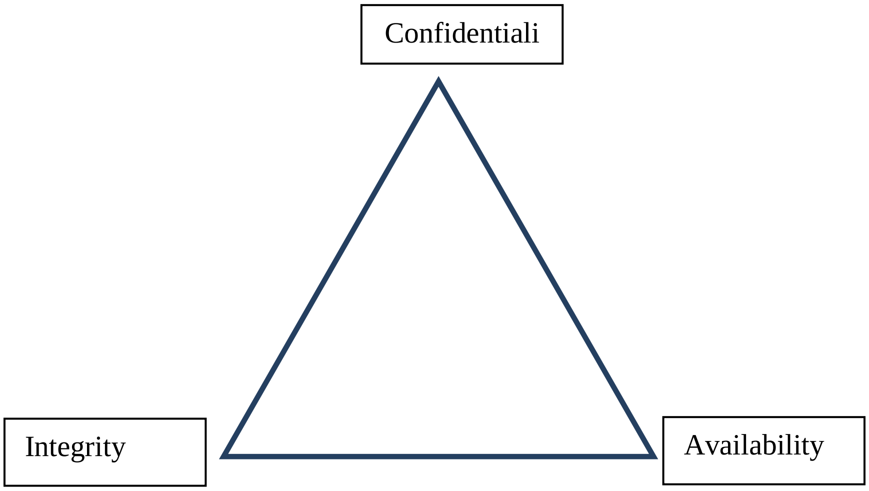
Important Instructions to examiners:

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 tryto assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more importance (Not applicable for subject English and Communication Skills.
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

Q. 1

A. Attempt any three:

a) State pillar of information security. Describe with neat diagram.
(Diagram 1M, each point 1M)



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

Confidentiality:

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

Integrity:

The concept of integrity ensures that

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

Availability:

The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate person. Availability guarantees that the systems are up and running when they are needed.

b) With respect to information security define following term:

1) **Trust computing base**
2) **Standard**
3) **Security policy**

1) Trust Computing Base
2) Standard
3) Security Policy

1. Trusted Computing Base (TCB): (2M)

Trusted Computing Base is a complete protection mechanism in any computer system and it is responsible for enforcing system-wide information security policies.

It is a combination of hardware, software and firmware that work together to implement a combined security policy for system or a product. It reduces the likelihood of threats within the TCB and improves the overall security of a computer system.

Software model / abstract machine is a reference monitor that passes all access from any subject (user) to any object (data / file) but it cannot be avoided. It gives access to object by subjects. The reference monitor has three properties:

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

It stands between each subject and object and its role is to verify the subject, meets the minimum requirements for access to an object, as shown in Fig.

In Unix / Linux operating system, a security kernel acts as a reference monitor. The security kernel handles all user/application requests for access to system resources.

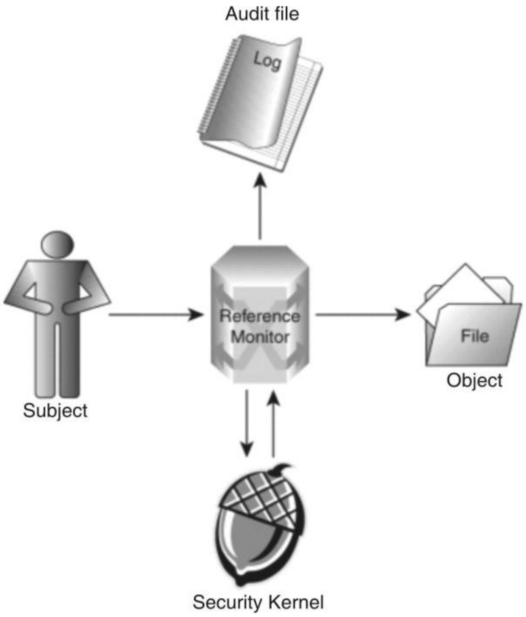


Fig: Reference Monitor

2) **Standard: (1M)**

Standard consists of specific low level mandatory controls that help enforce and support the information security policy.

Standard helps to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or software. For example, a password standard may set out rules for password complexity and a Windows standard may set out the rules for hardening Windows clients.

3) **Security policy: (1M)**

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

The policy outlines security roles and responsibilities, defines the scope of information to be protected, and provides a high level description of the controls that must be in place to protect information.

c) **Define following with diagram:**

1) **Encryption**
2) **Decryption**
3) **Cipher text**

1) **Encryption:** **1M**

The process of encoding plain text into cipher text message is known as Encryption.

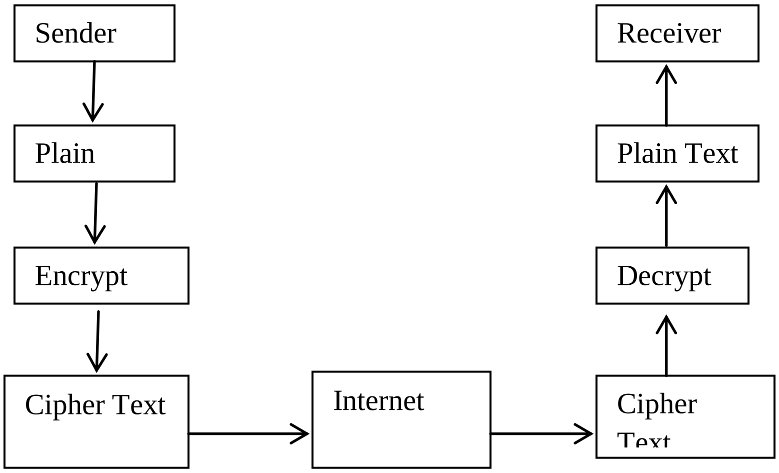
2) Decryption: 1M

The process of transforming cipher text message into plain text or original text is known as Decryption.

3) Cipher Text: 1M

The resultant message after coding a plain text by using some suitable method is known as Cipher Text.

Encryption and Decryption 1M



d) Stating mean of term 'cyber crime". List different type of cyber crime and explain any two.

(Definition-1M, List 1 Mark, for explanation-2 Marks (any 2))

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.

For example, unauthorized access, damage to computer data or programs, computer sabotages unauthorized interception of communications, computer espionage.

Different types of cyber crimes are:

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

1. Hacking

Every act committed towards breaking into a computer and/or network is hacking and it is an offence. Hackers write or use readymade computer programs to attack the target computer. They possess the desire to destruct and they get enjoyment out of such destruction. 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 by passing passwords or licenses in computer programs or in other ways intentionally breaches computer security. A cracker can be doing this for Profit maliciously, for some altruistic purpose or cause, or because the challenge is there. The term ―cracker" is not to be confused with “hacker”. Hackers generally deplore cracking.

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, ecommerce 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 Ecommerce, 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**

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

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.

B. Attempt any ONE:

a) Give classification of information. Describe different criteria for information classification.

(Classification- 3M (any 3), Criteria-3M(any 3))

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

Terms for information classification:

1. **Unclassified**
   Information that is neither sensitive nor classified. The public release of this information does not violet confidentiality.
2. **Sensitive but Unclassified (SBU)**
   Information that has been designated as a minor secret but may not create serious damage if disclosed.
3. **Confidential**
   The unauthorized disclosure of confidential information could cause some damage to the country's national security.
4. **Secret**
   The unauthorized disclosure of this information could cause serious damage to the countries national security.
5. **Top secret**
   This is the highest level of information classification. Any unauthorized disclosure of top secret information will cause grave damage to the country's national security.

Criteria for information Classification:

1. **Value**
   It is the most commonly used criteria for classifying data in private sector.
   If the information is valuable to an organization it needs to be classified.
2. **Age**
   The classification of the information may be lowered if the information value decreases over the time.
3. **Useful Life**
   If the information has been made available to new information, important changes to the information can be often considered.

4. **Personal association**
   If the information is personally associated with specific individual or is addressed by a privacy law then it may need to be classified.

b) Define risk. Describe how risk is managed for information security.

(Definition of Risk-2M, Risk Management-4M)

Risk is the potential of losing something of value. Risk can also be defined as the intentional interaction with uncertainty.

Risk Management

Risk management refers to the practice of identifying vulnerabilities of an organization's information systems and identifying potential risks in advance, analyze them and taking precautionary steps to reduce risk and to ensure confidentiality, integrity and availability of components in information system.

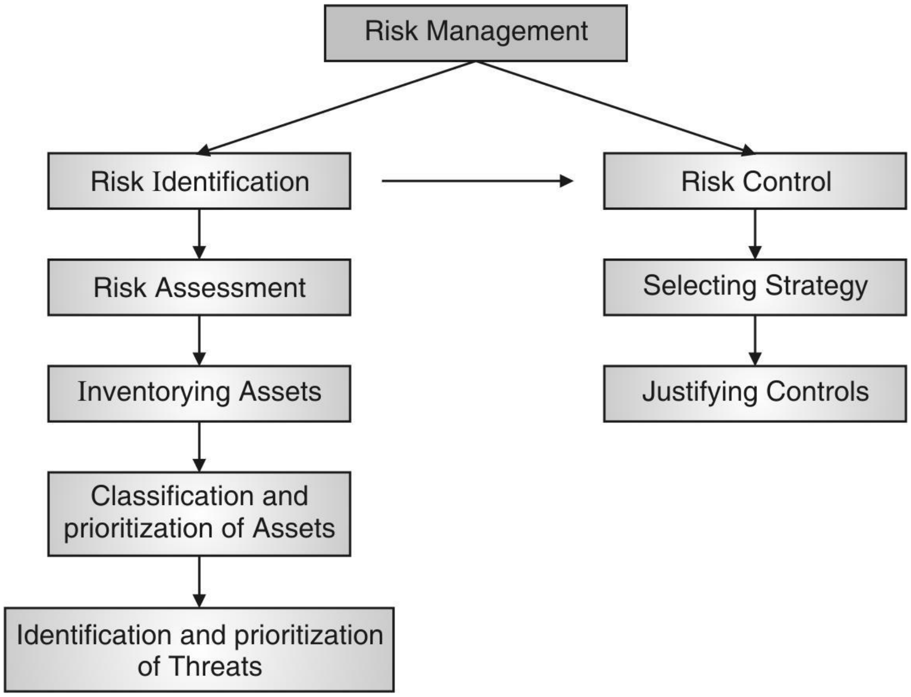


Fig: Components of Risk Management

Risk Identification:

It is the process of identification and documentation of security procedure and risk of an organization's information system.

For IT professionals it is necessary to identify the information assets of an organization - people, procedure, data and information, software, hardware, networking components etc. then classify and prioritize them.

Risk Control:

It is the processes of selecting and applying controls to decrease the risk of an organization's information system. There are following four strategies that can be used to control the risk

1. Avoidance

2. Transference
3. Mitigation
4. Acceptance

Quantitative Risk Analysis:
A process for assigning a numeric value to the probability of loss based on known risks, on financial values of the assets and on probability of threats.
It is used to determine potential direct and indirect costs to the company based on values assigned to company assets and their exposure to risk. E.g. the cost of replacing an asset, the cost of lost productivity, or the cost of diminished brand reputation.

Qualitative Risk Analysis:
It is a collaborative process of assigning relative values to assets, assessing their risk exposure, and estimating the cost of controlling the risk. It differs from quantitative risk analysis in that it utilizes relative measures and approximate costs rather than precise valuation and cost determination. In qualitative risk analysis:

1. Assets can be rated based on criticality - very important, important, not-important etc.
2. Vulnerabilities can be rated based on how it is fixed - fixed soon, should be fixed, fix if suitable etc
3. Threats can be rated based on scale of likely - likely, unlikely, very likely etc.

Q. 2 Attempt any two:

a) Define security. Describe different type of securities in organization.

(Definition 2M, types 4M, any suitable answer can be consider)
Security: It is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical)

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.

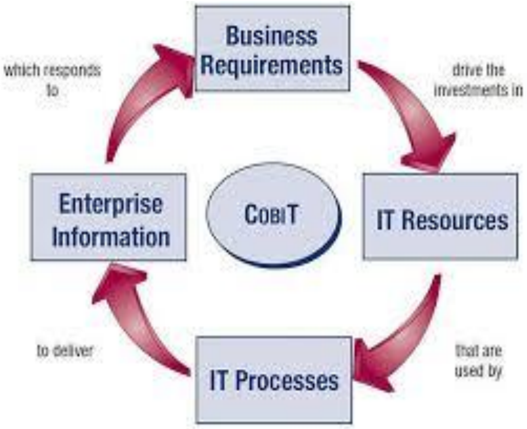
CARD INDUSTRY DATA SECURITY STANDARD

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

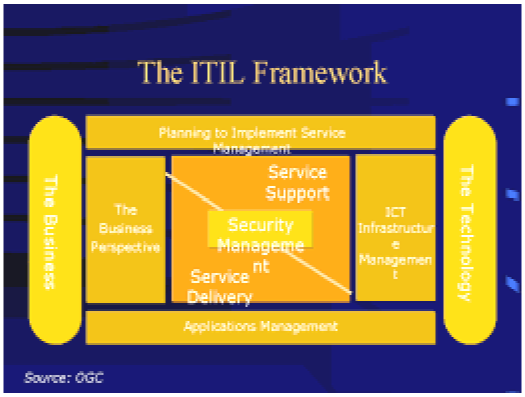
The Control Objectives for Information and related Technology (COBIT) is ―a control framework that links IT initiatives to business requirements, organizes IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives 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.



b) Consider plain text “Team’ and key as “HILL”. Convert given plain text into cipher text using Hill cipher. Write step by step procedure.

(Procedure-3M, Correct Answer-3M)

1. In the above example

   PlainText- “Team”

   Keyword- “Hill”

   Matrix- 2*2

2. Turn the keyword into matrix.

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}$$

3. To convert keyword into key matrix, convert each letter into a number by its position in the alphabet like A=0, B=1, C=2 etc.

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

4. Now split the plain text and write these as column vectors.

$$\begin{pmatrix} T \\ E \end{pmatrix} \begin{pmatrix} A \\ M \end{pmatrix}$$

5. Next step is to convert the plain text column vectors in the same way that

   We converted the keyword into the key matrix. Each letter is replaced by appropriate number.

$$\begin{pmatrix} 19 \\ 4 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

6. Now to perform matrix multiplication write key matrix with first column vector

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix}$$

Matrix multiplication will be (7 * 19) + (8 * 4) = 165
(11 * 19) + (11 * 4) = 253

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 165 \\ 253 \end{pmatrix}$$

7. Next take modulo 26 of each of the resultant column vector.

$$\begin{pmatrix} 165 \\ 253 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 9 \\ 19 \end{pmatrix}$$

Now convert keys 9 and 19 into letters ie J and T respectively.

$$\begin{pmatrix} 9 \\ 19 \end{pmatrix} = \begin{pmatrix} J \\ T \end{pmatrix}$$

8. Same procedure is followed for remaining plain text

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

Matrix multiplication will be (7 * 0) + (8 * 12) = 96
(11 * 0) + (11 * 12) = 132

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix} = \begin{pmatrix} 96 \\ 132 \end{pmatrix}$$

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

$$\begin{pmatrix} 96 \\ 132 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 18 \\ 2 \end{pmatrix}$$

Now convert keys 18 and 2 into letters ie S and C respectively.

$$\begin{pmatrix} 18 \\ 2 \end{pmatrix} = \begin{pmatrix} S \\ C \end{pmatrix}$$

9. Hence for plain text “Team” and keyword “Hill” the cipher text is “JTSC”.

c) Describe IT Act, 2008.

(Suitable Explanation: 6M)

- It is the information Technology Amendment Act, 2008 also known as ITA-2008
- It is a considerable addition to the ITA-2000 and is administered by the Indian Computer Emergency Response Team (CERT-In) in year 2008.
- Basically, the act was developed for IT industries, to control e-commerce, to provide e-governance facility and to stop cybercrime attacks.
- The alterations are made to address some issues like the original bill failed to cover, to accommodate the development of IT and security of e-commerce transactions.
- The modification includes
    - ➢ Redefinition of terms like communication device which reflect the current use.
    - ➢ Validation of electronic signatures and contracts.
    - ➢ The owner of an IP address is responsible for content that are accessed or distributed through it.
    - ➢ Organizations are responsible for implementation of effective data security practices.
- Following are the characteristics of IT ACT 2008
    - ➢ This Act provides legal recognition for the transaction i.e. Electronic Data Interchange (EDI) and other electronic communications. Electronic commerce is the alternative to paper based methods of communication to store information.
    - ➢ This Act also gives facilities for electronic filling of information with the Government agencies and further to change the Indian Penal Code-Indian Evidence Act 1872, Bankers code Evidence Act 1891 and Reserve Bank of India Act, 1934 and for matter connected therewith or incidental thereto.

- The General Assembly of the United Nations by resolution A/RES/51/162, dated 30 January 1997 has adopted the model law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.
- This recommends that all States give favorable consideration to the above said model law when they enact or revise their laws, in terms of need for uniformity of the law applicable to alternative to paper based methods of communication and storage of information.
- It is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

Q. 3 Attempt any four:

a) List confidentially and integrity models. Explain Bell-Lapadula model of confidentiality.

(List 2 Marks; Bell – LaPadula Model 2 Marks)

Confidentiality Models:-

- Bell LaPadula Model
- Biba Integrity Model
- The Clark-Wilson Integrity Model
- Discretionary Access Control - DAC
- Graham-Denning Model
- Multilevel security - MLS
- Security Modes of Operation
- Take-grant protection model

Bell – LaPadula: -

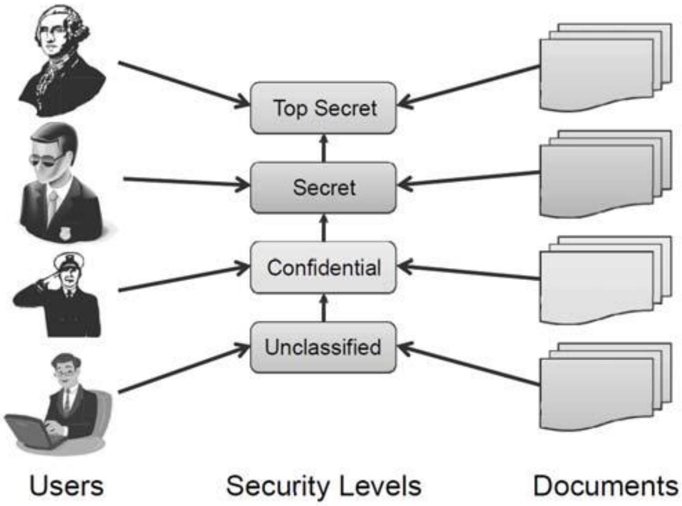
- The Bell-La Padula (BLP) model is a classic mandatory access-control model for protecting confidentiality.
- The BLP model is derived from the military multilevel security paradigm, which has been traditionally used in military organizations for document classification and personnel clearance.
- The BLP model has a strict, linear ordering on the security of levels of documents, so that each document has a specific security level in this ordering and each user is assigned a strict level of access that allows them to view all documents with the corresponding level of security or below.
- How Bell LaPadula Works?
- The security levels in BLP form a partial order, $\leq$
- Each object, x, is assigned to a security level, L(x). Similarly, each user, u, is assigned to a security level, L(u). Access to objects by users is controlled by the following two rules:
  - Simple security property. A user u can read an object x only if

$$L(x) < L(u)$$

  - A user u can write (create, edit, or append to) an object x only if

$$L(u) < L(x)$$

- The simple security property is also called the “no read up” rule, as it prevents users from viewing objects with security levels higher than their own.
- The property is also called the “no write down” rule. It is meant to prevent propagation of information to users with a lower security level.



b) Define term:

1) **Interruption**
2) **Interceptions**
3) **Fabrication**
4) **Modification**

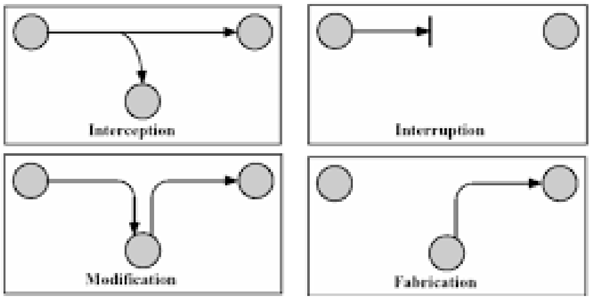
(Each term 1 Mark)

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

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

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

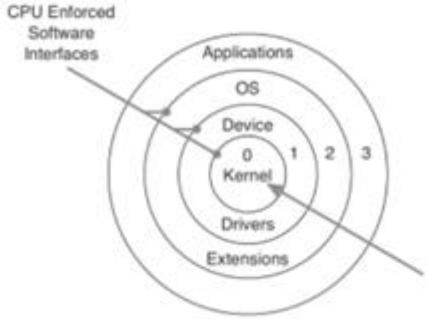
4) **Modification:** Modifications involve unauthorized changing of data or tampering with a service so that it no longer adheres to its original specifications. Examples of modifications include intercepting and subsequently changing transmitted data, tampering with database entries, and changing a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



c) **Describe ring of trust for single system and for networking.**

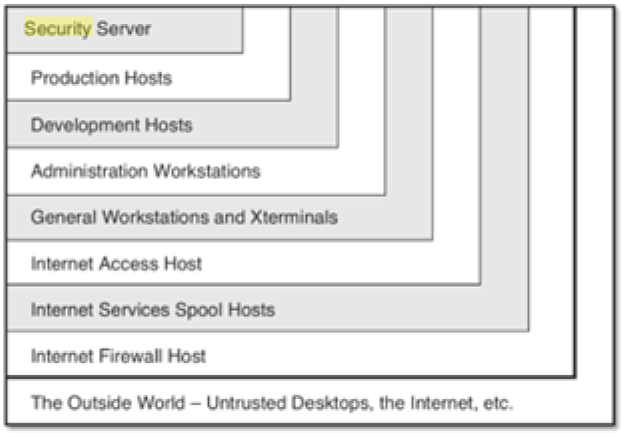
(Single System 2 Marks; Networking 2 Marks)

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



Rings of trust in stand-alone systems.

It's also possible to use the concepts of rings of trust to design security domains or operating environments for networks of systems. Fig below illustrates this concept.


Security Server
Production Hosts
Development Hosts
Administration Workstations
General Workstations and Xterminals
Internet Access Host
Internet Services Spool Hosts
Internet Firewall Host
The Outside World – Untrusted Desktops, the Internet, etc.

Rings of trust in networked environments.

This model divides the hosts into rings, based on the security rating of the services they provide to the network, and then uses these rings as the basis for trust between hosts.

To help determine the hierarchy of the rings, some questions must be answered:

- Is the host in a physically secure computer room?
- Does the host have normal (as opposed to privileged) user accounts?
- Is this host at a remote site and, hence, less trustworthy than the ones in the central computer room?
- Does this host operate software that relies on data obtained from the Internet?
- Does this host provide mission-critical services? How many people in the company would be affected by downtime on this host?

The following general rules apply to constructing rings of trust in network systems:

- Each host trusts hosts in a more inner ring than its own.
- No host trusts any host in a more outer ring than its own.
- Each host may trust hosts in the same ring as its own.
- Where a ring has been segmented into separate subnetworks, a host in one segment does not trust hosts in other segments.

As you can see, rings of trust apply equally well for stand-alone systems, small business or home networks, and large –scale corporate and government networks where security requirements are absolute.

To implement the rings of trust model, a number of software constructs and design objectives are used for security and resources protection.

d) Describe then term digital stenography with neat diagram.

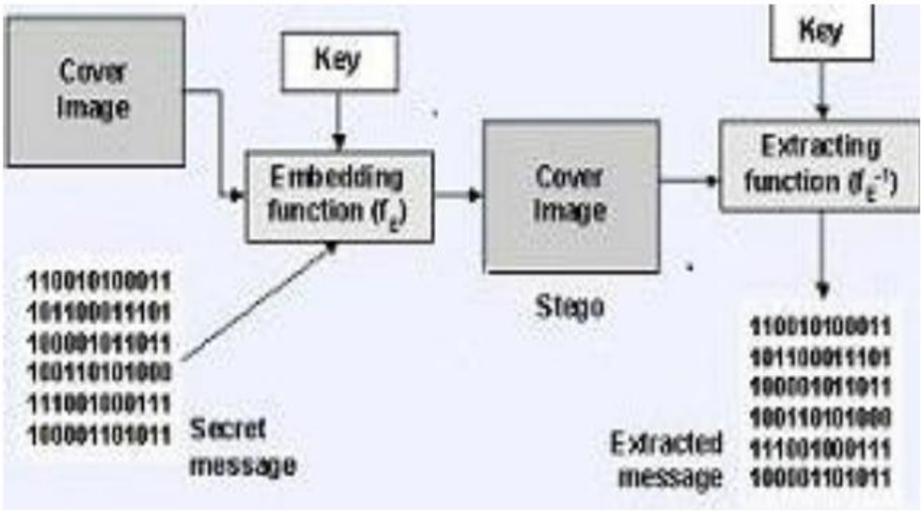
(Diagram 1 Mark; Explanation 3 Marks)

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

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

Special software is needed for Steganography, and there are freeware versions available at any good download site.

Steganography (literally meaning covered writing) dates back to ancient Greece, where common practices consisted of etching messages in wooden tablets and covering them with wax, and tattooing a shaved messenger's head, letting his hair grow back, then shaving it again when he arrived at his contact point.



e) **Describe then term hacker, cracker, mail bomb and software privacy.**

(1 Mark each term)

- **Hacker:** 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.

- **Cracker:** 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.

- **Mail Bomb:** 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.

- **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.

Q. 4

A. Attempt any three:

a) Describe any four type of protection mechanism in TCB.

(1 Mark for each type of protection)

The TCB is defined as the total combination of protection mechanisms within a computer system. The TCB includes hardware, software, and firmware. These are part of the TCB because the system is sure that these components will enforce the security policy and not violate it.

The components that do fall under the TCB need to be identified and their accepted capabilities defined. For example, a system that has a lower trust level rating may permit all authenticated users to access and modify all files on the computer. This subset of subjects and objects is large and the relationship between them is loose and relaxed. A system with a much higher trust level rating may permit only two subjects to access all files on a computer system, and only one of those subjects can actually modify all the files. This subset is much smaller and the rules being enforced are more stringent and detailed.

The TCB is the totality of protection mechanisms within a computer system that work together to enforce a security policy. The TCB contains the security kernel and all other security protection mechanisms.

The TCB is made up of all the protection mechanisms within a system (software, hardware, and firmware). All of these mechanisms need to work in an orchestrated way to enforce all the requirements of a security policy. When evaluated, these mechanisms are tested, their designs are inspected, and the supporting documentation is reviewed and evaluated. How the system is developed, maintained, and even delivered to the customer are all under review when the trust for a system is being gauged. All of these different evaluation components are put through an evaluation process to assign the correct level of trust and assurance. Customers then use this assignment, or rating, to determine which system best fits their security needs.

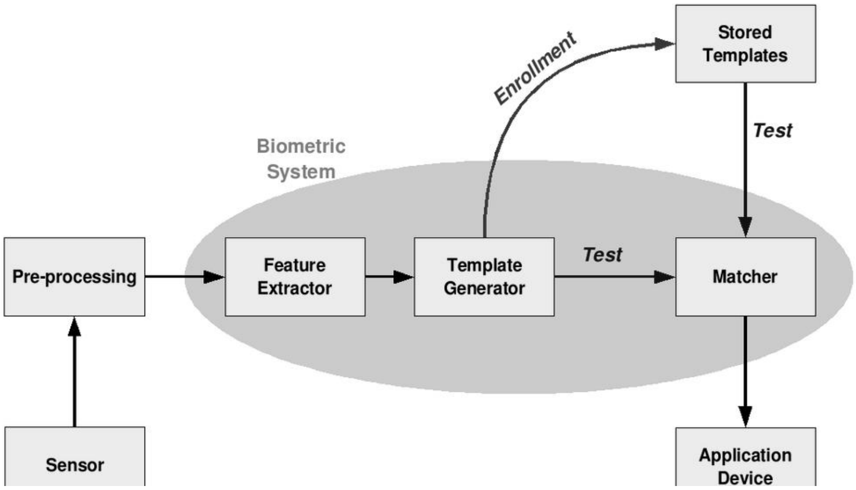
b) Define Access Control. Draw block diagram of biometric access control and explain.

(Access control 1 Mark; Block diagram 1 Mark; Explanation 2 Marks)

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

Biometrics Access Control:

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.

c) Describe then term TSEC.

(Description 4 Marks)

The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which is used to evaluate operating systems, applications, and different products. This evaluation criterion is published in a book with an orange cover, which is called appropriately the Orange Book. (We like to keep things simple in security!) Customers use the security rating that the criteria presents so they have a metric to use when comparing different systems. It also provides direction for manufactures so they know what specifications to build to, and provides a one-stop evaluation process so customers do not need to have individual components within the systems evaluated

TCSEC provides a graded classification of systems that is divided into hierarchical divisions of security levels:

A. Verified protection
B. Mandatory protection
C. Discretionary protection
D. Minimal security

The classification A represents the highest level of security and D represents the lowest level of security.

Each division can have one or more numbered classes and each has a corresponding set of requirements that must be met for a system to achieve that particular rating. The classes with higher numbers indicate a greater degree of trust and assurance. So B2would offer more trust than B1, and C2 would offer more trust than C1.

The criteria include four main topics: security policy, accountability, assurance, and documentation, but these actually break down into seven different areas:

- **Security policy** the policy must be explicit and well defined and enforced by the mechanisms within the system.
- **Identification** Individual subjects must be uniquely identified.
- **Labels** Access control labels must be associated properly with objects.
- **Documentation** this includes the test, design, specification documents, user guides, and manuals.
- **Accountability** Audit data must be captured and protected to enforce accountability.
- **Life cycle assurance** Software, hardware, and firmware must be able to be tested individually to ensure that each enforces the security policy in an effective manner throughout their lifetimes.
- **Continuous protection:** The security mechanisms and the system as a whole must perform predictably and acceptably in different situations continuously.

These categories are evaluated independently, but the rating that is assigned at the end does not specify these different objectives individually. The rating is a sum total of these items.

Each division and class incorporates the requirements of the ones below it. This means that C2 must meet its criteria requirements and all of C1 requirements, and B3has its requirements to fulfill along with those of C1, C2, B1, and B2. Each division or class ups the ante on security requirements and is expected to fulfill the requirements ofall the classes and divisions below it.

d) Describe any four protocols used for authentication.

(1 Mark each protocol)

- Direct authentication
    - Based on a shared secret master key
    - Based on a public-key system
    - Diffie-Hellman

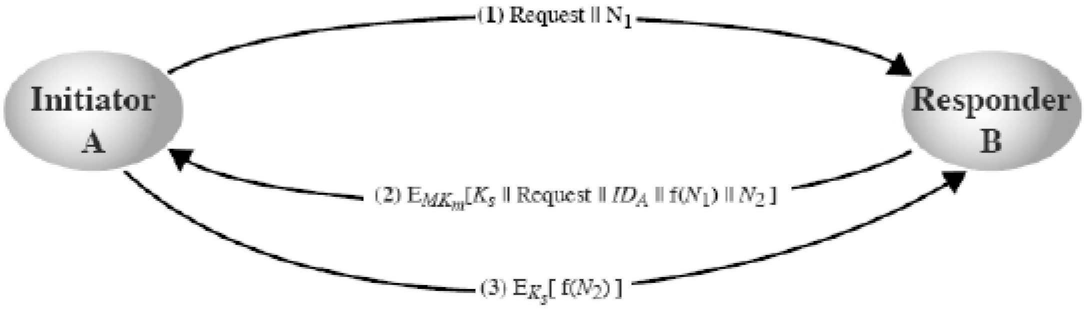
- Mediated authentication
    - Based on key distribution centers
    - Otway-Rees
    - Kerberos

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

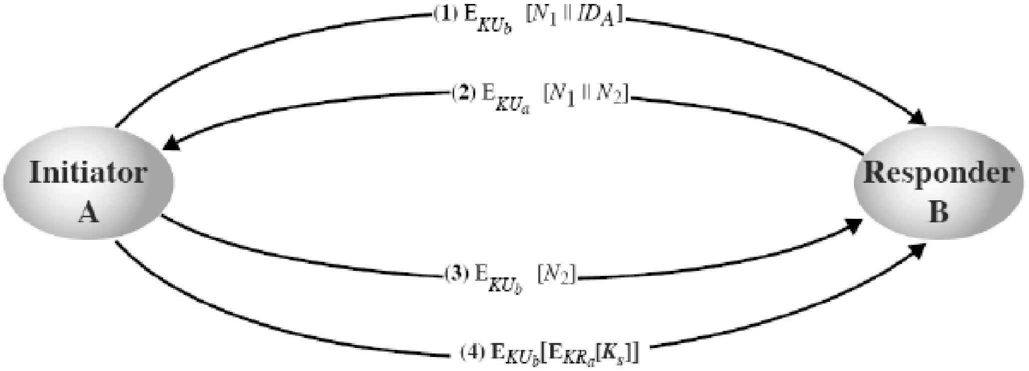
Using the new session key, A return $f(N_2)$ to B; B is sure of A‘s identity: only A can read the message he sent, including the session key B knows that the message is fresh: A sends a transformation on N_2.



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.


(1) E_{KU_b} $[N_1 \| ID_A]$
(2) E_{KU_a} $[N_1 \| N_2]$
Initiator A
Responder B
(3) E_{KU_b} $[N_2]$
(4) $E_{KU_b}[E_{KR_a}[K_s]]$

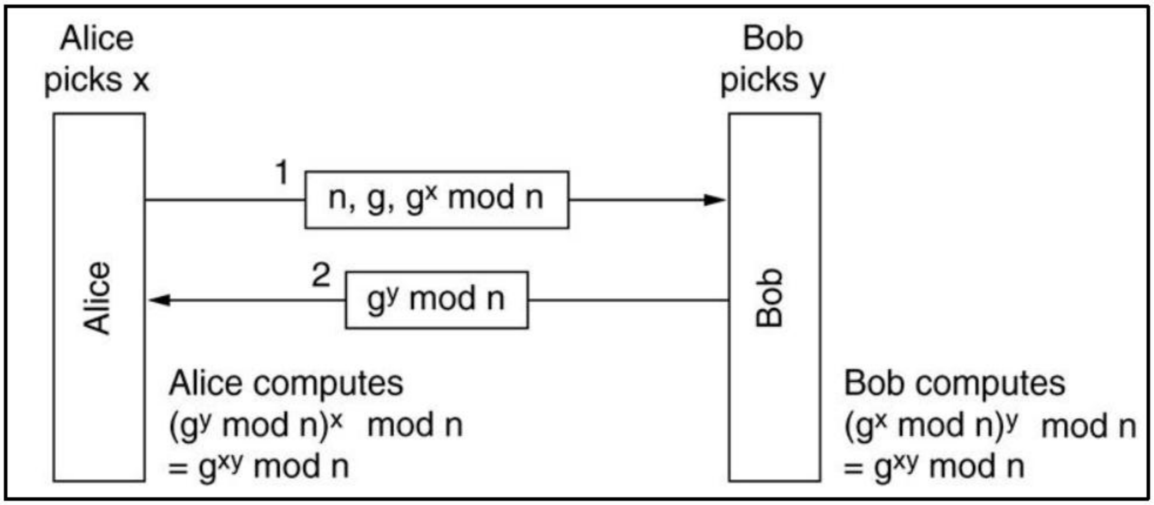
Diffie-Hellman key exchange

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 mod n) Bob sends Alice a message containing g^y mod 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:

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

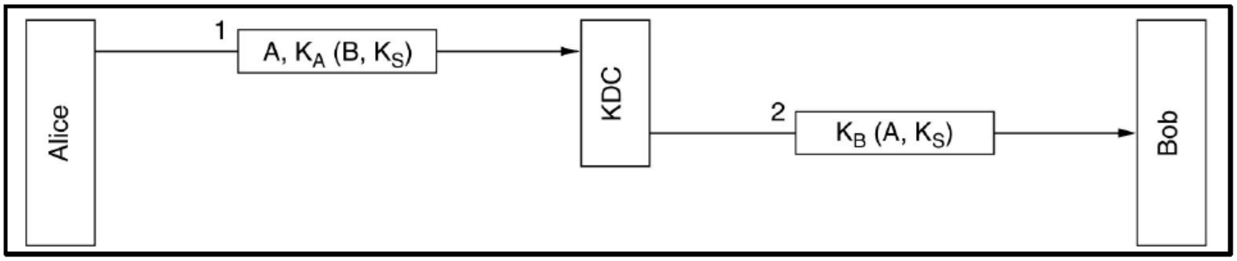


Based on key distribution centers:-

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.

B. Attempt any one:

a) Describe classical encryption techniques.

(Any two encryption methods are expected 3 Marks each)

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

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 TEXT	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 TEXT	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

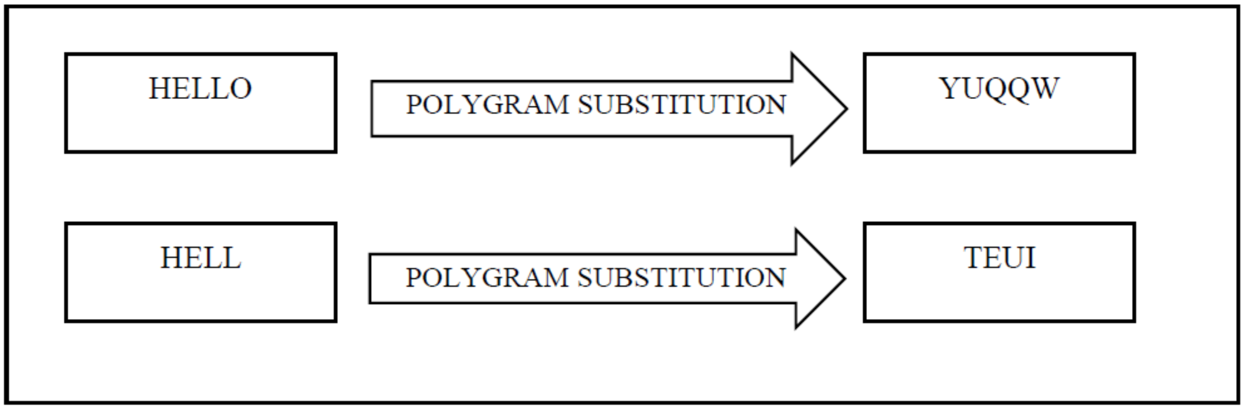
PLAIN TEXT: INFORMATION SECURITY
CIPHER TEXT: FCKMUHEBFMC WAXSUFBP

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 TEXT	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:

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

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:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} \equiv 6(16\cdot15-10\cdot17)-24(13\cdot15-10\cdot20)+1(13\cdot17-16\cdot20) \equiv 441 \equiv 25 \pmod{26}$$

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”**

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		

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.

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.

b) Describe play fair cipher and describe step by step encryption of plain with example.

(Description 2 Marks; Encryption 2 Marks; Decryption 2 Marks)

The Playfair Cipher was first described by Charles Wheatstone in 1854, and it was the first example of a Digraph Substitution Cipher. It is named after Lord Playfair, who heavily promoted the use of the cipher to the military.

When it was first put to the British Foreign Office as a cipher, it was rejected due to its perceived complexity. However, it was later adopted as a military cipher due to it being reasonably fast to use, and it requires no special equipment, whilst also providing a stronger cipher than a Monoalphabetic Substitution Cipher. It was used in the Second Boer War, and both World War I and World War II to different degrees. It is no longer used by military forces since the advent of powerful computers, but in its day it provided a relatively secure cipher which was easy to implement quite quickly.

Encryption

In order to encrypt using the Playfair Cipher, we must first draw up a Polybius Square (but without the need for the number headings). This is usually done using a keyword, and either combining "i" and "j" or omitting "q" from the square.

We must now split the plaintext up into digraphs (that is pairs of letters). On each digraph we perform the following encryption steps:

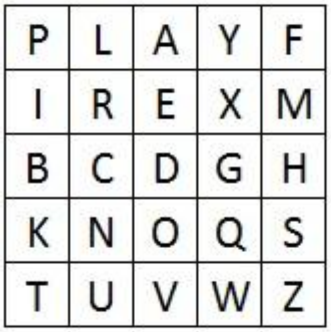
If the digraph consists of the same letter twice (or there is only one letter left by itself at the end of the plaintext) then insert the letter "X" between the same letters (or at the end), and then continue with the rest of the steps.

If the two letters appear on the same row in the square, then replace each letter by the letter immediately to the right of it in the square (cycling round to the left hand side if necessary).

If the two letters appear in the same column in the square, then replace each letter by the letter immediately below it in the square (cycling round to the top of the square if necessary).

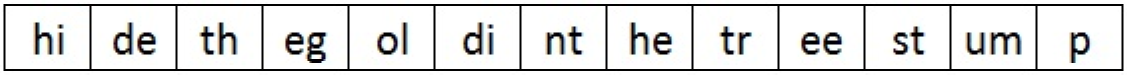
Otherwise, form the rectangle for which the two plaintext letters are two opposit corners. Then replace each plaintext letter with the letter that forms the other corner of the rectangle that lies on the same row as that plaintext letter (being careful to maintain the order).

As an example we shall encrypt the plaintext "hide the gold in the tree stump" using the keyphrase playfair example. Firstly we must generate the Polybius Square that we are going to use. We do this by setting out a 5x5 grid, and filling it with the alphabet, starting with the letters of the keyphrase, and ignoring any letters we already have in the square. We are also going to combine "I" and "J" in the square.



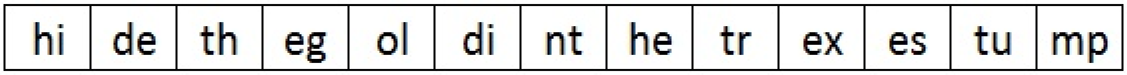
P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

We must now split the plaintext into digraphs. At this point it is a good idea to apply Rule 1, and split up any double letter digraphs by inserting an "x" between them. The first image below shows the initial digraph split of the plaintext, and the second image displays how we split up the "ee" into "ex" and "es". In this case, when we insert this extra "x", we no longer need to have one at the end of the plaintext.



hi	de	th	eg	ol	di	nt	he	tr	ee	st	um	p

The initial split into digraphs.

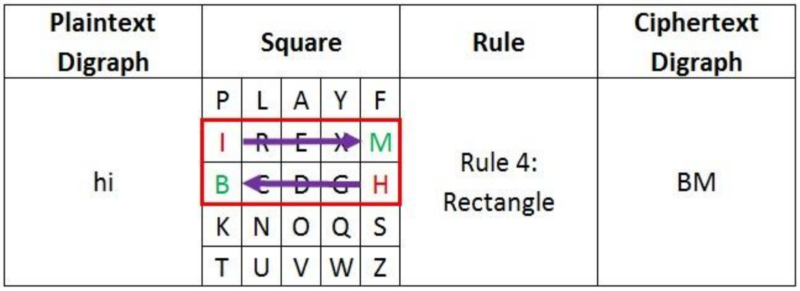


hi	de	th	eg	ol	di	nt	he	tr	ex	es	tu	mp

The digraph split once we apply Rule 1, and remove any digraphs made from two of the same letter.

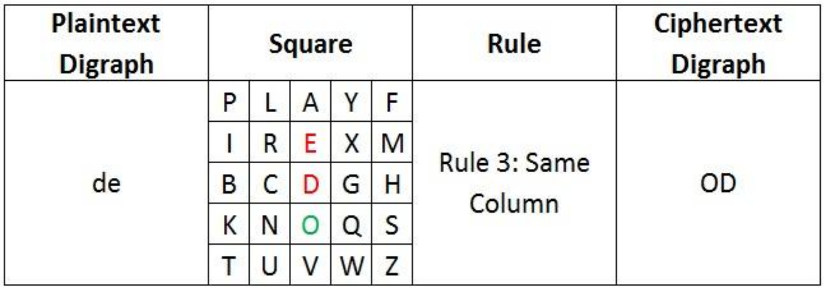
We now take each digraph in turn and apply rule 2, 3 or 4 as necessary. Each step is show below with a visual representation of what is done for each digraph.

Step 1:-



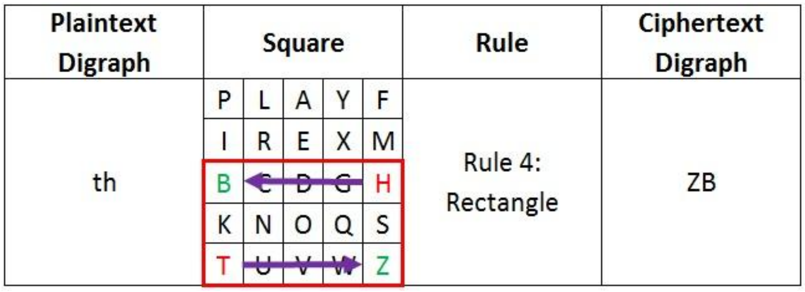
Plaintext Digraph	Square	Rule	Ciphertext Digraph
hi	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 4: Rectangle	BM

Step 2:



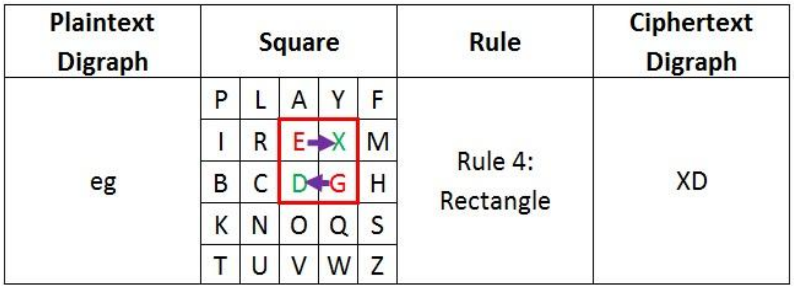
Plaintext Digraph	Square	Rule	Ciphertext Digraph
de	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 3: Same Column	OD

Step 3:



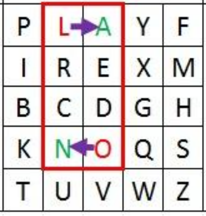
Plaintext Digraph	Square	Rule	Ciphertext Digraph
th	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 4: Rectangle	ZB

Step 4

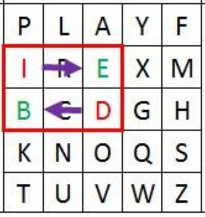


Plaintext Digraph	Square	Rule	Ciphertext Digraph
eg	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 4: Rectangle	XD

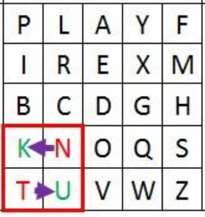
Step 5

Plaintext Digraph	Square	Rule	Ciphertext Digraph
ol	 P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 4: Rectangle	NA

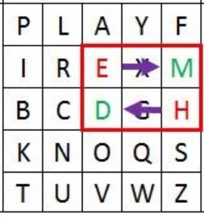
Step 6

Plaintext Digraph	Square	Rule	Ciphertext Digraph
di	 P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 4: Rectangle	BE

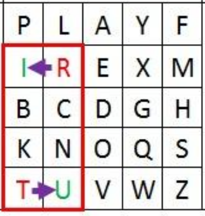
Step 7

Plaintext Digraph	Square	Rule	Ciphertext Digraph
nt	 P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 4: Rectangle	KU

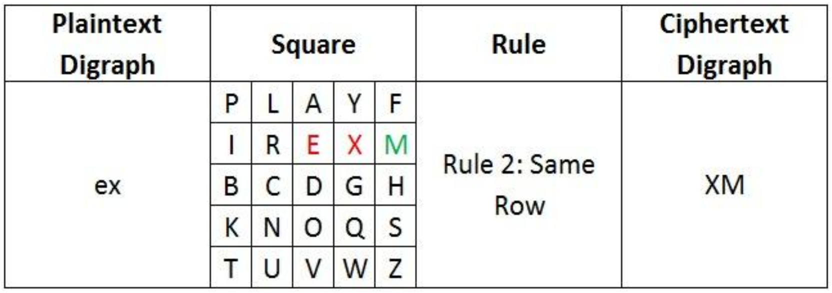
Step 8

Plaintext Digraph	Square	Rule	Ciphertext Digraph
he	 P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 4: Rectangle	DM

Step 9

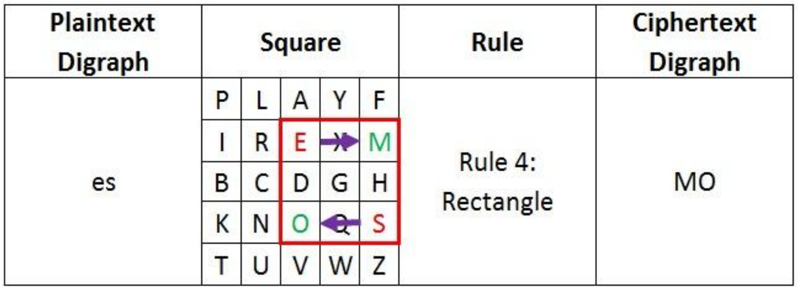
Plaintext Digraph	Square	Rule	Ciphertext Digraph
tr	 P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 4: Rectangle	UI

Step 10



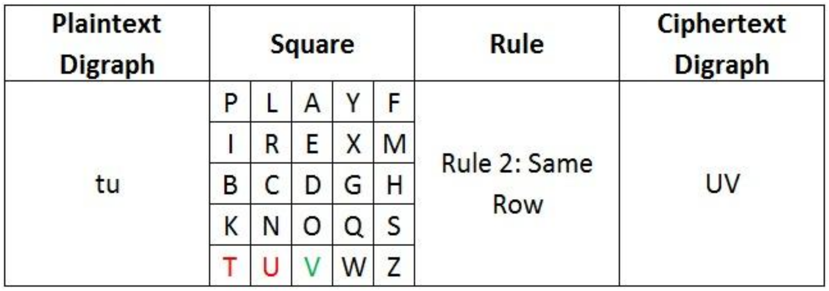
Plaintext Digraph	Square	Rule	Ciphertext Digraph
ex	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 2: Same Row	XM

Step 11



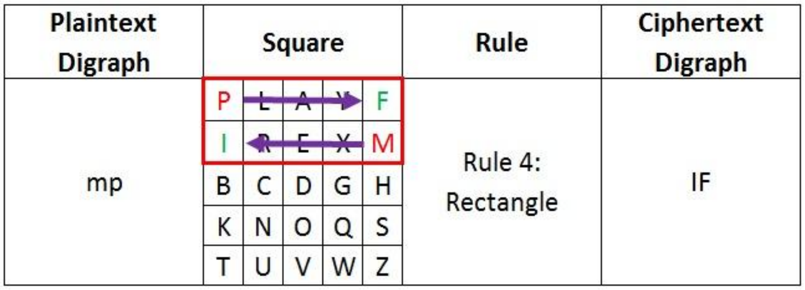
Plaintext Digraph	Square	Rule	Ciphertext Digraph
es	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 4: Rectangle	MO

Step 12



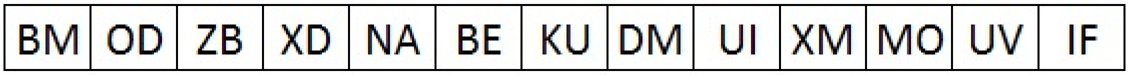
Plaintext Digraph	Square	Rule	Ciphertext Digraph
tu	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 2: Same Row	UV

Step 13



Plaintext Digraph	Square	Rule	Ciphertext Digraph
mp	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	Rule 4: Rectangle	IF

We can now take each of the ciphertext digraphs that we produced and put them all together.



BM	OD	ZB	XD	NA	BE	KU	DM	UI	XM	MO	UV	IF

We can now write out the ciphertext as a long string "BMODZBXDNABEKUDMUIXMMOUVIF" or split it into block of 5 "BMODZ BXDNA BEKUD MUIXM MOUVI F" or even give it the same layout as the original "BMOD ZBX DNAB EK UDM UIXMM OUVIF"

Decryption:-

Decryption is nearly identical to the encryption process, except for rules 2 and 3 we must take the letters to the left and above respectively. Also, we remove any extra "X" in the decrypted text to reveal the final plaintext.

We shall decipher the ciphertext "UA ARBED EXAPO PR QNX AXANR" which has been encrypted using the keyword example. Firstly we must generate the Polybius Square which we are using, as shown to the right.

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

The Mixed Square with keyword example

The next step is to split the ciphertext into digraphs. There is no need to add any "X" in the decryption process as these will be revealed as we decrypt.

UA	AR	BE	DE	XA	PO	PR	QN	XA	XA	NR

Now we apply the rules as needed to each digraph in the ciphertext.

Step 1:

Ciphertext Digraph	Square	Rule	Plaintext Digraph
UA	E ← A M P L B C D F G H I K N O Q R S T U → W Y Z	Rule 4: Rectangle	we

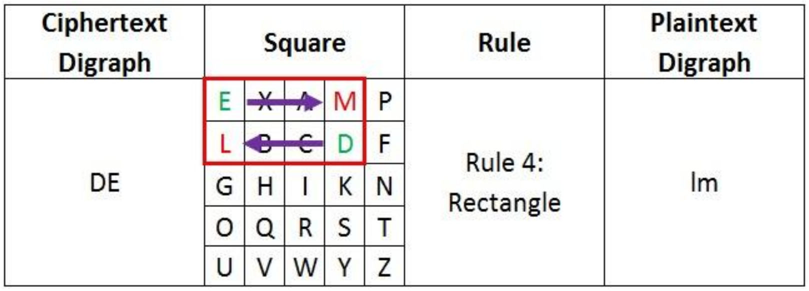
Step 2:

Ciphertext Digraph	Square	Rule	Plaintext Digraph
AR	E X A M P L B C D F G H I K N O Q R S T U V W Y Z	Rule 3: Same Column	wi

Step 3:

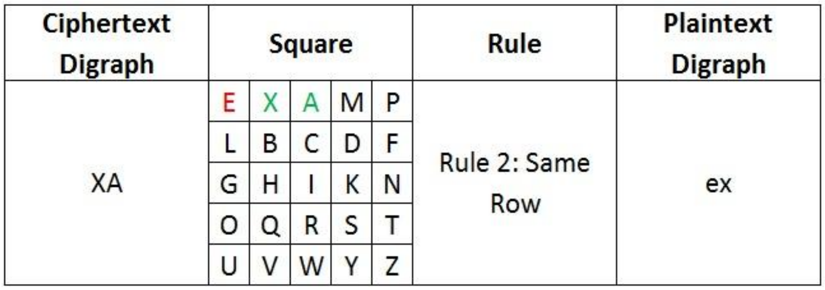
Ciphertext Digraph	Square	Rule	Plaintext Digraph
BE	E → X A M P L ← B C D F G H I K N O Q R S T U V W Y Z	Rule 4: Rectangle	lx

Step 4:



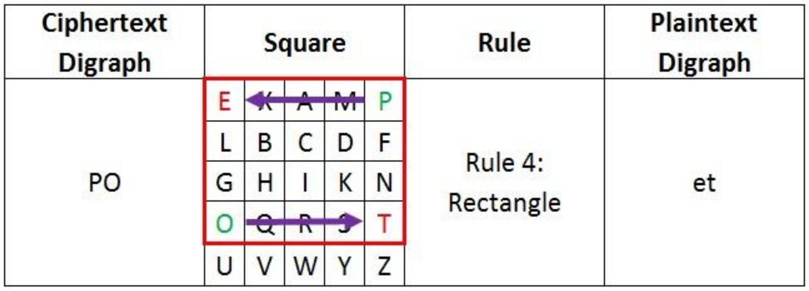
Ciphertext Digraph	Square	Rule	Plaintext Digraph
DE	E X A M P L B C D F G H I K N O Q R S T U V W Y Z	Rule 4: Rectangle	lm

Step 5:



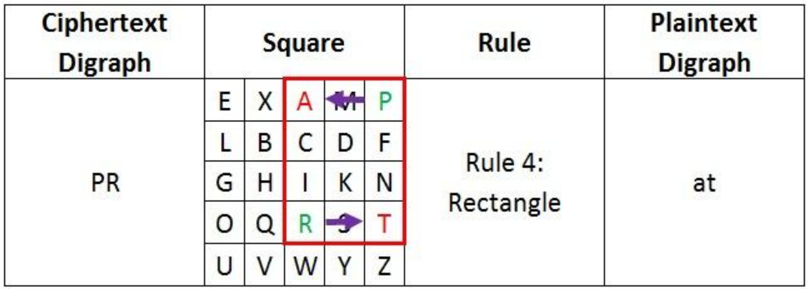
Ciphertext Digraph	Square	Rule	Plaintext Digraph
XA	E X A M P L B C D F G H I K N O Q R S T U V W Y Z	Rule 2: Same Row	ex

Step 6:



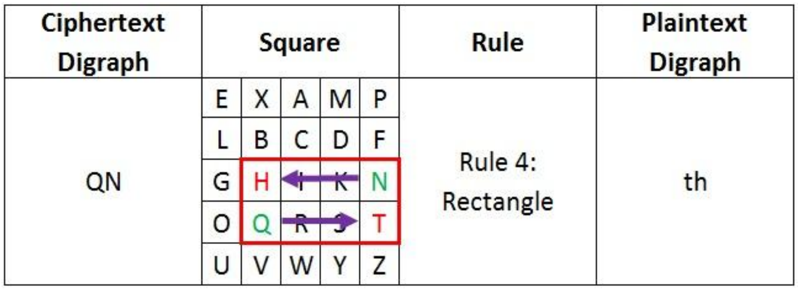
Ciphertext Digraph	Square	Rule	Plaintext Digraph
PO	E X A M P L B C D F G H I K N O Q R S T U V W Y Z	Rule 4: Rectangle	et

Step 7:



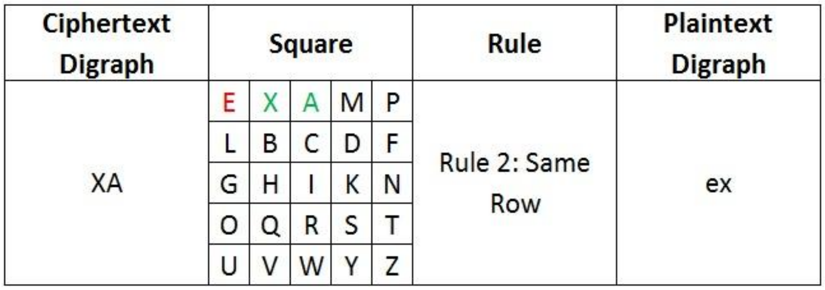
Ciphertext Digraph	Square	Rule	Plaintext Digraph
PR	E X A M P L B C D F G H I K N O Q R S T U V W Y Z	Rule 4: Rectangle	at

Step 8:



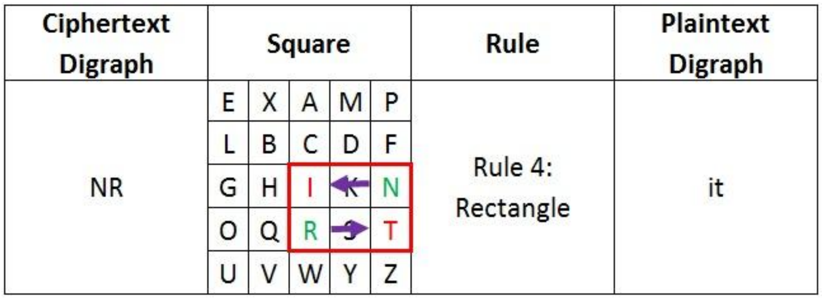
Ciphertext Digraph	Square	Rule	Plaintext Digraph
QN	E X A M P L B C D F G H I K N O Q R S T U V W Y Z	Rule 4: Rectangle	th

Step 9:



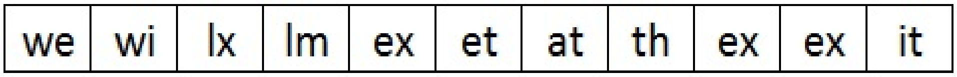
Ciphertext Digraph	Square	Rule	Plaintext Digraph
XA	E X A M P L B C D F G H I K N O Q R S T U V W Y Z	Rule 2: Same Row	ex

Step 10:



Ciphertext Digraph	Square	Rule	Plaintext Digraph
NR	E X A M P L B C D F G H I K N O Q R S T U V W Y Z	Rule 4: Rectangle	it

We now combine all the digraphs together.



we	wi	lx	lm	ex	et	at	th	ex	ex	it

So we get the message "we wilxlmexet at thex exit". When we remove the unnecessary "x"s we get a final plaintext of "we will meet at the exit". Note that we cannot just remove all the "x"s as one is part of the word "exit".

Q .5 Attempt any two.

a) State importance of data recovery. State Procedure to recover the delete file.
(Importance- 4 marks Procedure- 4 Marks)

Ans. Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible for some reason.

When files have been mistakenly deleted and need to be recovered, data recovery is necessary. This is the act of retrieving deleted or erased files using one of several methods.

Data can be lost because of reasons:
Accident deletion of files
Due to disk malfunction or failure
Due to accidentally formatting the storage device
Due to problem with system and/or application software
Due to physical damage to the storage device

File Deletion

Any file that's deleted actually stays on your drive until it's overwritten with another file. This means that if you act fast, you actually have a pretty good chance of getting the file back. In the case of file deletion, you can use file recovery software like TestDisk to recover the file.

File Corruption

If you got "corrupt hard drive" errors. it's still possible that data could be recovered. If you attach the hard drive to another computer, you might find that only the operating system has been corrupted, and that the rest of your data is fine in this case, it's just a matter of copying everything to another hard drive.

File System Format or Damage

Similar to deleting a file, formatting a file system destroys information about the previous files and structure of the disk, but the amount of data that's erased depends on the system format.

For example, formatting with FAT results in the destruction of a large amount of data and rewriting that section of the disk with zeroes, significantly reducing the likelihood that you'll be able to recover your data. Some file systems, like NTFS, will have a higher likelihood of recovery if they're overwritten with the same file system, while others actually have a smaller chance if they're overwritten with the same system..

Physical Drive Damage

Recovering files that have been deleted or formatted is one thing getting files off of a drive that's been damaged is another. When a hard drive fails because of physical damage, it can be related to a number of factors, such as a broken controller board or a crashed head. These issues can be fixed by replacing the broken part.

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.

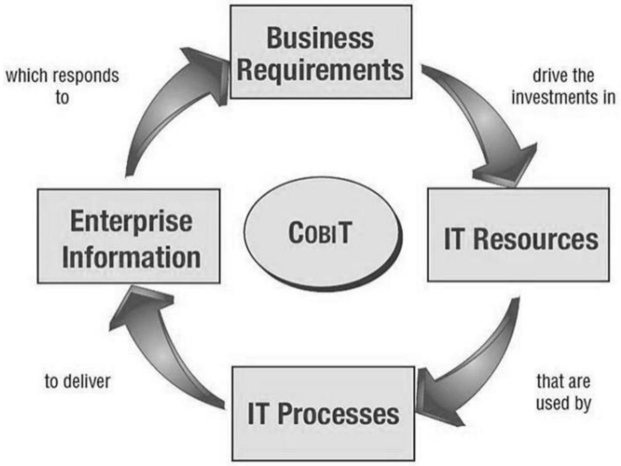
If the file is deleted from the recycle bin, or by using shift + delete button, the simplest and easiest way to recover deleted file is by using a data recover software.

- 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.

b) Describe ITIL framework. (Diagram -2 Marks Explanation -6Marks)
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.



The ITIL framework is a source of good practice in service management. The ITIL library has the following components:
• ITIL Core: Best-practice publications that may be used by any organization that provides services to a business.
• ITIL Complementary Guidance: A complementary set of publications with guidance specific to industry sectors, organization types, operating models and technology architectures.

The objective of the ITIL Service Management framework is to provide services that are fit for purpose, stable and so reliable that the business views them as a trusted provider. ITIL has been deployed successfully around the world for over 20 years. Over this time, the framework has evolved from a specialized set of Service Management topics with a focus on function, to a process-based framework which now provides a broader holistic Service Lifecycle.

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

c) Explain transposition cipher techniques with example.
(Explanation 4m, Example-4M)

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.

Q.6 Attempt any four

a) How cybercrime are investigated?

(Explanation -4Marks any suitable points can be consider)

Computer crime or cybercrime, is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Netcrime is criminal exploitation of the Internet, inherently a cybercrime.

COMPUTER CRIME INVESTIGATION

The computer crime investigation should start immediately following the report of any alleged criminal activity. Many processes ranging from reporting and containment to analysis and eradication should be accomplished as soon as possible after the attack. An incident response plan should be formulated, and a Computer Emergency Response Team (CERT) should be organized before the attack. The incident response plan will help set the objective of the investigation and will identify each of the steps in the investigative process.

Detection and Containment

Before any investigation can take place, the system intrusion or abusive conduct must first be detected. The closer the detection is to the actual intrusion not only helps to minimize system damage, but also assists in the identification of potential suspects. To date, most computer crimes have either been detected by accident or through the laborious review of lengthy audit trails.

Report to Management

All incidents should be reported to management as soon as possible. Prompt internal reporting is imperative to collect and preserve potential evidence. It is important that information about the investigation be limited to as few people as possible. Information should be given on a need-to-know basis, which limits the possibility of the investigation being leaked. In addition, all communications related to the incident should be made through an out-of-band method to ensure that the intruder does not intercept any incident-related information. In other words, E-mail should not be used to discuss the investigation on a compromised system.

Determine if Disclosure is Required

Determine if a disclosure is required or warranted due to laws or regulations. Disclosure may be required by law or regulation or may be required if the loss affects the corporation's financial statement. Even if disclosure is not required, it is sometimes better to disclose the attack to possibly deter future attacks. This is especially true if the victim organization prosecutes criminally or civilly. Some of these attacks would probably result in disclosure:

· A bank fraud.

· An attack on a public safety system (e.g., air traffic control)

Investigation Considerations

Once the preliminary investigation is complete and the victim organization has made a decision related to disclosure, the organization must decide on the next course of action. The victim organization may decide to do nothing, or it may attempt to eliminate the problem and just move on. Deciding to do nothing is not a very effective course of action; because the organization may be held culpably negligent should another attack or intrusion occur. The victim organization should at least attempt to eliminate the security hole that allowed the breach, even if it does not plan to bring the case to court. If the attack is internal, the organization may wish to conduct an investigation that might only result in the dismissal of the subject. If it decides to further investigate the incident, the organization must also determine if it is going to prosecute criminally or civilly, or merely conduct an investigation for insurance purposes. If an insurance claim is to be submitted, a police report is usually necessary.

Who Should Conduct the Investigation?

Based on the type of investigation (i.e., civil, criminal, or insurance) and extent of the abuse, the victim must decide who is to conduct the investigation. This used to be a straightforward decision, but high-technology crime has altered the decision-making process. Inadequate and untested laws, combined with the lack of technical training and technical understanding, has severely hampered the effectiveness of the criminal justice system when dealing with computer related crimes.

The Investigative Process

As with any type of criminal investigation, the goal of the investigation is to know the who, what, when, where, why, and how. It is important that the investigator log all activity and account for all time spent on the investigation. The amount of time spent on the investigation has a direct effect on the total dollar loss for the incident, which may result in greater criminal charges and, possibly, stiffer sentencing. Finally, the money spent on investigative resources can be reimbursed as compensatory damages in a successful civil action. Once the decision is made to further investigate the incident, the next course of action for the investigative team is to establish a detailed investigative plan, including the search and seizure plan. The plan should consist of an informal strategy that will be employed throughout the investigation, including the search and seizure:

· Identify what type of system is to be seized.

· Identify the search and seizure team members.

· Determine if there is risk that the suspect will destroy evidence or cause greater losses.

Identify the Type of System that is to Be Seized

It is imperative to learn as much as possible about the target computer systems. If possible, the investigator should obtain the configuration of the system, including the network environment (if any), hardware, and software. The following questions should be answered before the seizure:

· Who are the system experts? They should be part of the team.

· Is a security system in place on the system? If so, what kind? Are passwords used? Can a root password be obtained?

· Where is the system located? Will simultaneous raids be required?

· What are the required media supplies to be obtained in advance of the operation?

· What law has been violated? Are there elements of proof? If yes, these should be the focus of the search and seizure. · What is the probable cause? Is a warrant necessary?

· Will the analysis of the computer system be conducted on site, in the investigator's office, or in a forensics lab? Identify the Search and Seizure Team Members.

There are different rules for search and seizure based on who is conducting the search. Under the Fourth Amendment, law enforcement must obtain a warrant, which must be based on probable cause. In either case, a team should be identified and should consist of these members:

· The lead Investigator.

· The information security department.

· The legal Department.

· Technical assistance--the system administrator as long as he or she is not a suspect.

Obtaining and Serving Search Warrants.

If it is believed that the suspect has crucial evidence at his or her home or office, a search warrant will be required to seize the evidence. If a search warrant is going to be needed, it should be done as quickly as possible before the intruder can do further damage. The investigator must establish that a crime has been committed and that the suspect is somehow involved in the criminal activity. He or she must also show why a search of the suspect's home or office is required. The victim may be asked to accompany law enforcement when serving the warrant to identify property or programs.

Executing the Plan

The first step in executing the plan is to secure the scene, which includes securing the power, network servers, and telecommunications links. If the suspect is near the system, it may be necessary to physically remove him or her. It may be best to execute the search and seizure after normal business hours to avoid any physical confrontation. Keep in mind, that even if a search is conducted after hours, the suspect may still have remote access to the system through a LAN-based modem connection, PC based modem connection, or Internet connection. The area should be entered slowly so as not to disturb or destroy evidence. The entire situation should be evaluated. In no other type of investigation, can evidence be destroyed more quickly. The keyboard should not be touched, because this action may invoke a Trojan Horse or some other rogue or malicious program. The computer should not be turned off unless it appears to be active (i.e., formatting the disk, deleting files, or initiating some I/O process). The disk activity light should be looked at, as well as listening for disk usage. If the computer must be turned off, the wall plug should be pulled, rather than using the On/Off switch. Notes, documentation, passwords, and encryption codes should be looked for. The following questions must be answered to control the scene effectively:

· Is the computer system turned on?
· Is there a modem attached? If so,
  --Are there internal modems?
  --Are telephone lines connected to the computer
· Is the system connected to a LAN?

Surveillance

Two forms of surveillance are used in computer crime investigations: physical and computer. Physical surveillance can be generated at the time of the abuse, through CCTV security cameras, or after the fact. When after the fact, physical surveillance is usually performed undercover. It can be used in an investigation to identify a subject's personal habits, family life, spending habits, or associates. Computer surveillance is achieved in a number of ways. It is done passively through audit logs or actively by way of electronic monitoring. Electronic monitoring can be accomplished through keyboard monitoring, network sniffing, or line monitoring. In any case, it generally requires a warning notice or explicit statement in the corporate security policy, indicating that the company can and will electronically monitor any and all system or network traffic. Without such a policy or warning notice, a warrant is normally required.

Investigative and Forensic Tools

Investigative Information Sources When conducting an internal investigation, it is important to remember that the witness statements and computer related evidence are not the only sources of information useful to the investigation. Personnel files provide a wealth of information related to an employee's employment history. It may show past infractions by the employee or disciplinary action by the company. Telephone logs can possibly identify any accomplices or associates of the subject. At a minimum, they will identify the suspect's most recent contacts. Finally, security logs, time cards, and check-in sheets will determine when a suspected insider had physical access to a particular system.

Investigative Reporting

The goal of the investigation is to identify all available facts related to the case. The investigative report should provide a detailed account of the incident, highlighting any discrepancies in witness statements. The report should be a well organized document that contains a description of the incident, all witness statements, references to all evidentiary articles, pictures of the crime scene, drawings and schematics of the computer and the computer network (if applicable), and finally, a written description of the forensic analysis. The report should state final conclusions, based solely on the facts. It should not include the investigator's opinions. The investigator should keep in mind that all documentation related to the investigation is subject to discovery by the defense, so that he or she should exercise caution in any writings associated with the investigation.

COMPUTER FORENSICS

Computer forensics is the study of computer technology as it relates to the law. The objective of the forensic process is to learn as much about the suspect system as possible. This generally means analyzing the system by using a variety of forensic tools & processes, and that the examination of the suspect system may lead to other victims and other suspects. The actual forensic process is different for each system analyzed, but the guidelines in Exhibit 4 should help the investigator or analyst conduct the forensic process.

b) What is access control? Lit types of access control. Describe any one.
(Access control-1M, List-1 M, Desciption-2M)

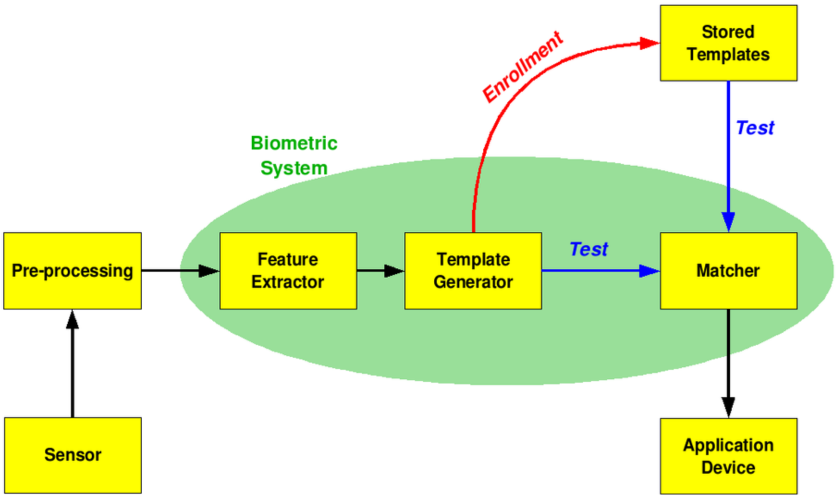
Access control model is a framework that dictates access control using various access- control technologies. There are standard access control models which are highly domain and implementation independent. Each access control model has its own merits and demerits, and the specific business objectives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

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

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

Biometrics

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.

Authentication:

Authentication or identification is the first step in any access control solution. It is the process of identifying the user to verify whether he/she is what he/she claims to be. Normally, identification is done with the help of information that is known to everyone (i.e., user name or user ID) and some personal information known only to the subject (i.e. password). Faced with the threat of identity theft and increasing consequences associated with failing to secure information, enterprises are increasingly looking for stronger forms of authentication to enhance their overall security capabilities. At the same time, enterprises and governments need to take into account other important considerations such as usability, total cost of deployment and maintenance, and integration with existing security solution offerings. Usernames and passwords are the most common authentication techniques. But most organizations do not depend on user name authentication alone since username and passwords are an authentication solution for low-value transactions and for accessing non-sensitive information over the network. Also, experience has shown that usernames and passwords provide relatively weak authentication because they can often be guessed or stolen. They are often difficult to deploy because each application may implement its own scheme, adding to both development cost and user complexity. Also, it is very difficult to maintain and reset the password. Determining the appropriate level of authentication that meets your budget requirements is essential when implementing your secure identity management solution. It is very crucial to identify the appropriate authentication technique depending upon the nature of the business and sensitivity of the information. One has to consider various authentication methods and their pros and cons. The means of authentication are often discussed in terms of “factors” of proof, such as:

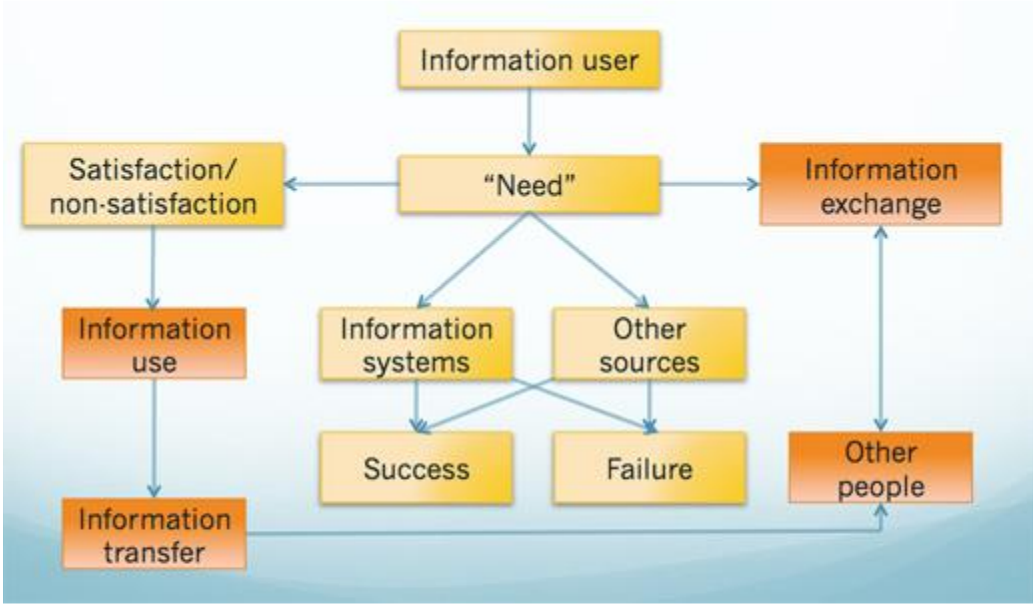
● Something you know to prove your identity (e.g., a PIN)
● Something you have to prove your identity (e.g., a smart card)
● Something you are to prove your identity (e.g., a fingerprint)

A good authentication technique contains at least two of the above methods.

In a client server environment, strong authentication is a combination of server and client authentication: ● Server authentication is when the server proves its identity to the client.
● Client authentication is when clients prove their identity to the server.

c) **Describe clerk Wilson model of integrity.(**diagram -1M Explanation 3 Marks)

The Clark-Wilson security model is based on preserving information integrity against the malicious attempt of tampering data. The security model maintains that only authorized users should make and be allowed to change the data, unauthorized users should not be able to make any changes, and the system should maintain internal and external data consistency.



The Clark-Wilson model requires well-formed transaction. A well-formed transition is that operations and data feeds and processing are consistent within the system. According to Sonya Blake o "The principle of well-formed transaction is defined as a transaction where the user is unable manipulate data arbitrarily, but only in constrained (limitations or boundaries) ways that preserve or ensure the integrity of the data. A security system in which transactions are well-formed ensures that only legitimate actions can be executed. Ensures the internal data is accurate and consistent to what it represents in the real world" (Blake).

Data objects can only be manipulated by a certain set of programs. Users have access to the programs rather than to the data. (e.g. this is like the WWW or a database). Think of the discussion last week about restricting access based on "role".

Separation of duties: assigning different roles to different users. Users might have to collaborate in order to achieve some secure operation. For instance, think of the dual-key approach to arming nuclear warheads. Or in Star Trek, the authorization and command sequence to self-destruct the Enterprise by three ranking officers with voice-print identification combined with a simple, easy to remember sequence (sufficiently complicated to avoid accidents).

The Clark-Wilson model also tries to address the relationship between the system and the acceptance of information from outside world by insisting on auditing of transactions. This will not help security/integrity but it can detect breaches. In summary:

Subjects/users are identified and authenticated.

Objects/data can only be accessed by authorized programs (ensures integrity).

Subjects/users only have access to certain programs.

An audit log is maintained over external transactions.

The system must be certified in order for it to work.

d) Explain the following :
(Each explanation -2Marks)

Authorization

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

Authentication

-Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.
-To access most technology services of Indiana University, you must provide such proof of identity.
-In private and public computer networks (including the Internet), authentication is commonly done through the use of login passwords or passphrases; knowledge of such is assumed to guarantee that the user is authentic.
-Thus, when you are asked to "authenticate" to a system, it usually means that you enter your username and/or password for that system.

e) Describe double columnar transposition cipher technique with example. also state criteria for selecting keyword.
(Explanation -1M, Example-2Marks, Criteria-1Marks)

Double Transposition Cipher:
Here we take the original plaintext P and encipher it using a column transposition with one keyword creating an intermediate ciphertext C'. Then we will encipher C' using a second keyword in a column transposition creating the final ciphertext C.
Criteria: It is not necessary for the two keywords to be of the same length. If necessary, we can pad C' with null characters so that it becomes the appropriate length. In decrypting, these nulls would have to be deleted after properly decrypting the first step.

Here is an example of double transposition:

Keyword #1: HOMES Keyword #2: PICNIC

Plaintext: ITBETTERSTOPRAININGBEFORETHEGAME

First, store the plaintext in an array with 5 columns:

1	3	2	0	4	
H	O	M	E	S	= Keyword #1

I	T	B	E	T
T	E	R	S	T
O	P	R	A	I
N	I	N	G	B
E	F	O	R	E
T	H	E	G	A
M	E	X	X	X

Now, to get the intermediate ciphertext, read off the columns in the designated order, based on the keyword:

Intermediate Ciphertext: ESAGRGXITONETMBRPNOEXTEPIFHETTIBEAX

Now, copy these into an array with 6 columns:

5 2 0 4 3 1
P I C N I C = Keyword #2

E	S	A	G	R	G
X	I	T	O	N	E
T	M	B	R	R	N
O	E	X	T	E	P
I	F	H	E	T	T
I	B	E	A	X	X

To get the final ciphertext, read these off of the columns in the designated order.

Final Ciphertext: ATBXHEGENPTXSIMEFBRNRETXGORTEAEXTOII