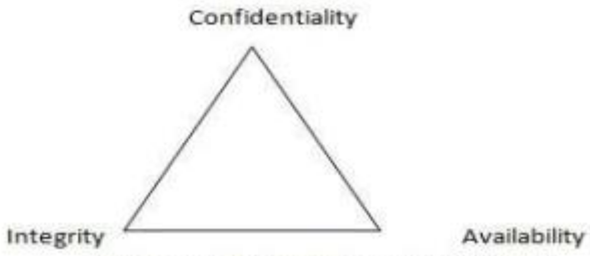
WINTER– 1

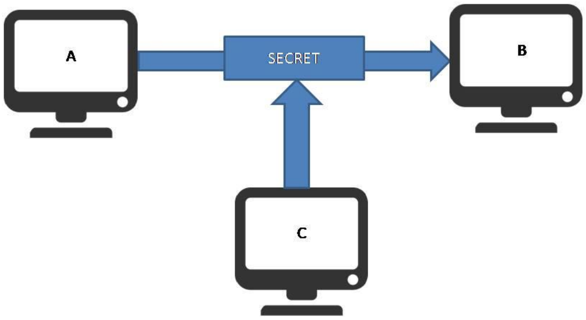
Subject Name: Information Security **Model Answer** Subject Code: 17518

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.	Answer	Marking Scheme
1	A	**Attempt any THREE**	**12**
	a	**List pillars of information security and explain any one with neat sketch.**	4M
	Ans	Three pillars of information security: 1. Confidentiality 2. Integrity 3. Availability  Fig: Three pillars of Information Security **1. Confidentiality:** It is used as an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many ways	List 1M; explain any one with diagram 3M

such as through the intentional release of private company information or through a misapplication of networks right.



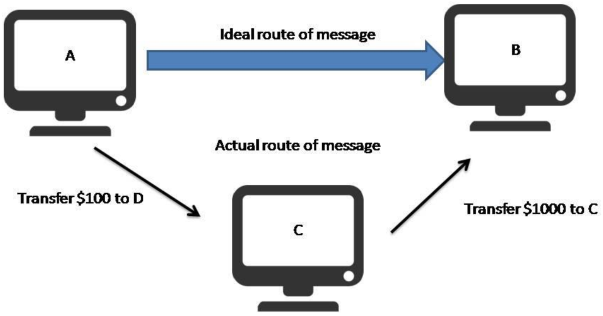
2. Integrity:

The concept of integrity ensures that

i. Modifications are not made to data by unauthorized person or processes.

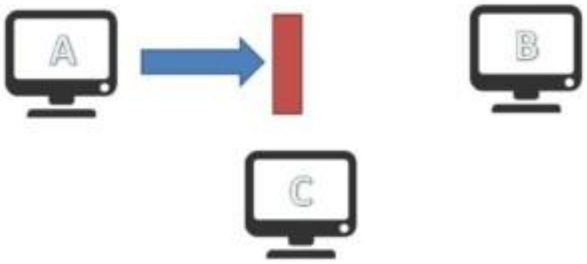
ii. Unauthorized modifications are not made to the data by authorized person or processes.

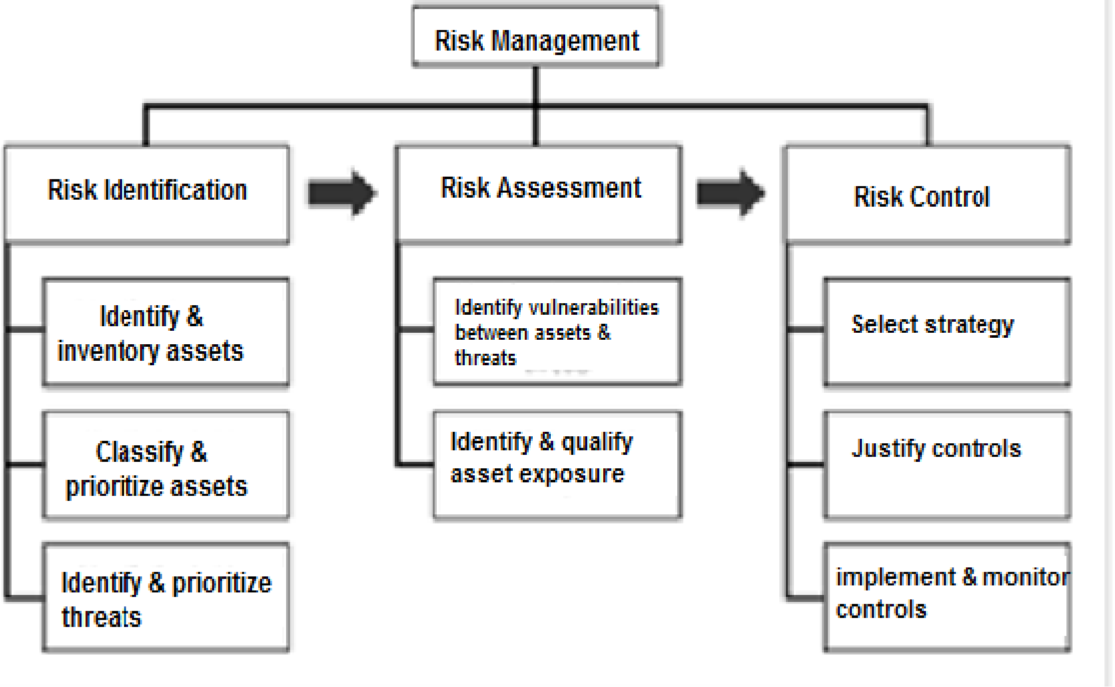
iii. The data is internally and externally consistent.



3. Availability:

The concept of availability ensures the reliable and timely access to data or computing 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.  Attack on Availability	
	b	**Define RISK. Describe how RISK is managed for information Security**	4M
	Ans	**Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) The adverse impacts that would arise if the circumstance or event occurs; and (ii) (ii) The likelihood of occurrence. Or The process of identifying risk, as represented by vulnerabilities, to an organization's information assets and infrastructure, and taking steps to reduce this risk to an acceptable level. Risk management involves three major undertakings: □ Risk identification, □ Risk assessment, □ Risk control.	Define RISK : 1M, Diagram: 1M, Explaination: 2M

		Risk management: This is the process of identifying and controlling risks facing an organization  Risk Management Risk Identification Identify & inventory assets Classify & prioritize assets Identify & prioritize threats Risk Assessment Identify vulnerabilities between assets & threats Identify & qualify asset exposure Risk Control Select strategy Justify controls implement & monitor controls • 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.	
	c	**Define following terms:** **(i)Cryptography** **(ii)Cipher text** **(iii)Encryption** **(iv) Cryptology**	4M
	Ans	**(i) Cryptography** It is the art and science of achieving security by encoding messages to make them non-readable. **(ii) Cipher text** The resultant message after coding a plain text by using some suitable method is known as Cipher Text. **(iii)Encryption** The process of encoding plain text into cipher text message is known as Encryption	1M for each

(iv)Cryptology

It is combination of Cryptography and cryptanalysis.

Or

Cryptology is the art or science comprising the principles and methods of transforming an intelligible message into one that is unintelligible and unintelligible message back to intelligible one.

CRYPTOGRAPHY + CRYPTANALYSIS = CRYPTOLOGY

d **Define following terms:** 4M

(i)Hacking

(ii)Cracking

(iii)Cyber crime

(iv)Data recovery

Ans **(i) Hacking** 1M for each

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.

(ii) Cracking

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

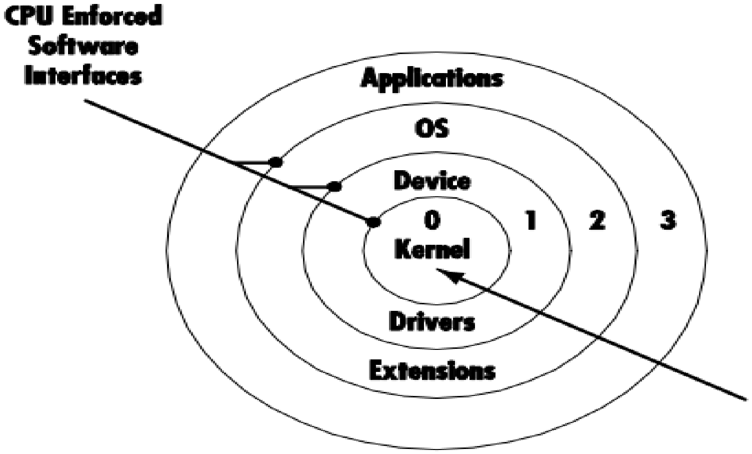
(iii) Cyber crime

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

(iv)Data recovery

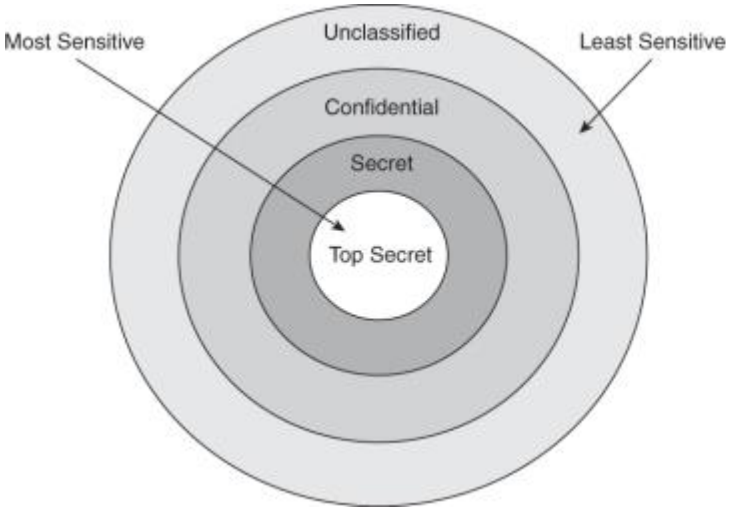
Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible for some reason. When files have been mistakenly deleted and need to be recovered, data recovery is necessary.

	B	**Attempt Any ONE**	**6 M**
	a	**Define information classification. Describe criteria for information classification.**	6M
	Ans	**Information classification:** 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 **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.	Classification 2M, Criteria 4M
	b	**Describe following terms with neat sketch:** **(i) Ring of trust in single system.** **(ii) Ring of trust in networked system.**	6M
	Ans	**(i) Ring of trust in single system**	1M for any one diagram, 2M for explanation



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

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



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

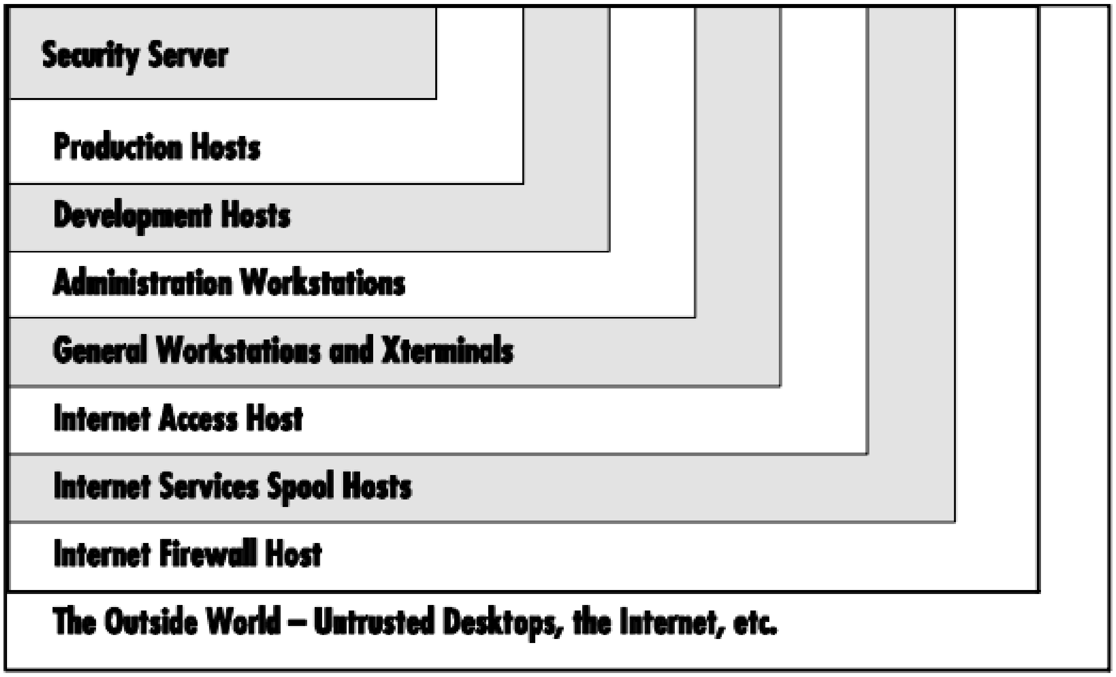
The rings provide much granularity.

The layer number increases and the level of trust decreases.

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

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

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

		Layer 3: At this level applications and procedures operate. Users usually interact with this level. Operations working at this level generally called working in User Mode. **(ii) Ring of trust in networked system**  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. The hosts of networks are divided into rings as per the security ratings of services provided by the host to network. The created ring can be treated as a trust between different host of the network. The hierarchy of the ring can be decided on the basis of Whether the host is in the room or not i.e physically secured or not Whether the hosts are having normal user accounts Whether the host is at remote place or not Whether the host need data from the internet Whether the host provide critical services or not. Whether the large amount of people affected because of downning of the host.	1M for any one diagram, 2M for explanation
2		**Attempt any TWO**	**16**
	a	**Define security. Describe principles of information security with neat sketch.**	8M
	Ans	**Security:** Security is the method which makes the accessibility of information or system more reliable. Security means to protect information or system from unauthorized user like attackers, who do harm to system or to network intentionally or unintentionally. Security is not only to protect information or network, but also allow authorized user to access the system or network. Principles of information security:	Security 2M, 2M each principle with daigram

1. Confidentiality

2. Integrity

3. Availability

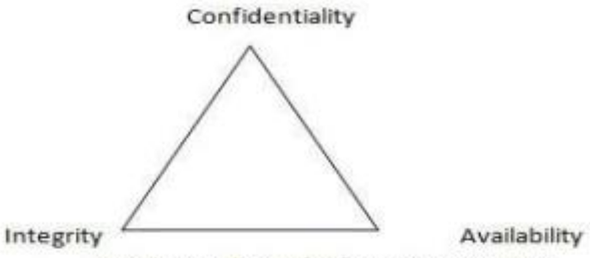
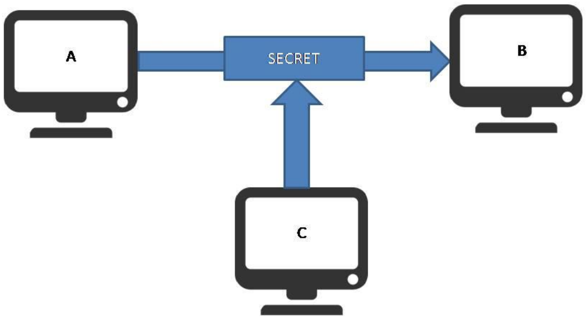


Fig: Three pillars of Information Security

1. **Confidentiality:**

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



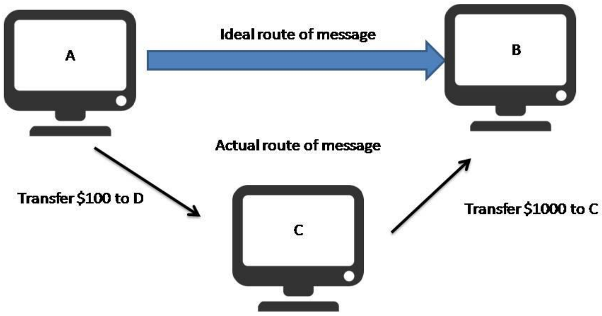
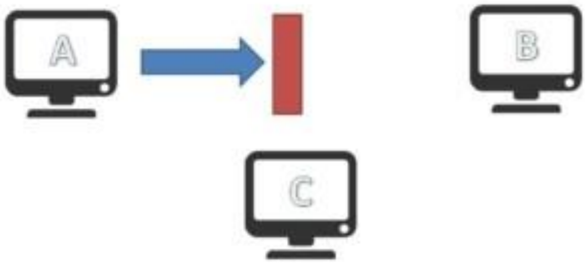
2. **Integrity:**

The concept of integrity ensures that

iv. Modifications are not made to data by unauthorized person or processes.

v. Unauthorized modifications are not made to the data by authorized person or processes.

vi. The data is internally and externally consistent.

		 A B C Ideal route of message Actual route of message Transfer $100 to D Transfer $1000 to C **3. Availability:** The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate person. Availability guarantees that the systems are up and running when they are needed. In addition, this concept guarantees that the security services needed by the security practitioner are in working order.  Attack on Availability	
	b	**Explain different phases in Play fair cipher with suitable example.**	8M
	Ans	**(Note: Any other correct example may also be considered).** The Play fair cipher or Play Fair Square is a manual symmetric encryption technique and was the first literal digraph substitution cipher. It uses group of two letters to generate cipher text. The encryption process is divided into 2 parts. 1. Creation of the matrix: a. Enter the key matrix (Ex Playfair example)in the matrix row-wise left to right and then	Explanation 4M, Example 4M

top to bottom

b. Drop duplicate letters

c. Fill the remaining spaces in the matrix with the rest of the English Alphabets (A – Z) that were not part of the keyword. Combine I & J in the same cell of the table.

d. If I or J is a part of the keyword, disregard both I and J while filling the remaining slots.

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

b) 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.

Eg. Plain text : “I am Rahul”

Key : “Playfair Example”

a. Plain text is broken into groups of two alphabets I AM RAHUL becomes IA MR AH UL.

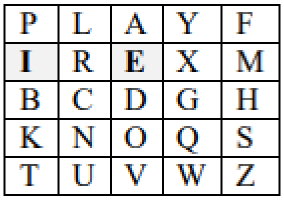
b. Taking each pair the rules are applied for encryption, as given below.

1. IA : From the matrix, since the two alphabets do not appear on the same row and column, replace the text with the diagonally opposite text, EP.

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

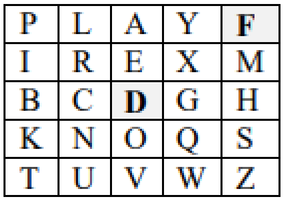
2. MR: Since these two alphabets appear in the same row, replace them with their

immediate right text as, IE. (The right side alphabet is replaced by wrapping around to the left side of row)



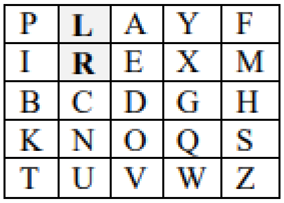
P	L	A	Y	F
I	R	**E**	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

3. AH: From the matrix, since the two alphabets do not appear on the same row and column, replace the text with the diagonally opposite text, FD.



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

4. UL: Since these two alphabets appear in the same column, replace them with their immediately below text as LR. (The bottom side alphabet is replaced by wrapping around to the top side of the row)



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

c **Explain concept of hacking and cracking. Explain different types of Hackers.** 8M

Ans

Cracking: 2M, Hacking : 2M, types of hackers: 4M

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

Example:

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

Hacking:
Every act committed towards breaking into a computer and/or network is hacking and it is an offence. Hackers write or use readymade computer programs to attack the target computer. They possess the desire to destruct and they get enjoyment out of such destruction.

Example:
Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by

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

1. **White Hat:**

   This type of hackers is someone who has no malicious purpose whenever he breaks into security systems. In fact, a large number of white hat hackers are security experts themselves who want to push the boundaries of their own IT security ciphers and shields or event, penetration testers specifically hired to test out how vulnerable or impenetrable (at the time) a present protective setup currently is. A white hat that does vulnerability assessments and penetration tests is also known as an ethical hacker.

2. **Black Hat:**

   This type of hackers is also known as a cracker and he Has a malicious purpose whenever he goes about breaking into computer security systems with the use of technology such as a network, telecommunication system, or computer and without authorization. His malicious purposes can range from all sorts cybercrimes such as piracy, identity theft, credit card fraud, damage, and so forth. He may or may not utilize questionable tactics such as deploying worms and malicious sites to meet his ends.

3. **Grey Hat:**

   A grey hat hacker is a combination of both white hats and black hats. This is the kind of hacker that is not a penetration tester but will go ahead and surf the Internet for vulnerable systems he could exploit. Like a white hat, he will inform the administrator of the website of the vulnerabilities he found after hacking through the site. Like a black hat and unlike a pen tester, he will hack any site freely and without any prompting or authorization from owners what so ever. He will even offer to repair the vulnerable site he exposed in the first place for a small fee.

4. **Elite Hacker:**

   As with any society, better than average people are rewarded for their talent and treated as special. This social status among the hacker underground, the elite are the hackers among hackers in this subculture of sorts. They are the masters of deception that have a solid reputation among their peers as the cream of the hacker crop.

5. **Script Kiddie:**

   A script kiddie is basically an part-time or no expert hacker, who breaks into people's computer systems not through his knowledge in IT security and the ins and outs of given website, but through the pre-packaged automated scripts (hence the name), tools, and software written by people who are real hackers, unlike him. He usually has little to know knowledge of the underlying concept behind how those scripts he has on hand works.

3		**Attempt any FOUR :**	**16 M**
	a	**Describe confidentiality model of Information Security.**	4M
	Ans	Bell-LaPadula model (BLP) : Confidentiality Models □ This model was developed in the 1970s for the US Military by David Bell and Leonard LaPadula of Mitre Corporation. □ is a ***confidentiality model*** intended to preserve the principle of least privilege □ It was developed in response to a single problem –information leakage. E.g The Military using time-sharing mainframe systems. □ This model can specify how security tools are used to achieve the desired level of confidentiality. □ BLP model defines the relationship between objects (files) and subjects (users) □ BLP is a Hierarchical State Machine Model having many layers □ BLP is a formal model of security policy which defines set of rules for access controls like: □ **Dominance Relation:** Users with a particular clearance will only be able to access files of a particular classification and below. □ **Discretionary Security:** specific subjects(users) are granted specific modes of access. □ **Data flows upwards**: BLP enforces the confidentiality aspect of access control in that data can only move up from lower levels of classification to higher □ BLP is also categorized as an Information Flow Model □ BLP was the first model to define 3 fundamental modes of access- read, write and read/write, though users cannot be assigned to more than one access mode. □ BLP has three properties: □ **Simple Security Property**: Users can read data of a lower classification □ **Star Security Property**: Users can write data to an area of higher classification □ **Strong Star (Tranquility) Property**: Users can read and write to own level only. □ BLP is a WURD (Write Up, Read Down)	Explanation 4M

	b	**Describe any four major sources of physical security threats.**	4M
	Ans	• Physical Security Threats: – Weather – Fire and Chemical – Earth Movement – Object Movement (Structural failure) building collapse, falling truck, plane, car – Energy (electricity, magnetism, radio wave etc.) – Organism (Biological): Virus, bacteria, animal etc. – Equipment: Mechanical/electronic component failure – Human: Strike, War, Sabotage etc.	
	c	**List any two integrity & describe clark & Wilson model.**	4M
	Ans	▪ Clark and Wilson Model ● Non-interference Model ● State machine Model ● Access Matrix Model ● Information flow Model **Clark and Wilson model** ❑ This model was published in year 1987 by David Clark and David Wilson builds on BLP and Biba. ❑ It requires mathematical proof that steps are performed in order exactly as they are listed, authenticates the individuals who perform the steps, and defines separation of duties ❑ It addresses all three integrity goals: ○ Preventing unauthorized users from making any modifications ○ Preventing authorized users from making unauthorized	List 2M Explanation 2M

		modifications ○ Maintaining internal and external consistency. A well formed transaction is one that only permits modification of data if that modification meets the three integrity goals listed above.	
	d	**Consider plaintext “PIET “and key “HILL” and convert into cipher text using Hill cipher.**	4M
	Ans	(consider A=0) Selected Hill matrix for encryption: H[t] = [H I] [L L] This matrix encoded to numbers: H[n] = [07 08] [11 11] Encryption of the plaintext: "PI": This plaintext vector P is below encoded to numbers: P[n1] = $\begin{bmatrix} 15 \\ 08 \end{bmatrix}$ Computation of the Hill encryption by the row*column matrix*vector product (the vector P[n] is a column vector): N <-- 13= 07*15 + 08*08 (mod 26) T <-- 15 = 11*15 + 11*08 (mod 26) The Hill cipher text is: "NT". Encryption of the plaintext: "ET": This plaintext vector P is below encoded to numbers: P[n2] = $\begin{bmatrix} 04 \\ 19 \end{bmatrix}$ Computation of the Hill encryption by the row*column matrix*vector product (the vector P[n] is a column vector): Y<-- 24 = 07*04 + 08*19 (mod 26) T<-- 18 = 11*04 + 11*19 (mod 26)	Correct answer : 4 marks . Marks for the correct steps shall be given.

		The Hill ciphertext is: "YT". CIPHER TEXT: NTYT	
	e	**Describe pornography & intellectual property.**	4M
	Ans	**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. **Intellectual property** Intellectual property is any innovation, commercial or artistic; any new method or formula with economic value; or any unique name, symbol, or logo that is used commercially. Intellectual property is protected by patents on inventions; trademarks on branded devices; copyrights on music, videos, patterns, and other forms of expression; and state and federal laws. Stealing intellectual property is cheap and easy. All a thief has to do is copy someone else’s ideas or product. The other person or company—the victim—has done all the work, but thieves can reap huge profits. Intellectual property theft can cost people their jobs, damage the reputation of the original maker of the counterfeited product, cause sickness and bodily harm, deprive governments of desperately needed tax revenue, and even result in the spread of organized crime and gangs—which in turn can damage more lives and destroy neighborhoods.	Each Explanation 2M
4	A	**Attempt any THREE :**	**12 M**
	a	**Describe TCB with neat sketch.**	4M
	Ans	The trusted computing base (TCB) is the sum total of all software and hardware required to enforce security	Diagram: 2 M, Explanation : 2 M

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

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

Reference Monitor.

3. A reference monitor is a separable module that enforces access control decisions

4. All sensitive operations are routed through the reference monitor

5. The monitor then decides if the operation should proceed.

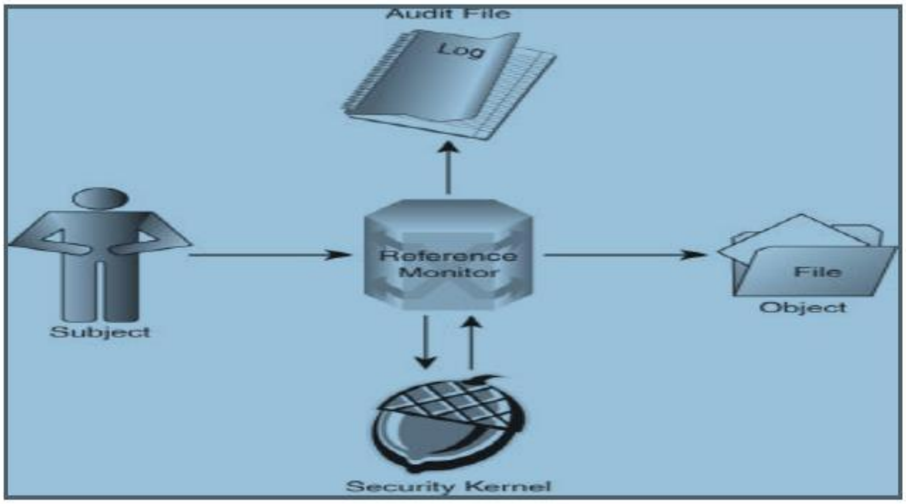


Fig: Reference Monitor

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

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

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

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

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

b **Describe following terms:** 4M

(i)Authorization

(ii)Authentication

(iii)Access

		(iv)Identification	
	Ans	i. Authorization. It is a process of verifying that the known person has the authority to perform certain operation. It cannot occur without authentication. It is nothing but granting permissions and rights to individual so that he can use these rights to access computer resources or information. ii. Authentication. Authentication is the process of determining identity of a user or other entity. It is performed during log on process where user has to submit his/her username and password. There are three methods used in it. 1. Something you know User knows user id and password. 2. Something you have Valid user has lock and key. 3. Something about you User’s unique identity like fingerprints, DNA etc. iii. Access Access, in the context of security, is the privilege or assigned permission to use computer data or resources in some manner. For instance, a user may be allowed read access to a file, but will not be allowed to edit or delete it. Access is also the amount of admittance allowed to any given entity; or, it can simply mean the permission for admittance. Access is important in maintaining security in computer systems. It restricts the use and distribution of information, settings and the general use of a system. iv. Identification Identification uniquely identifies the users of an information system. Identification equates to a user’s offline identity through his or her name, initials, e-mail address or a meaningless string of characters.	Each Explanation 1M
	c	**Explain Biba model for integrity.**	4M
	Ans	Biba integrity model Integrity is the protection of system data from intentional or accidental	Relevant Explanation

		unauthorized changes. • Biba Uses a ***read up, write down [RUWD]*** approach. Subjects cannot read objects of lesser integrity and subjects cannot write to objects of higher integrity. • The major drawback of BLP Model is that users were free to read all data at their own and lower levels of classification. • Hence Ken Biba developed a model that considered data integrity. • Biba model is concerned with preventing data from low integrity environments polluting high integrity data. • The challenge of the security program is to ensure that data is maintained in the state that users expect. • The security program cannot improve the accuracy of data that is put into the system by users, it can help ensure that any changes are intended and correctly applied. • Biba Model has following three properties: **Simple Integrity Property** : Data can be read from a higher integrity level. **Star Integrity Property**: Data can be written to a lower integrity level. **Invocation Property:** User cannot request service(invoke) from a higher integrity level. • In Biba model, the subject with top secret clearance can able to see information that is labelled with top secrets clearance. • Higher clearances will not view information at the lower level of integrity as well as highest level of integrity	4 M
	d	**Describe any four applications of cryptography.**	4M
	Ans	1. **Data Hiding:** The original use of cryptography is to hide something	Each application :

		that has been written. 2. **Digital Code:** Cryptography can also can be applied to software, graphics or voice that is, it can be applied to anything that can be digitally coded. 3. **Electronic payment:** When electronic payments are sent through a network, the biggest risk is that the payment message will alter or bogus messages introduced and the risk that someone reads the messages may be minor significance. 4. **Message Authentication:** One cannot entirely prevent someone from tampering with the network and changing the message, but if this happens it can certainly be detected. This process of checking the integrity of the transmitted message is often called message authentication. The most recent and useful development in the uses of cryptography is the digital signature.	1 M
	B	**Attempt any ONE :**	**6 M**
	a	**Elaborate what is cryptography. Explain integrity and non-repudiation with respect to cryptography.**	6M
	Ans	- **Cryptography** - It is the art and science of achieving security by encoding messages to make them non-readable. Cryptography ensures security of communication over insecure medium. The original use of cryptography is to hide something that has been written. - Cryptography can be applied to software, graphics or voice that is; it can be applied to anything that can be digitally coded. - **Integrity**: - It is the process of assuring the receiver that the received message has not been changed in any way from the original. - In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached. - **Non-repudiation :** - It is the process to prove that the sender has really sent this message and he cannot deny it. - Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.	Cryptogrphy Eplanaxtion 2M Integrity explanation 2M Non repudiation Explanation
	b	**Enlist authentication protocol and describe any two in detail.**	6M

Ans

Enlist 2M each Explanation 2M

List of Authentication Protocol

1. Challenge Handshake Authentication Protocol
2. Extensible Authentication Protocol
3. Password Authentication Protocol
4. Shiva Password Authentication Protocol
5. Data Encryption Standard
6. Remote Authentication Dial-In User Service protocol
7. S/KEY

1) CHAP: It is a Challenge Handshake Authentication Protocol. This

protocol is used by servers to validate the identity of remote client. CHAP verifies the identity by using 3- way handshaking and by using shared secrete.

After establishment of link, the server sends a challenge message to the client.

Then client responds with a value obtained by using a one-way hash function.

Server compares the response i.e. hash value with its own calculated hash value.

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

2) EAP: It is Extensible Authentication Protocol and mainly used for wireless networks and point to point connections. It may support various authentication mechanisms like tokens, certificate, one-time password, smart cards etc. In EAP protocol

- A user requests connection to WLAN through an access point.
- Then the access point requests identification (ID) data from the user and transmits that data to an authentication server.
- The authentication server then request the access point for proof of the validity of the ID.
- After the verification from the user, access point sends it back to the authentication server and the user is connected to the network.

3) PAP: It is Password Authentication Protocol. It is used by Point to Point Protocol to validate users before allowing them access to server resources. In this protocol, a user‟s name and password are transmitted over a network and compared to a table of name-password pairs. It is a two way handshaking protocol.

- Client sends username and password.

Server sends “authentication-ack”, if credentials are OK or “authentication-

		nak”. **4) SPAP**: It is Shiva Password Authentication Protocol and it is an encrypting authentication protocol used by Shiva remote access servers. SPAP offers a higher level of security than other authentication protocols such as PAP, but it is not as secure as CHAP. **5) DES:** It is a Data Encryption Standard (DES) is the classic among the symmetric block cipher algorithms. DES was developed in the 1970s as a US-government standard for protecting non-classified information. DES encrypts 64-bit clear-text blocks under the control of 56-bit keys. Each key is extended by a parity byte to give a 64-bit working key. It uses both substitutions as well as transposition techniques of cryptography. **6) RADIUS**: It is a Remote Authentication Dial-In User Service protocol. It is a client/server protocol and used for authentication and authorization of users who are dialing in remotely to servers on the network. □ RADIUS client sends username and encrypted password to the RADIUS server. □ RADIUS server responds with Accept, Reject, or Challenge. □ The RADIUS client acts upon services and services parameters bundled with Accept or Reject. **7) S/KEY**: It is a one-time password system developed for operating systems like UNIS. One-time password allows you to log on only once with a password, Authentication Protocol (MS-CHAP). It is based on CHAP and was developed to authenticate remote Windows- based workstations. It uses the Message Digest 4 (MD4) hashing algorithm and the Data Encryption Standard (DES) encryption algorithm to generate the challenge and response. It also provides mechanisms for reporting connection errors and for changing the user‟ password. It only works on Microsoft Systems.	
5		**Attempt any TWO :**	**16 M**
	a	**Enlist two types of failures. How deleted files can be recovered?**	8M
	Ans	Two types of failures: 1. Logical Failure 2. Physical Failure (Any other types can be considered) **Deleted files 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.	Listing Failure 1M, Explanation of Recovery 7M

For example: When storing files into hard disk, system would firstly write file names and size in FAT and successively write file content on FAT at the data field starting location in accordance with free space, then it begins to Write real content in data field to complete 'file storage.

So, when anyone deletes a file, it does not disappear.

Every computer file is a set of binary data i.e. in forms of l's and 0's. The physical space is declared as available space for new data to be written when a file is deleted. So if anyone performs any new activity on a disk after deleting a file, then there is a chance that the file Would be replaced partially or completely by new data.

For example: When deleting a file, system will just write a mark in the front of this file within FAT to mean this file is deleted and space it occupies is released for other files. Therefore, user is only required to employ a tool to remove the deletion mark when he wants to recover data.

Certainly, all these should he performed under the requirement of no new files are written to occupy previous space of lost file in same way, if anyone performs disk defragmentation, the file may be overwritten.

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

OR

Deleted files recovery

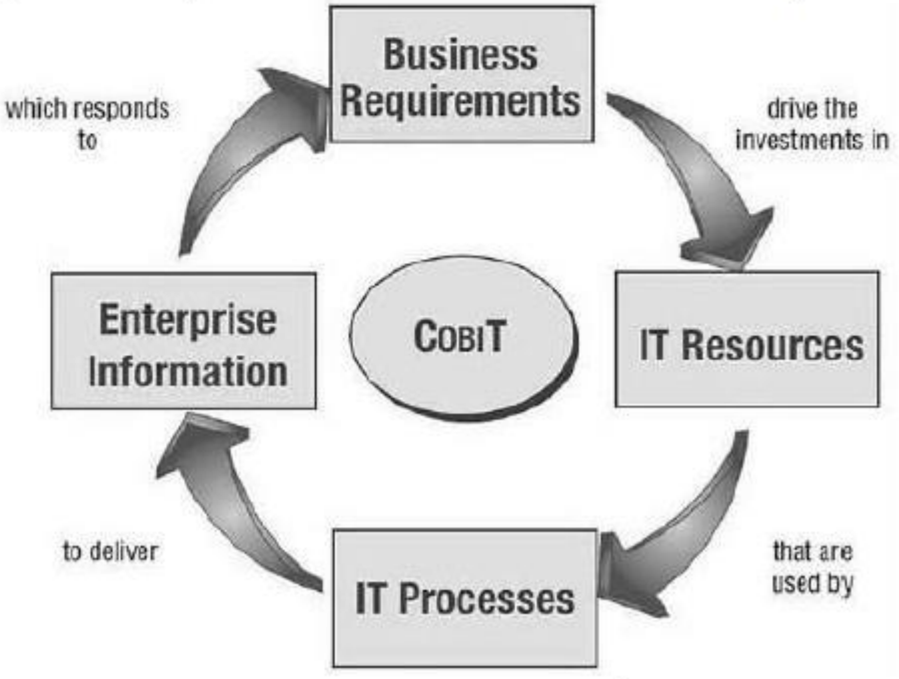
1. Download, install and run the program on your computer. A welcome screen will appear.
   Click "Next" to proceed.

2. It will ask you which kind of files you are trying to retrieve? Check any one of the given options. If you want to retrieve two kinds of files, ex. pictures and music then you cannot select both the options simultaneously.

3. Select the location where you want to retrieve the files from.

4. In the next screen, click "Start" button. Don't select deep scan option until you fail on your first attempt to recover the file. Note that "Deep scan" could take over an hour depending upon the size of your hard disk. The process will start.

		5. It will show all the deleted files. To retrieve the file, check the box next to file name and click on “Recover” button. 6. Select the folder where you want to recover your file. You should select a drive or a folder different from the scanned drive (Say you scanned C drive to search all the deleted files so you should select D drive to recover those files). After selecting the appropriate location, click OK button. 7. Now check the folder. You will get your file back.	
	B	**Describe COBIT framework with neat sketch.**	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‖. COBIT is a framework developed by ISACA (Information System Audit and Control Association) in year 1996 for IT management and IT governance. COBIT is a set of guidance materials for IT governance that allows managers to bridge the gap between control requirements, technical issues and business risks. The main aim of COBIT is to research, develop, publicize and promote an authoritative, up to date, international set of generally accepted information technology control objectives for day to day use by business managers, IT professionals and assurance. In COBIT, a control is the policy, procedure, practices and organizational structures, which are designed to achieve reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. Control objective is a statement of desired result or purpose to be achieved by implementing control procedures in a particular activity. The COBIT framework is based on the following principle: To provide the information that the organization requires to achieve its objectives, the organization requires investing in and managing and controlling IT resources using a structured set of Processes to provide the services which deliver the required enterprise information.	Explanation 6M, Diagram 2M



COBIT Framework

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

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

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

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

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

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

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

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

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

The COBIT framework provides a reference process model and common language for everyone in an enterprise to view and manage IT activities.

The most necessary and early step towards good governance is use of an operational model and a common language for all different parts of the business in IT.

COBIT will provide a structure to measure and monitor the performance of IT, communication with service providers and incorporation of best management practices.

A process model encourages process ownership, enabling responsibilities and accountability
to be defined.

	c	Describe Stepwise Working of Single Sign On (SSO)	8M
	Ans	**Single Sign-On**	Explanation

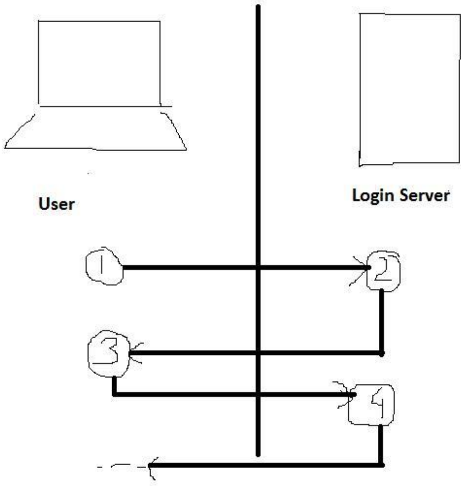
4M

- Single sign-on is a user/session authentication process that permits a user to enter one name and password in order to access multiple applications.
- The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

Working of SSO

- Whenever a user accesses an application, the Login Server first authenticates that user.

Authenticating to the Login Server

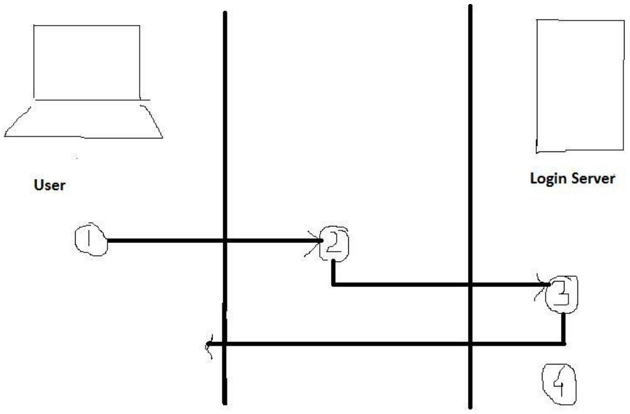


Login Server checks for login cookies. If one is present, the login server identifies the user from the encrypted information in the login cookie.

1) If a login cookie is not present, the login server prompts the user for the user's credentials
2) The user provide user name and password
3) The Login Server authenticates the user by passing the provided name and password to the configured authentication routine.

If authentication is successful, the Login Server establishes a Login Cookie on the client browser to facilitate SSO for future authentication requests.

Accessing a Partner Application



1) The user seeks the access to the partner application directly.

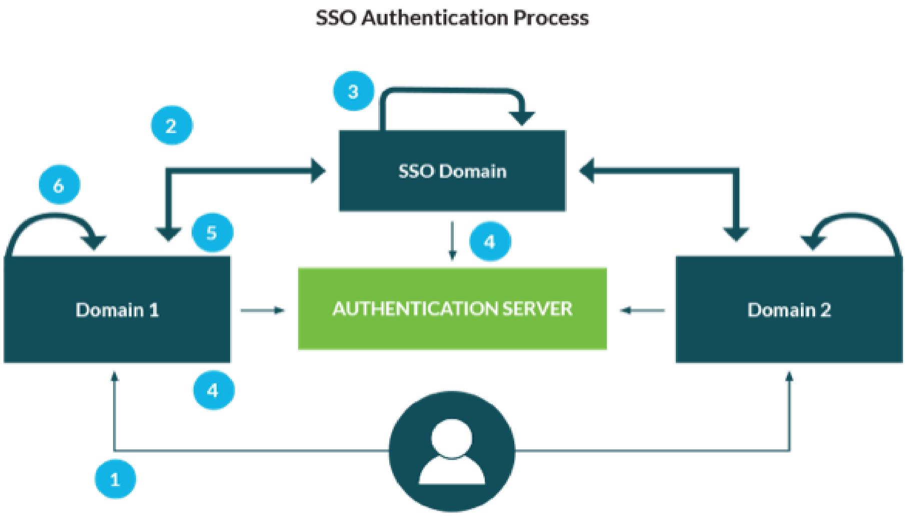
2) For the first time during a session, the user is accessing partner application, and then the partner application transparently directs the user to the Login Server to obtain authentication credentials.

3) The Login Server authenticates the user as describe in "Authenticating to the Login Server"

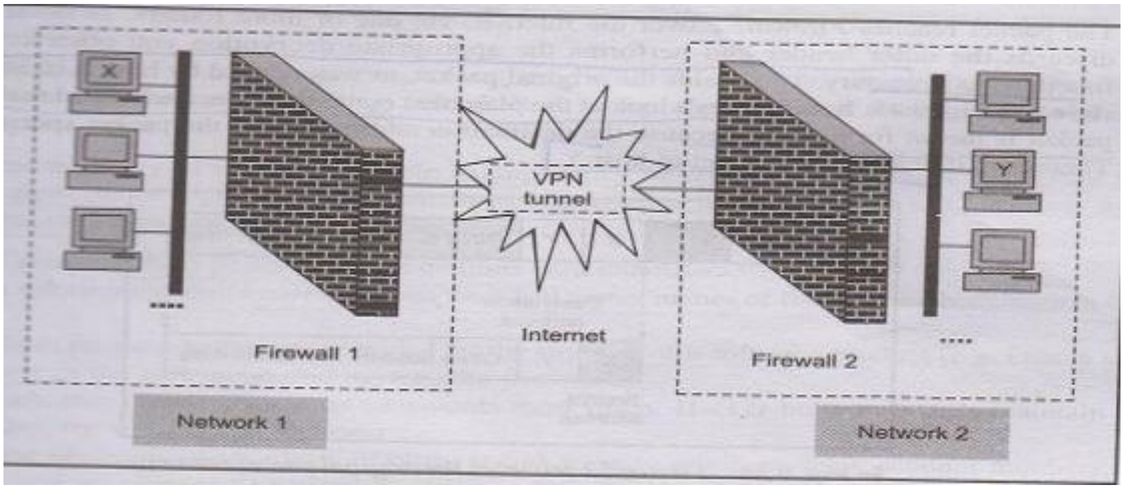
4) The Login Server transparently directs the user to the partner application. It does this by using a URL with an encrypted parameter containing the user's identity.

5) The Partner Application then decrypts the parameter, identifies the user, and establishes its own session management.

OR



		Here is the SSO authentication process detailed in 5 steps: 1. The user arrives on the target website they want to log into. 2. The domain automatically redirects the user to a central SSO domain to log in. 3. The user enters their login credentials. 4. The central SSO domain submits the credentials to the authentication server to validate them. 5. When the user’s credentials are validated, the central SSO domain redirects the user to the original website and embeds a token to guarantee their authentication. 6. The embedded token is then used to automatically authenticate the user, logging them into the original website. 7. The authentication token is then stored so that the user can safely access any other websites that share the central SSO domain. If the user wants to log into Domain 2 the same process will apply, but since all login attempts are made on the SSO Domain, the user doesn’t need an additional set of credentials to log in.	
6		**Attempt any FOUR :**	**16 M**
	a	**Describe IT ACT 2000**	4M
	Ans	The IT Act 2000 gives very good solution to the cybercrimes these solutions are provided in the following ways. In this Act several sections and Chapters are there which are defined in the following manner: 1**. Chapter 1** the preliminary chapter of IT Act 2000 gives all of the information about the short title, territory up to which it is extendable, and the basic application of related laws. 2. **Chapter 2 to 7** of this Act defines “access‟, “addressee‟, “adjudicating officer‟, “affixing digital signature‟, “Asymmetric Cryptography‟, “cyber‟, “computer‟, “digital signature‟, “Digital Signature Certificate‟ and other numerous basic terms, which are defined in its appendix. **3. Other chapters of this Act** define those crimes which can be considered as cognizable offences, i.e. for which the police can arrest the wrongdoer immediately. 4. **Section 80 of this Act** gives a freedom to the police officer to search, arrest the offender who is indulged in that crime or going to commit it. 5. **Section 65 to 70** covers all of the cognizable offences, namely, “tampering of documents‟, “hacking of the personal computer‟, “obscene information transmission or publication‟, “failure of compliance by certifying authority or its employees, of orders of the Controller of certifying authorities‟, “Access or attempt to access by any unauthorized person, a protected system notified by Govt. in the Official Gazette‟ in which non-bailable warrant is issued or no warrant is required.	Explanation 4M

	b	**Explain working of Virtual Private Network with neat sketch.**	4M
	Ans	A VPN is a mechanism of employing encryption, authentication, and integrity protection so that we can use a public network as if it is a private network Suppose an organization has two networks, Network 1 and Network 2, which are physically apart from each other and we want to connect them using VPN approach. In such case we set up two firewalls, Firewall 1 and Firewall 2. The encryption and decryption are performed by firewalls. Network 1 connects to the Internet via a firewall named Firewall 1 and Network 2 connects to the Internet with its own firewall, Firewall 2.  X Y VPN tunnel Internet Firewall 1 Firewall 2 Network 1 Network 2 Working Let us assume that host X on Network 1 wants to send a data packet to host Y on Network 2. 1) Host X creates the packet, inserts its own IP address as the source address and the IP address of host Y as the destination address. 2) The packet reaches Firewall 1. Firewall 1 now adds new headers to the packet. It changes the source IP address of the packet from that of host X to its own address (i.e. IP address of Firewall 1, F1). 3) It also changes the destination IP address of the packet from that of host Y to the IP address of Firewall 2, F2. It also performs the packet encryption and authentication, depending on the settings and sends the modified packet over the Internet 4) The packet reaches to firewall 2 over the Internet, via routers. Firewall 2 discards the outer header and performs the appropriate decryption. It then takes a look at the plain text contents of the packet and realizes that the packet is meant for host Y. It delivers the packet to host Y Diagram (1 marks)	Explanation 3M, Diagram 1M
	c	**Describe what is ITSEC.List out various classes of ITSEC**	4M
	Ans	**ITSEC: Information Technology Security Evaluation Criteria.** 1. ITSEC focuses more on integrity and availability. It tries to provide a uniform approach	Description of ITSEC 3M, Listing

		to product and system. 2. ITSEC will also provide security targets like: i. Policy for system security ii. Required mechanism for security iii. Required rating to claim for minimum strength iv. Level for evaluating targets –functional as well as evaluation ITSEC classes contain hierarchical structure where every class will be added to the class above it. This class contains some particular function. F-IN This class will provide high integrity. F-AV This class will provide high availability. F-DI This class will provide high data integrity. F-DX This class is used for networks. Of provide high integrity while exchanging data in networking. ITSEC uses following I classes from E0 to E6 to evaluate the security. E0 – Minimal protection. E1 – Security target and informal architecture design must be produced. E2 – An informal detail design and test document must be produced. E3 – Source code or hardware drawing to be produced. Correspondence must be shown between source codes of detailed design. E4 – Formal model of Security and Semi – formal specification of Security function architecture and detailed design to be produced. E5 – Architecture design explain the inter relationship between Security component. E6 – Formal description of architecture and Security function to be produced. Information could leak from those users who were cleared to see it, down to those users who are not. Design must be produced. E2 – An informal detail design and test document must be produced. E3 – Source code or hardware drawing to be produced. Correspondence must be shown between source codes of detailed design.	1M

		E4 – Formal model of Security and Semi – formal specification of Security function architecture and detailed design to be produced. E5 – Architecture design explain the inter relationship between security component. E6 – Formal description of architecture and Security function to be produced. Information could leak from those users who were cleared to see it, down to those users who are not.	
	d	**Describe TCSEC model.**	4M
	Ans	The Trusted Computer System Evaluation Criteria (1983-1999), better known as the Orange Book, was the first major computer security evaluation methodology. The Orange Book was part of a series of books developed by the Department of Defense in the 1980's and called the Rainbow Series because of the colorful report covers. The TCSEC defines 6 evaluation classes identified by the rating scale from lowest to highest: D, C1, C2, B1, B2, B3, and A1. An evaluated computer product could use the appropriate rating based upon the TCSEC evaluation of that product. Such an evaluated product is called a rated product. Evaluation Classes D. Minimal Protection • No security characteristics • Evaluated at higher level and failed C1. Discretionary Protection • DAC • Require identification & authentication • Assurance minimal • Nothing evaluated after 1986 C2. Controlled Access Protection • C1 + • Auditing capable of tracking each individuals access or attempt to each object • More stringent security testing • Most OSs at end of the TCSEC incorporated C2 requirements B1. Labelled Security Protection • C2 +	Any Valid Explanation 4M

- MAC for specific sets of objects
- Each controlled object must be labelled for a security level & that labelling is used to control access
- Security testing requirements more stringent
- Informal security model for both hierarchical levels and non-hierarchical categories informal security model shown consistent with its axioms.

	e	**Describe working of steganography with neat diagram.**	4M

Ans

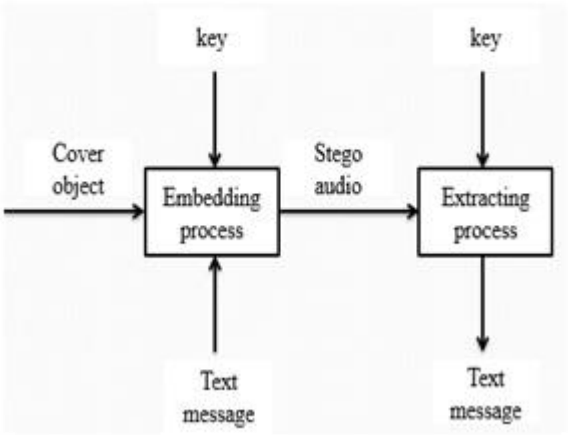
Explanation 3M, Any Valid Diagram 1M

Steganography is the art and science of writing hidden message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.

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.

In modern steganography, data is first encrypted by the usual means and then inserted, using a special algorithm, into redundant data that is part of a particular file format such as a JPEG image.



Steganography process:

Cover-media + Hidden data + Stego-key = Stego-medium

Cover media is the file in which we will hide the hidden data, which may also be encrypted using stego-key. The resultant file is stego-medium. Cover-media can be image or audio file.

Stenography takes cryptography a step further by hiding an encrypted message so that no one

		suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data. Stenography has a number of drawbacks when compared to encryption. It requires a lot of overhead to hide a relatively few bits of information. (Consider any other relevant diagram)	