



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: **17518**

Important Instructions to examiners:

- 1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
- 2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
- 3) The language errors such as grammatical, spelling errors should not be given 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. No.	Sub Q. N.	Answers	Marking Scheme
1.	(A)	Attempt any THREE:	3x4 = 12
	(a)	Define information. State need and importance of information.	4M
	Ans:	<p>Information: It is a resource fundamental to the success of any business.</p> <p>Data: It is a collection of all types of information which can be stored and used as per requirement.</p> <p>Knowledge: It is based on data that is organized, synthesized or summarized and it is carried by experienced employees in the organization.</p> <p>Action: It is used to pass the required information to a person who needs it with the help of information system.</p> <p>Need and importance of Information:</p> <ol style="list-style-type: none"> 1. Information is essential in organization because damage to information/data can cause disruptions in a normal process of organization like financial loss. 2. Information is the most valuable resources of an organization so its management is crucial to making good business decision. 3. Main objective of an information system is to monitor and document the operations of other systems 4 To satisfy the decision making capability, the information system should be call for intensive and complex interaction between different units in the organization. 	(Define: 1 mark, Need and importance: 3 marks)

(b)	Define information security. Explain the concept of risk management with its components.	4M
Ans:	<p>Information security (IS) is designed to provide the confidentiality, integrity and availability of computer system data from those with malicious intentions.</p> <div style="text-align: center; margin: 10px 0;"> <pre> graph TD RM[Risk Management] --> RI[Risk Identification] RM --> RA[Risk Assessment] RM --> RC[Risk Control] RI --> RA RA --> RC RI --- RI1[Identify & inventory assets] RI --- RI2[Classify & prioritize assets] RI --- RI3[Identify & prioritize threats] RA --- RA1[Identify vulnerabilities between assets & threats] RA --- RA2[Identify & qualify asset exposure] RC --- RC1[Select strategy] RC --- RC2[Justify controls] RC --- RC3[implement & monitor controls] </pre> </div> <p style="text-align: center;">Fig: Risk management components</p> <p>Risk management: This is the process of identifying and controlling risks facing an organization</p> <ul style="list-style-type: none"> • Risk identification: This is the process of examining an organization’s current information technology security situation. • Risk Assessment: Risk assessment is the determination of the extent to which the organization’s information assets are exposed or at risk • Risk control: applying controls to reduce risks to an organizations data and information systems <p>Four strategies to control each risk:</p> <ol style="list-style-type: none"> 1. Avoidance: Apply safeguards that eliminate or reduce residual risk 2. Transference: Transfer the risk to other assets, other processes or other organizations. 3. Mitigation: Reduce the impact should the vulnerability be exploited 4. Acceptance: Understand the consequences and accept the risk without control or mitigation 	<p>(Define: 1mark, Diagram: 1 mark, Explanation: 2 marks)</p>



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: **17518**

(c)	Difference between symmetric and asymmetric cryptography.	4M																								
Ans:	<table border="1"> <thead> <tr> <th data-bbox="237 390 548 474">Categories</th> <th data-bbox="548 390 940 474">Symmetric Cryptography</th> <th data-bbox="940 390 1365 474">Asymmetric Cryptography</th> </tr> </thead> <tbody> <tr> <td data-bbox="237 474 548 617">Key used for encryption /decryption</td> <td data-bbox="548 474 940 617">Same key is used for encryption & decryption.</td> <td data-bbox="940 474 1365 617">One key is used for encryption & another different key is used for decryption.</td> </tr> <tr> <td data-bbox="237 617 548 688">Key process</td> <td data-bbox="548 617 940 688">Ke=Kd (Same)</td> <td data-bbox="940 617 1365 688">Ke# Kd (not same)</td> </tr> <tr> <td data-bbox="237 688 548 793">Speed of encryption decryption</td> <td data-bbox="548 688 940 793">Very fast</td> <td data-bbox="940 688 1365 793">Slower</td> </tr> <tr> <td data-bbox="237 793 548 907">Size of resulting encrypted text</td> <td data-bbox="548 793 940 907">Usually same as or less than the original clear text size.</td> <td data-bbox="940 793 1365 907">More than the original clear text size.</td> </tr> <tr> <td data-bbox="237 907 548 1012">Key agreement/exchange</td> <td data-bbox="548 907 940 1012">A big problem</td> <td data-bbox="940 907 1365 1012">No problem at all.</td> </tr> <tr> <td data-bbox="237 1012 548 1167">Usage</td> <td data-bbox="548 1012 940 1167">Mainly used for encryption and decryption, cannot be used for digital signatures.</td> <td data-bbox="940 1012 1365 1167">Can be used for encryption and decryption as well as for digital signatures.</td> </tr> <tr> <td data-bbox="237 1167 548 1323">Efficiency in usage</td> <td data-bbox="548 1167 940 1323">Symmetric key cryptography is often used for long messages.</td> <td data-bbox="940 1167 1365 1323">Asymmetric key cryptography is more efficient for short messages.</td> </tr> </tbody> </table>	Categories	Symmetric Cryptography	Asymmetric Cryptography	Key used for encryption /decryption	Same key is used for encryption & decryption.	One key is used for encryption & another different key is used for decryption.	Key process	Ke=Kd (Same)	Ke# Kd (not same)	Speed of encryption decryption	Very fast	Slower	Size of resulting encrypted text	Usually same as or less than the original clear text size.	More than the original clear text size.	Key agreement/exchange	A big problem	No problem at all.	Usage	Mainly used for encryption and decryption, cannot be used for digital signatures.	Can be used for encryption and decryption as well as for digital signatures.	Efficiency in usage	Symmetric key cryptography is often used for long messages.	Asymmetric key cryptography is more efficient for short messages.	(Any 4 differences: 1 mark each)
Categories	Symmetric Cryptography	Asymmetric Cryptography																								
Key used for encryption /decryption	Same key is used for encryption & decryption.	One key is used for encryption & another different key is used for decryption.																								
Key process	Ke=Kd (Same)	Ke# Kd (not same)																								
Speed of encryption decryption	Very fast	Slower																								
Size of resulting encrypted text	Usually same as or less than the original clear text size.	More than the original clear text size.																								
Key agreement/exchange	A big problem	No problem at all.																								
Usage	Mainly used for encryption and decryption, cannot be used for digital signatures.	Can be used for encryption and decryption as well as for digital signatures.																								
Efficiency in usage	Symmetric key cryptography is often used for long messages.	Asymmetric key cryptography is more efficient for short messages.																								
(d)	Describe in brief Cyber Crime. List different types of Cyber Crime.	4M																								
Ans:	<p>Cyber Crimes: Cyber Crime is an activity done using computers and internet. It is an unlawful act wherein the computer is either a tool or target or both.</p> <p>Categories of cyber Crime:</p> <p>Cyber Crime is categorized in two ways.</p> <ol style="list-style-type: none"> 1. The computer as a target: - using a computer to attacks other computer, e.g. Hacking, virus/worms attacks, Dos attack etc. 2. The computer as a weapon: - using a computer to commit real world crime e.g. cyber terrorism, credit card fraud and pornography etc. <p>Types of cyber crime</p> <ol style="list-style-type: none"> 1) Hacking 2) Cracking 	(Description: 2 marks, List (Any 4): 2 marks)																								



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

- 3) Viruses and worms
- 4) Child pornography
- 5) Cyber terrorism
- 6) Software piracy
- 7) Intellectual property
- 8) Mail bombs
- 9) Bug exploits

(B) Attempt any ONE :

1x6 = 6

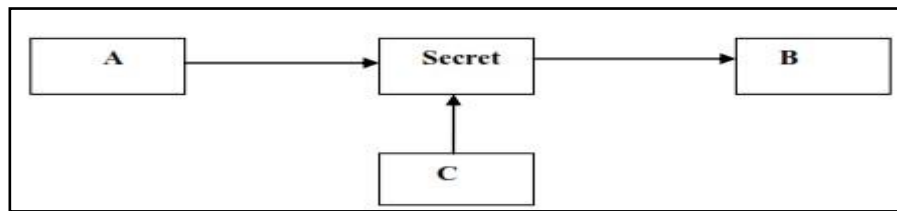
(a) Explain the three pillars of information security. Describe with neat diagram.

6M

Ans: The three Pillars of Information security are

1) Confidentiality:

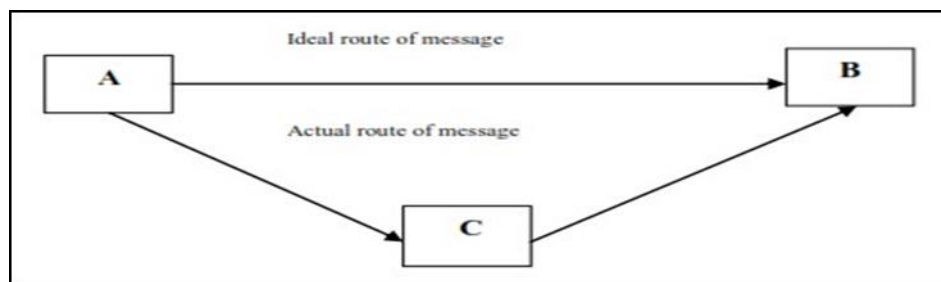
It is used as an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many ways such as through the intentional release of private company information or through a misapplication of networks right.



2) Integrity:

The concept of integrity ensures that

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



3) Availability:

The concept of availability ensures the reliable and timely access to data or computing

(Explanation : 1 mark each, Diagram: 1 mark each)

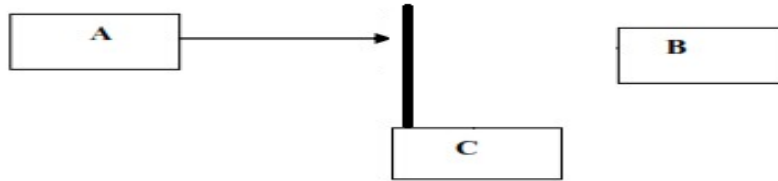
SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

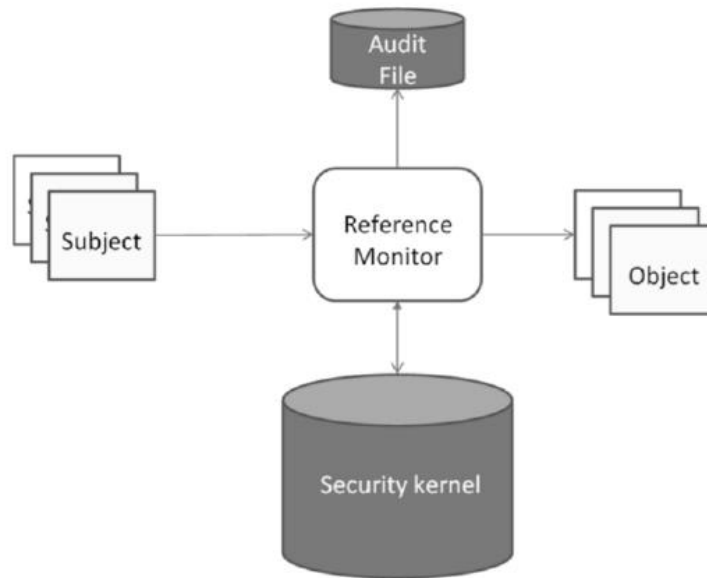
resources by the appropriate person. Availability guarantees that the systems are up and running when they are needed. In addition, this concept guarantees that the security services needed by the security practitioner are in working order.



(b) Explain the concept of Trusted Computing Base.

6M

Ans:



**(Diagram: 2 marks,
Explanation: 4 marks)**

Fig: Trusted Computing Base

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.

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 objects by subjects. The reference monitor has three properties:

- Cannot be bypassed and controls all access.
- Cannot be altered and is protected from modification or change
- 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.



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: **17518**

2.		Attempt any TWO :	2x8 = 16
	(a)	Define security. Describe different types of securities in organization	8M
	Ans:	<p>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)</p> <p>A successful organization should have the following multiple layers of security in place to protect its operations:</p> <ol style="list-style-type: none">1. Physical security, to protect physical items, objects, or areas from unauthorized access and misuse2. Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations3. Operations security, to protect the details of a particular operation or series of activities4. Communications security, to protect communications media, technology, and content5. Network security, to protect networking components, connections, and contents6. Information security: To protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.	(Definition: 2 marks, List: 2 marks, Description of any 4: 1 mark each)
	(b)	State the substitution cipher. List the substitution cipher techniques and explain any two.	8M
	Ans:	<p>{ **Note: Any other substitution cipher shall be considered }</p> <p>In cryptography, a substitution cipher is a method of encrypting by which units of plaintext are replaced with cipher text, according to a fixed system; the "units" may be single letters, pairs of letters, and triplets of letters, mixtures of the above, and so forth.</p> <ol style="list-style-type: none">1. Caesar cipher2. Monoalphabetic ciphers3. Polyalphabetic ciphers <p>1. 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.</p>	(State: 1 mark, List (any 2): 1 mark, Explanation(any 2): 3 marks each)



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Example:

Plain text: INFORMATION

Convert each alphabet in the plain text, using the table, the cipher text can be written as

Cipher text: LQIRUPDWLRQ

2. 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:

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

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

Example:

Plain text: INFORMATION

Convert each alphabet in the plain text, using the table, the cipher text can be written as

Cipher text: UFGJDQZUGF



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

3. Polyalphabetic Cipher: In Polygram Substitution cipher instead of replacing one plain text alphabet with one cipher text alphabet at a time, a block of alphabets is 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.

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

Example:

Plain text: Information

Key: abc

Encrypted text: "iohosoaukoo"

(c) List and explain different data Recovery tools.

8M

Ans: Following are the data recovery tools:

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

1. NTFS Data Recovery Tools: NTFS Recovery is a fully automatic utility that recovers data from damaged or formatted disks. It is designed with a home user in mind. You don't need to have any special knowledge in disk recovery.

(List: 2 marks, Explanation of each: 1 ½ marks)



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

Example: - Diskinternals' NTFS Data Recovery tool. The tool supports

- i. A disk volume containing valuable info was damaged due to a system malfunction
- ii. A disk volume was damaged due by a dangerous virus
- iii. Windows cannot access a disk drive
- iv. Disk was damaged
- v. You have mistakenly formatted a disk volume
- vi. Files or folders are not readable
- vii. Corrupt or damaged partition table

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

Example: - Diskinternals' FAT Data Recovery tool. Works for all:

Formatted drive (to NTFS, to/from FAT32/FAT16)

- i. Inaccessible drive
- ii. Drive not booting
- iii. Missing or deleted file or directory
- iv. Corrupt or damaged partition table.
- v. Damaged Dynamic Disks

FAT Recovery is fully wizard-based, meaning there is no technical knowledge needed. Any person can recover data from damaged or formatted disks on their own, without hiring a technician. FAT Recovery does not write anything to the damaged disk, therefore you can try the program without any risk of losing data you want to be recovered. It does not matter whether Windows recognizes a disk or not, nor does it matter if all directory information is missing – all recoverable data will be recovered and the original disk structure will be restored. Because the program scans every single sector, it never —overlooks or misses recoverable data. Another important advantage of FAT Recovery is its capability to recover data from virtual disks, and it does not matter if the data was deleted prior to recovery or not. FAT Recovery supports the following file systems - FAT12, FAT16, FAT32, and VFAT. Files up to 64 KB are recovered by FAT Recovery.

3. Digital Camera Data recovery tool Digital camera data recovery has the leading photo recovery software for memory card used by digital camera or phone. It can effectively recover lost, deleted, corrupted or formatted photos and video files from various memory cards. It supports almost all memory card types including SD Card, Micro SD, SDHC, and CF (Compact Flash) Card, Picture Card, Memory Stick and more.

Example: - Diskinternals' Digital Camera Data Recovery tool.

Features :

- i. Recover deleted photos from memory cards
- ii. Recover lost photos from memory cards



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518


- iii. Recover lost movies from memory cards
- iv. Recover photos from formatted memory cards
- v. Recover photos from damaged, unreadable or defective memory cards
- vi. Recover pictures from removable storage including flash drives
- vii. Recover images, video files from mobile phones

4. Removable media data recovery tool: The process of recovery is a very straightforward one - insert disk, press "Recover" and get the files you need. The software is easy to use and does not require any additional skills. We tried to make working with it as comfortable as possible. The program starts working automatically and doesn't require the additional set up change. Comfortable Recovery Wizard will do everything for you. The result of the Wizard work is the list of all the recoverable files. All you have to do is to choose the necessary files and press a "Recover" button! The innovation scanning technology economizes greatly your time that otherwise would be spent on a damaged disc recovery.

The advanced users can use a manual recovering. In this case you can work individually with each session\track and chose the file system depending on session.

Example:-

- i. CardRecovery
- ii. PhotoRec
- iii. Recover My Files
- iv. Recuva

3.	Attempt any FOUR of the following:	4x4 = 16
(a)	<p>With respect to information security define following term:</p> <ul style="list-style-type: none"> (i) Security policy (ii) Standards (iii) Guideliness 	4M
Ans:		(Diagram: 1 mark, Definition: 1 mark each)



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

i) Security policy: An information security policy consists of **high 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.
- Policies are of following types:
 - Senior Management Policy
 - Regulatory Policy
 - Advisory Policy
 - Informative Policy

ii) Standards:

- Standards consist of specific low level mandatory controls that help enforce and support the information security policy.
- Standards help to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or software.
- For e.g. a password standard may set out rules for password complexity and a Windows standard may set out the rules for hardening Windows Clients.

iii) Guidelines:

- Guidelines consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.
- Guidelines should be viewed as best practices that are not usually requirements, but are strongly recommended.
- For example, a standard may require passwords to be 8 characters or more and a supporting guideline may state that it is best practice to also ensure the password expires after 30 days

(b) What is information? Explain Data Obfuscation.

4M

Ans:

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

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

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

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

Data Obfuscation:

1) It involves protection of sensitive information with techniques other than encryption.

**(Definition:
1mark,
Explanation:
3 marks)**



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

- 2) Data Obfuscation is one of the solutions for data theft.
- 3) Protecting credit card numbers, medical data and other sensitive information has become more important.
- 4) It is important to keep in mind that encryption refers to some method of modifying data so that they are meaningless and unreadable in their encrypted form. They also must be reasonably secure that is they must not be easily decrypted without the proper key. Anything less than that will be referred as obfuscation.
- 5) Data obfuscation makes the data unusable by some means, but are not considered as a serious form of encryption.
- 6) A good example would be an audit report on a medical system. This report may be generated for an external auditor and contains sensitive information.
- 7) The auditor will be examining the report for information that indicated possible cases of fraud or abuse.
- 8) Assume that the management has required that patient names, permanent account number (PAN) and other personal information (PI) should not be available to the auditor except on an as needed basis.
- 9) The data need to be presented to auditor but in a way that allows the examination of all data, so that only patterns in the data may be detected.
- 10) When the auditor finds a possible case of abuse, he will need the real name and PAN of the party involved. He could obtain this by calling a customer service representative at the insurance company that supplied the report and ask for the real information.
- 11) The obfuscated data re read to the customer service representative, who then inputs it into an application that supplies the real data.
- 12) To summarize, data obfuscation, it would not be very difficult to decipher the obfuscation scheme given enough data.

(c) State the importance of information classification. State the criteria for information classification.

4M

Ans: Importance of Information Classification:

1. The main reason for classifying is that not all data/information have the same level of importance or same level of relevance/ criticality to an organization.
2. Some data are more valuable to the people who make strategic decisions (senior management) because they aid them in making long-range or short range business

(Importance : 2 marks, Criteria: 2 marks)



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

direction decisions.

3. Some data such as trade secrets, formulae (used by scientific and/or research organizations) and new product information (such as the one used by the marketing staff and sales force) are so valuable that their loss could create a significant problem for the enterprise in the market.
4. Thus it is obvious that information classification provides a higher, enterprise-level benefit.
5. Classification of information is used to prevent the unauthorized disclosure and the resultant failure of confidentiality

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.

(d) Consider a plain text message 'I AM A HACKER'. Encrypt it with the help of Caesar's Cipher technique with steps. 4M

Ans: Caesar Cipher: It is proposed by Julius Caesar. In cryptography Caesar cipher also known as Caesar's cipher/code, shift cipher/code. It is one of the simplest and most widely known encryption techniques. It is a type of substitution technique in which each letter in the plain text is replaced by a letter some fixed number of position down the alphabet. For example, with a shift of 3, A would be replaced by D, B would became E, and so on as shown in the table below.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

		Given Plain text: "I AM A HACKER" Convert each alphabet in the plain text, using the table, the cipher text can be written as Cipher text: "L DQ D KDFNIU"	
	(e)	Define the following terms : (1) Hacking (2) Bug Exploits (3) Mail Bomb (4) Intellectual Property	4M
	Ans:	1) HACKING: Hacking in simple terms means an illegal intrusion into a computer system and/or network. Government websites are the hot target of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage. 2) Bug exploits: Application Software exploit are those that take advantage of weaknesses of particular application programs, such weaknesses are called as Bugs. 3) Mail Bombs: It refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing. 4) Intellectual Property: Intellectual property (IP) refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.	(Define: 1 mark each)
4.	(A)	Attempt any THREE :	3x4 = 12
	(a)	Explain Reference model with neat diagram.	4M
	Ans:	{ **Note: Instead of Reference model, Reference Monitor to be considered** }	(Diagram: 2 marks, Explanation: 2 marks)
		<pre> graph TD Subject[Subject] --> RM[Reference Monitor] RM --> Object[Object] RM <--> SK[Security kernel] RM --> AF[Audit File] </pre>	



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

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

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 objects by subjects. This is as shown in the figure.

The reference monitor has three properties:

- Cannot be bypassed and controls all access.
- Cannot be altered and is protected from modification or change
- 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.

(b) Describe various physical Access threats

4M

Ans: Physical Access Threats:

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

(Any 4: 1 mark each)

(c) Explain TCSEC in detail.

4M

Ans: Trusted Computer System Evaluation Criteria (TCSEC):

- Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defence (DOD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system.
- This evaluation criterion is published in a book with an orange cover, which is called appropriately the Orange Book
- The TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information.
- TCSEC provides a graded classification of systems that is divided into hierarchical divisions of security levels:

(Explanation : 2 marks, Divisions: 2 marks)



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

The TCSEC defines four divisions:

- 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.

D — Minimal protection

Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division

C — Discretionary protection

C1 — Discretionary Security Protection

C2 — Controlled Access Protection

B — Mandatory protection

B1 — Labelled Security Protection

B2 — Structured Protection

B3 — Security Domains

A — Verified protection

A1 — Verified Design

(d) Consider a plain text message “Hi How Are You”. Encrypt it with the help of Rail Fence Technique.

4M

Ans: { **Note: Alphabets should not be considered as Case sensitive}

Rail Fence Technique: It is one of the easiest transposition techniques to create cipher text. When plain text message is codified using any suitable scheme, the resulting message is called Cipher text or Cipher.

Steps are: Plain text = **Hi How Are You**

Step 1: Write down Plain text as sequence of diagonal.

Read Plain text written in Step 1 as sequence of rows. As,

H		H		w		r		Y		u
	i		o		A		e		o	

(Procedure: 2 marks, Correct Cipher text: 2 marks)



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: **17518**

Then concatenate these two sequences of text as one to create following

Cipher Text: **HHwrYuioAeo**

OR

The rail-fence cipher is inscribed by zigzag pattern and extracted by rows.

H				w				Y		
	i		o		A		e		o	
		H				r				u

Cipher Text: **HwYioAeoHru**

(B) Attempt any ONE :

1x6 = 6

(a) Describe the term Digital Signature with its working.

6M

Ans: Digital Signatures:

- Digital signature is a strong method of authentication in an electronic form.
 - It includes message authentication code (MAC), hash value of a message and digital pen pad devices. It also includes cryptographically based signature protocols.
 - Digital Signature is used for authentication of the message and the sender to verify the integrity of the message.
 - Digital Signature may be in the form of text, symbol, image or audio.
 - In today's world of electronic transaction, digital signature plays a major role in authentication. For example, one can fill his income tax return online using his digital signature, which avoids the use of paper and makes the process faster.
 - Asymmetric key encryption techniques and public key infrastructure are used in digital signature.
 - Digital signature algorithms are divided into two parts-
 - Signing part: It allows the sender to create his digital signature.
 - Verification part: It is used by the receiver for verifying the signature after receiving the message.
- Generation and Verification of digital signatures:

(Description: 2 marks, Diagram: 2 marks, Working: 2 marks)

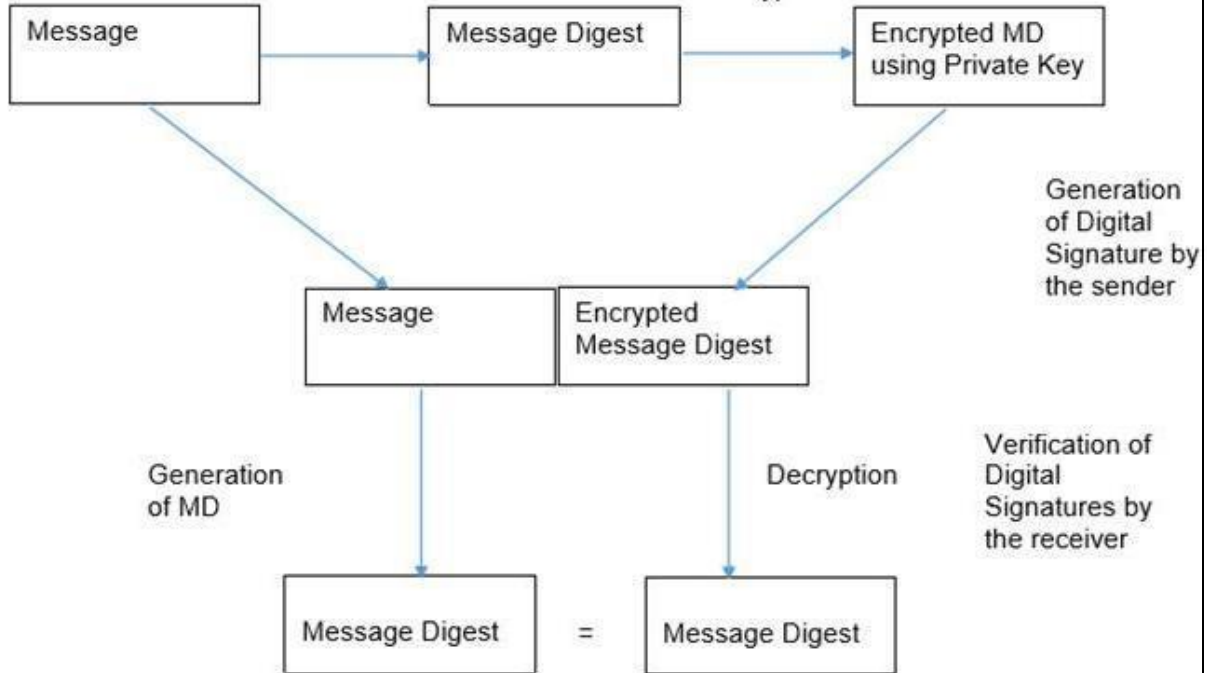


SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518



Working:

1. Message digest is used to generate the signature. The message digest (MD) is calculated from the plaintext or message.
2. The message digest is encrypted using user's private key.
3. Then, the sender sends this encrypted message digest with the plaintext or message to the receiver.
4. The receiver calculates the message digest from the plain text or message he received.
5. Receiver decrypts the encrypted message digest using the sender's public key. If both the MDs are not same then the plaintext or message is modified after signing.

(b) Describe play Fair Cipher with example Step by Step.

6M

Ans: Play Fair Cipher:

a) Preparing plain text:

1. To prepare plain text write all letters of plain text in lowercase, in pairs without punctuation.
2. In plain text if j is present, all j's are replaced with i's.
3. In plain text if double letters occur in a pair, divide them by X or a Z

4. If there are an odd number of letters in plain text, an extra letter is chosen and it is added at the end.

b) Preparing a key matrix:

1. A key matrix is a five-by-five matrix of letters constructed using a keyword.
2. The key phrase is first written without repeating any letters. The remaining letters of the



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

alphabet are filled in the alphabetic order.

c) Encryption process:

The plain text is encrypted two letters at a time using the following steps:

1. Each letter in a pair that is on the same row is replaced by the letter to the right.
2. Letters in the same column are replaced by the next letter below in the same column.
3. When the letters are neither in the same row nor in the same column, then the substitution based upon their intersection. Start with the first letter and move across until it is lined up with the second letter. Then start with the second, and move up or down until it is lined up with the first. Perform the transformation for each pair of letters in the modified plain text and remove the spaces.

Example:

Plaintext: We live in a world full of beauty.

Keyword: Another

Step 1: Preparing plain text

The plain text matrix is:

we	li	ve	in	aw
or	ld	fu	lx	lo
fb	ea	ut	yz	

Step 2: Preparing key matrix

The key matrix is:

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

Step 3: Encryption

By following the above rules for encryption of plain text the cipher text is:

VRFKAFGONVNBULLMIZIHIEFESHZY

5. Attempt any TWO :

2x 8 = 16

(a) How do you recover the data in below situations?

- (1) Deleted file Recovery
- (2) Formated partition Recovery

8M



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

<p>Ans:</p>	<p>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.</p> <p>(1) Deleted file recovery:</p> <ul style="list-style-type: none">• 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 you 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 1s and 0s. 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 be performed under the requirement of no new files are written to occupy previous space of lost file. In same way, if anyone performs disk defragmentation, the file may be over-written. In defragmentation, the utility copies files in closer sectors and tracks. This will help the computer to access a file quickly and it improves systems speed. Thus, it also involves a lot of over-writing on available space (where your deleted files may be).• 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	<p>(Deleted file Recovery: 4 marks, Formatted partition Recovery: 4 marks)</p>
--------------------	---	---



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

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.

(2) Formatted Partition Recovery:

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

(b)	Describe COBIT framework	8M
Ans:	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.	(Diagram: 2 marks, Explanation: 4 marks, Services: 2 marks)

SUMMER- 18 EXAMINATION
Model Answer

Subject Name: Information Security

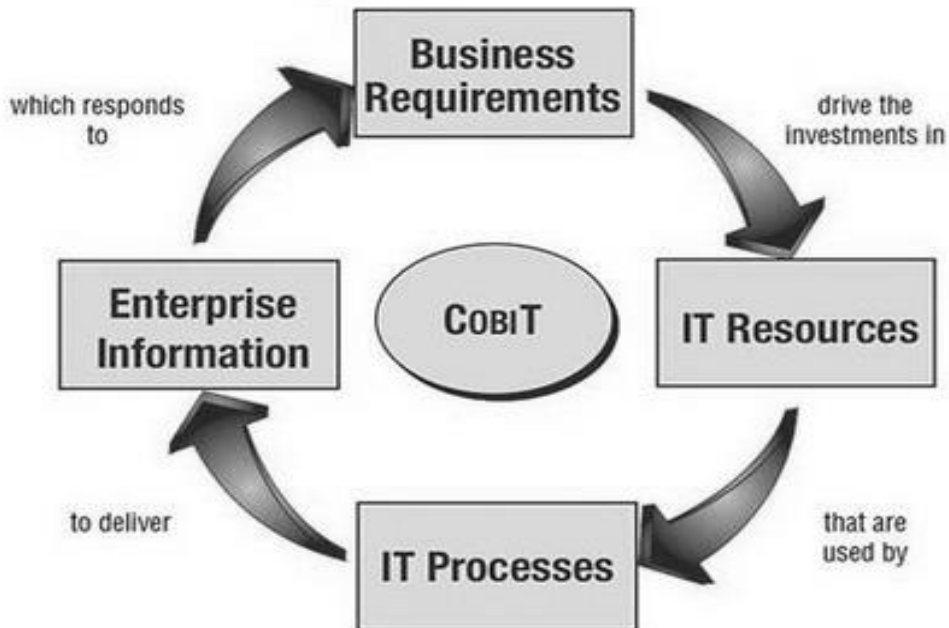
Subject Code: 17518

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
- 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.



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

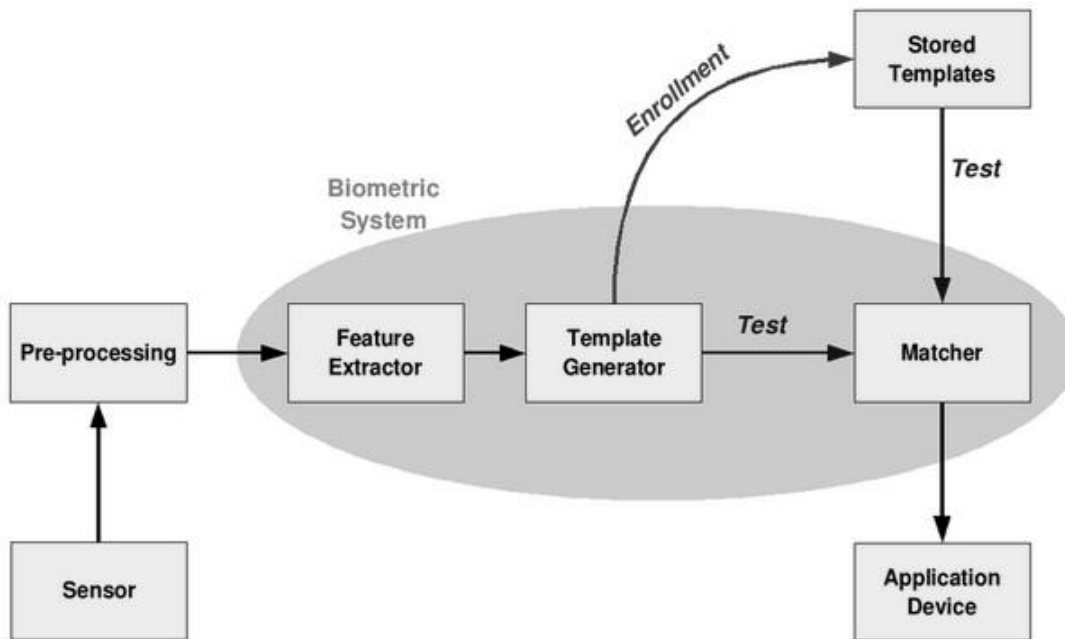
- Services provided by the COBIT:**
1. Manage operations
 2. Manage service request and incidence
 3. Manage problems
 4. Manage continuity
 5. Manage security services
 6. Manage business process control

(c) Describe Biometric system. Describe the classification of Biometric characteristics.

8M

Ans: Biometrics refers to metrics related to human characteristics and traits. Biometrics authentication is used in computer science as a form of identification and access control.

**(Diagram: 2 marks,
Explanation: 4 marks,
Characteristics: 2 marks)**



1. The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database.
2. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison.



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

3. Second, in identification mode the system performs a one-to-many comparison against biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

4. The first time an individual uses a biometric system is called enrolment. During the enrolment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrolment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust.

5. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way.

6. During the enrolment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyse the template with the input.

Biometric characteristics can be divided in to classes

1. Physiological Characteristics:

The physiological characteristics are based on the direct measurement of parts of human body such as iris, fingerprint, shape, and position of fingers, etc.

There are some physical traits which remain unaltered throughout a person's life. They can be an excellent resource for identification of an individual.

For example :

- Fingerprint Recognition
- Hand Geometry Recognition system
- Facial Recognition System
- Iris Recognition System
- Hand Geometry Recognition System
- Retinal Scanning System
- DNA Recognition System



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

2. Behavioral Characteristics: Behavioral biometrics pertains to the behavior exhibited by people or the manner in which people perform tasks such as walking, signing, and typing on the keyboard.

Behavioral biometrics characteristics have higher variations as they primarily depend on the external factors such as fatigue, mood, etc. This causes higher FAR and FRR as compared to solutions based on a physiological biometrics.

For example :

- Gait (the way one walks)
- Rhythm of typing keys
- Signature
- Voice

6. **Attempt any FOUR :** **4x4 = 16**

(a) **Describe IT Act, 2008** **4M**

Ans: IT act 2008: **(Correct Answer: 4 marks)**

- 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 ecommerce, 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



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

	<p>January 1997 has adopted the model law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.</p> <ul style="list-style-type: none">• This recommends that all States give favourable 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.	
(b)	Explain working of SSO	4M
Ans:	<p>SSO-Single sign-on is the ability for a user to enter the same Id and Password to Log on to multiple applications with an enterprise.</p> <ul style="list-style-type: none">• Once logged in user can switch from one system to the next without logging in again.• It can work between enterprises using federated authentication. <p>For example: A business partner employee may successfully log on to their enterprise system.</p> <p>The basic process of SSO is as follows:</p> <ul style="list-style-type: none">• The first step is logging into the main service (Facebook or Google, for instance).• When you visit a new service, it redirects you to the original (or parent) service to check if you are logged in at that one.• An OTP (One-time password) token is returned.• The OTP token is then verified by the new service from the parent's servers, and only after successful verification is the user granted entry. <p>A good example of the use of SSO is in Google's services. You need only be signed in to one primary Google account to access different services like YouTube, Gmail, Google+, Google Analytics, and more.</p> <p>Authenticating to the Login Server in Single Sign On:</p> <ol style="list-style-type: none">1. The Login Server checks for a login cookie. If one is present, the Login Server identifies the user from the encrypted information in the login cookie.2. If a login cookie is not present, the Login Server prompts the user for the user's credentials.3. The user provides the user name and password.4. The Login Server authenticates the user by passing the provided name and password to	(Correct Answer: 4 marks)

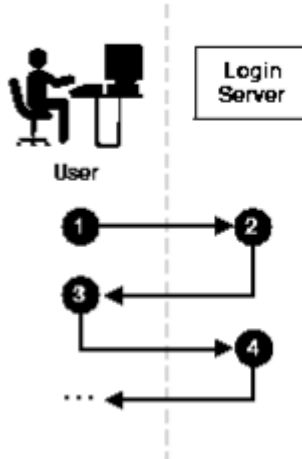
SUMMER– 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

the configured authentication routine-either the local routine or one provided by an external authentication module for an external repository. If the authentication is successful, the Login Server establishes a login cookie on the client browser to facilitate Single Sign-On for future authentication requests.



(c) Explain BIBA model for integrity.

4M

Ans:

- The major drawback of the BLP model was that it only considered the confidentiality of data. Consideration is not given to —need to know principle. Data is freely available to user to read data to its own level and lower level.
- The BIBA model addresses the problem with the star property of the Bell-LaPadula model, which does not restrict a subject from writing to a more trusted object.
- Hence ken BIBA developed a model in 1977 that considered data integrity. It focuses on commercial sector where, data integrity is more important than confidentiality.
- Integrity is the protection of system data from intentional or accidental unauthorized changes.
- Although the security program cannot improve the accuracy of data, it can help to ensure that any changes are intended and correctly applied.
- Additional element of integrity is the need to protect the process and program used to manipulate the data from unauthorized modification.

The BIBA model has following three properties:

1. Simple Integrity Property (No Read-Down): - Data can be read from higher integrity level.

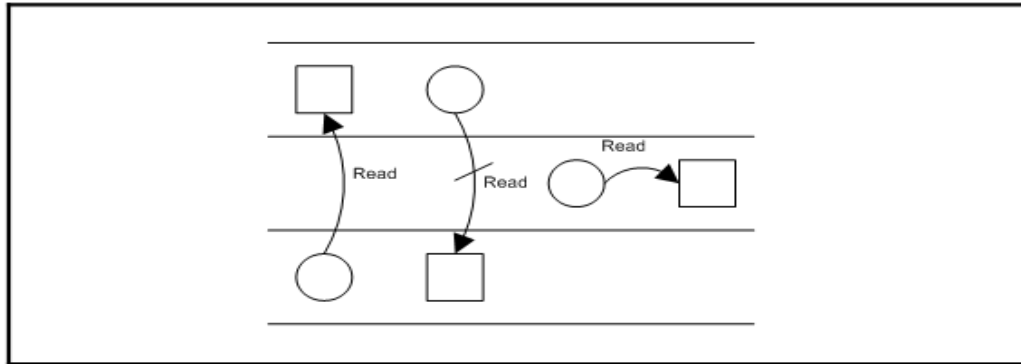
(Correct Answer: 4 marks)

SUMMER- 18 EXAMINATION

Subject Name: Information Security

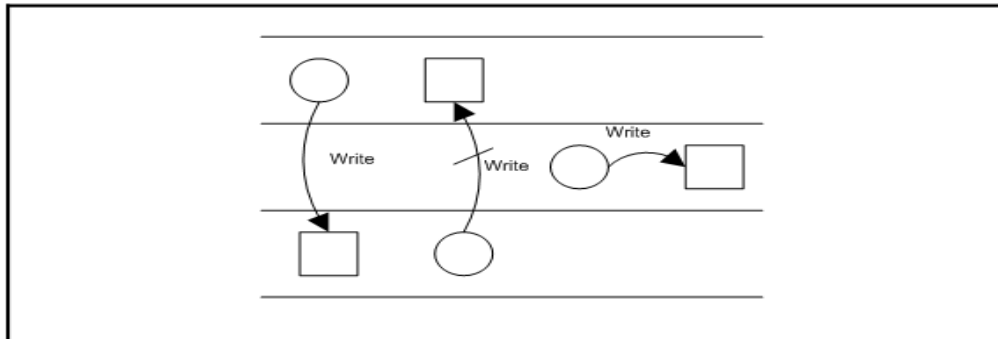
Model Answer

Subject Code: 17518



circle = subject, square = object

2. Star Integrity property: - Data can be written to lower integrity level.



circle = subject, square = object

3. Invocation Property: - User cannot request services from higher integrity level.

Thus, BIBA is RUWD model (Read up, write down).

(d) Describe ITSEC with its classes.

4M

Ans: ITSEC(Information Technology Security Evaluation Criteria) with its target evaluation levels :

ITSEC is developed by European country for security equation criteria.

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

(Description
2 marks;
Classes: 2
marks)



SUMMER– 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: **17518**

iv. Level for evaluating targets –functional as well as evaluation (F- xx and E – yy)

ITSEC classes contain non- hierarchical structure which are specialized classes are as given below. (F- xx)

- F-IN for high integrity.
- F-AV for high availability.
- F-DI for high data integrity.
- F-DX for networks that require high demands for confidentiality and integrity during data exchanges.

ITSEC uses following evaluation (Assurance) classes from E0 toE6 to evaluate the security.

E0 – Minimal protection, levels which fail to meet E1 requirements.

E1 – Security target and informal architecture design containing informal description must be produced.

E2 – E1 requirements plus an informal detailed design and test document must be produced.

E3 – E2 requirements plus source code or hardware drawing to be produced. Correspondence must be shown between source codes of detailed design.

E4 – E3 requirements plus formal model of Security and Semi – formal specification of Security function architecture and detailed design to be produced.

E5 – E4 requirements plus architecture design to explain the inter relationship between security component.

E6 – E5 requirements plus formal description of architecture and Security function to be produced in addition to consistency with the formal security model.

(e) Explain HILL cipher technique with example for 2 x 2 matrix.

4M

Ans: Hill Cipher was invented by Lester S. Hill in 1929, and like other Biographic Cipher it act on group of letters. It work on digraphs, tri-graphs or theoretically any sized blocks.

Encryption:

- To encrypt a message using the Hill Cipher we must first turn our keyword into a key matrix (2*2) for working with digraphs.
- We also turn plaintext into digraphs and each of these into column vector.
- We then perform matrix multiplication modulo the length of the alphabet (i. e.26) on each vector. These vectors are then converted back in to letters to produce the cipher

(4 marks for example with Steps) Or any other suitable example can be considered)



text.

Decrypt:

To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

For Example:

Consider Plain text=COMP

And key=HILL

1. Turn the keyword into matrix

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

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

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

3. Now split the plain text and write this as a column vectors.

$$\begin{pmatrix} C \\ O \end{pmatrix} \quad \begin{pmatrix} M \\ P \end{pmatrix}$$

4. Next step to convert the plain text column vectors in a same way that we converted the keyword in to the key matrix. Each letter is replaced by appropriate number.

$$\begin{pmatrix} 2 \\ 14 \end{pmatrix} \quad \begin{pmatrix} 12 \\ 15 \end{pmatrix}$$

5. Now perform matrix multiplication write key matrix with first column vector.

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 2 \\ 14 \end{pmatrix} = \begin{pmatrix} 126 \\ 176 \end{pmatrix}$$

Matrix multiplication will be,

$$(7 \times 2) + (8 \times 14) = 14 + 112 = 126$$

$$(11 \times 2) + (11 \times 14) = 22 + 154 = 176$$



SUMMER- 18 EXAMINATION

Subject Name: Information Security

Model Answer

Subject Code: 17518

6. Same procedure is followed to remaining plain text.

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

Matrix multiplication will be,

$$(7 \times 12) + (8 \times 15) = 84 + 120 = 204$$

$$(11 \times 12) + (11 \times 15) = 132 + 165 = 297$$

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

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

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

8. Now, Convert 22 and 20 into letters "W" and "U" respectively.

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

Same procedure is for remaining plain text.

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

Hence, the plaintext "COMP" and keyword "HILL" then the Cipher text is "WUWL"