CMR INSTITUTE OF TECHNOLOGY

((Approved by AICTE, Permanently Affiliated to JNTUH, Hyderabad, Accredited by NBA and NAAC with 'A' Grade)
Kandlakoya, Medchal Road, Hydarabad-501401
UGC Autonomous

COURSE: III - **B.Tech / M.Tech / MBA** I . **SEM**

Date of Examination	:	12/01/2024.
Regulation	:	R20
Regular / Supply	:	Regular
Branch	:	CSE, CSE(AI&ML), CSE(DS)
Subject Name	:	Information & Cyber security.
Subject Code	:	20-CS-PC-313

PART-A

1. Define Reverse Engineering [2M]

-> Reverse engineering is the act of dismantling an object to see how it works. [1M]

-> It is done primarily to analyze and gain knowledge about the way something works but often is used to duplicate or enhance the object. [1M].

2. Examine the difference between Threat and attack [2M]

	Threat	Attack:
i)	A Potential for violation of security, which exists when there is a circum-stance, capacity, action or event that could breach security & cause harm	An attack on system security that derives from an intelligent threat.
ii)	A Threat is a possible danger that might exploit a vulnerability	An attack that deliberate attempt to evade security services & violate the security policy of a system.

3. Define Cyberstalking. [2M]

Cyberstalking has been defined as the use of information and communication technology, Particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals or organisation.

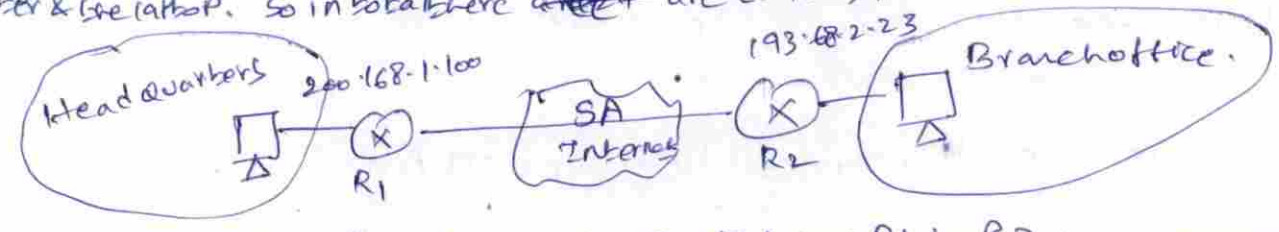
4. Name the two different categories of cybercrime. [2M]

1. The target of the crime.
2. whether the crime occurs as a single event or as a series of event. (or)

1. Crime targeted at individual, 2. Crimes target at Property, 3. Targeted at organization.

5. Assume that there is bi-directional IPsec traffic between headQuarters and 5 branch offices in a VPN. Enter the number of SA's to be established [2M]

There are 2 SA's b/w the headquarters gateway router and the branch office gateway router, for each salesPerson LaPtop, there are 2 SA's b/w the headQuarters gateway router & the laPtop. So in total there ~~are~~ are (2+2n) SA's.



Security Association [SA] from R1 to R2.

6. Differentiate SSL & TLS. [2M]

	SSL	TLS
1.	SSL stands for Secure Socket Layer	TLS Stands For Transport Layer security
2.	In SSL, the Message digest is used to Create a master secret	In TLS, a Pseudo-random function is used to create a master secret.
3.	In SSL, the Message Authentication code Protocol is used	In TLS, Hashed message Authentication code Protocol is used.

7. Define Logging. [2M]

Logging is to create an ongoing record of application events. Every activity on your environment, from emails to logins to firewall update is considered as security event. All of these events are logged in order to keep tabs on everything that's happening in your technology landscape.

8. Recall the different ways in which the asset is classified. [2M]

i) Highly Restricted
ii) Confidential
iii) Internal use only
iv) Public.

9. Recite Copyright Law. [2M]

Copy Right Law - Rights to Copy.

Copyright Law grants the exclusive rights to authors and artists to control how their works will be copied. The Law Protects the intellectual Property rights of authorship for a certain number of years. Legally Protecting works of creative expression set in a Fixed, tangible form such as a book or audio recording.

10. Skate any 2 cyber Laws in india. [2M]

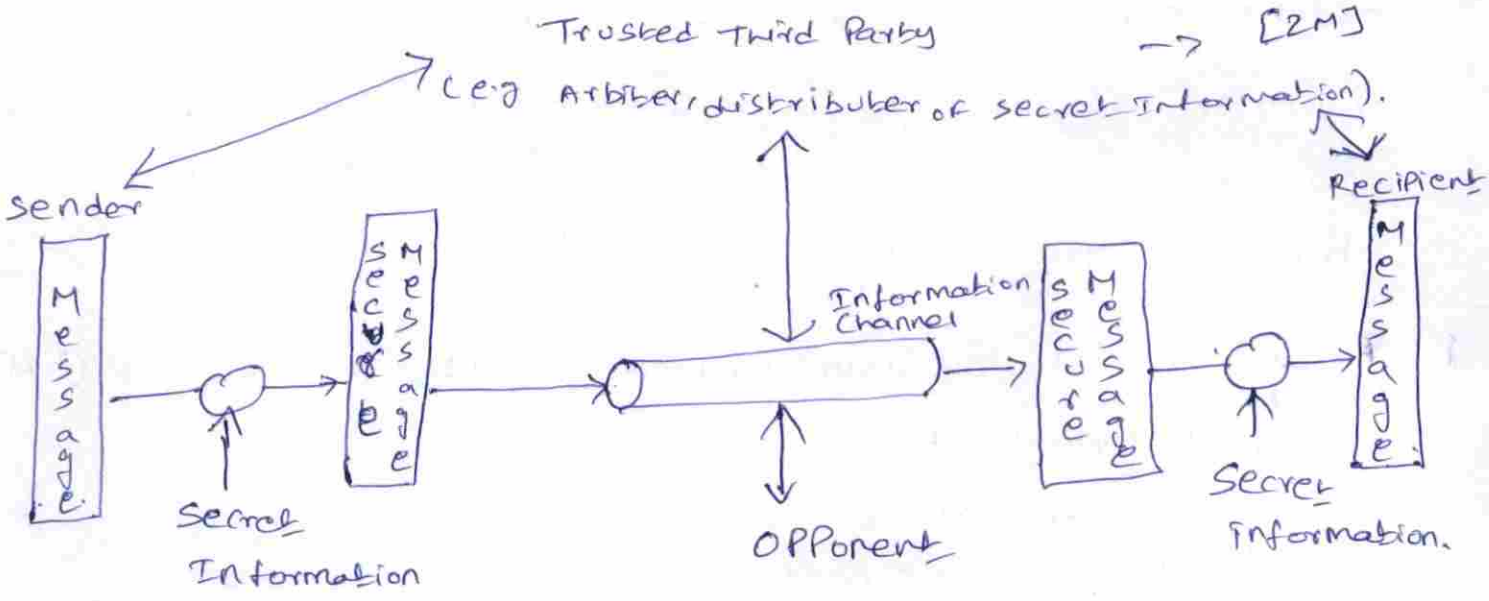
1. Patent Law.
2. Copyright Law.

1. Patent Law: Patent Law is the branch of Intellectual Property that deals with new inventions.

2. Copyright Law: Copyright Law grants the exclusive right to authors and artists to control how their works will be copied.

Part-B.

11. A. i) with a neat Diagram, explain the network Security Model. [5M]



All the Techniques for Providing security have 2 components:

→ A security related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

→ Some secret information shared by the 2 Principals and it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

2M

→ A Trusted 3rd Party may be needed to achieve secure transmission. for ex, a third party may be responsible for distributing the secret information to the 2 Principals while keeping it from any opponent, or a 3rd Party may be needed to arbitrate disputes b/w the 2 Principals concerning the authenticity of a message transmission

This general model shows that there are 4 basic tasks in designing a particular security service: [2M]

1. Design an algorithm for performing the security related transformation. The algorithm should be such that an opponent can't defeat its purpose.
2. Generate the secret information to be used with the algorithm
3. Develop methods for the distribution & sharing of the secret information
4. Specify a Protocol to be used by the 2 Principals that makes use of the security algorithm and the secret information to acheive a particular security service.

---

11. A. ii) Describe different types of Operating System attacks [3M]

Operating system attacks: attackers look for vulnerabilities in OS such that they can exploit through vulnerabilities and gain access to the target system or network.

The vulnerabilities in the OS can be open ports & services as most of the operating system install these services and ports by default. These are the most common vulnerabilities found by attackers to gain access to the an operating system.

Some of the OS vulnerability list:

- -> Buffer overflow vulnerability
- -> Bugs in the OS
- -> UnPatched OS

2M

Some of the attacks performed by OS level:

- -> Exploiting specific NW Protocol Implementation
- -> Attacking built-in authentication system
- -> Breaking file system security
- -> Cracking Pwd's & encryption mechanism.

Misconfiguration Attacks: [CIM] It can be defined as "occurence of errors while implementing the security controls".

-> It may occur either at any stage like developing, deploying or maintaining, etc. Due to this attackers gain unauthorized access to the system & affect web servers, databases etc.

Prevention: Administrators need to change default configuration of the devices & deploy automated scanners

Application-Level attacks: [CIM] It is defined as "A program or software which can perform a specific function to an end user or for some other application.

-> Since the code for an application comes with more features & functionalities, there may be some undiscovered security holes or vulnerabilities leaving behind.

-> This is the opportunity for an attacker to find these vulnerabilities & exploit using diff techniques to gain access & steal data.

Prevention: These kind of attacks error checking or handling of applications must be strict.

Shrink-wrap code attacks: [CIM] It is defined as "exploiting the default configuration & setting of libraries & code".

Prevention: Have to fine tune every part of the code & make it more secure.

11. B) Explain any five types of web application attacks. [5M]

1. SQL Injection: SQL Injection has become a common issue with database-driven websites [2M]

username & password '1'='1'

2. Phishing: Phishing attack entailing fraudulent communications appearing to come from a trusted source. Phishing attack is that the practice of sending emails that appear to be from trusted sources with the goal of gaining Personal Information or influencing users to do something. [2M]

3. Denial of service: It prevents normal use of communication facilities. This attack may have a specific target victim ex: server attacking by keeping many requests. [2M]

4. Session Hijacking: An attacker hijacks a session between a trusted client and network server. [2M]

5. Man in the Middle: A MITM attack is one where the attacker intercepts & relays messages b/w 2 parties who believe they are interacting with one another. [2M]

12. A. Explain in detail about the Phases Involved in Planning Cybercrime. [10M.] (8)

The following Phases are involved in Planning Cybercrime.

1. Reconnaissance (Information gathering) is the First Phase and is treated as Passive attacks
2. Scanning & Scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities
3. Launching an attack (gaining & maintaining the system access).

1. Reconnaissance: It is an act of reconnitering - explore, often with the goal of finding something or somebody.

-> It begins with footPrinting

-> footPrinting gives an overview about system vulnerability & Provides a judgement about Possible exploitation of those vulnerabilities

-> The objective of this Phase is to understand the system, its N/w Ports & services and any other aspects of its security that are needful for launching the attack.

Thus an attacker attempts to gather information in 2 Phases:

a) Passive attack
b) Active attack.

a) Passive attack:

A Passive attack involves gathering information about a target without his/her knowledge.

examples: 1. Google or yahoo search; People search to locate information about employees

2. Surfing online community groups like facebook will prove to gain information about individual.

3. organization website may Provide information about employees
   ex: contact details, mail id.

4. Blogs, newsgroups, Press releases etc.

5. Going through the job opening or Posting to gain information about individuals

b) ~~Passive~~ Active attack:

An Active attack involves Probing the NIW to discover individual hosts to confirm the information gathered in the Passive attack Phase. It involves the risk of detection & also called Active reconnaissance.

→ using many tool Active attack can be Performed tool like NMAP, Ping, ScanSSH.

2. Scanning & ~~Sorting~~ Scrutinizing Gathered Information:

Scanning is a key step to gather info about target. The objective are 1. Port Scanning: Identify open / close ports & services
2. NIW scanning: understand IP address & related information about the computer NIW systems
3. Vulnerability scanning: understand the existing weakness in the system.

3M

The scrutinizing Phase is called enumeration in the hacking world. The objective behind this step is to identify:
1. The valid user accounts or groups
2. NIW resources & / or shared resources
3. OS & diff appln's that are running in the OS.

3. Attack (Gaining & Maintaining the System Access).

After the scanning & enumeration, the attack include following steps:
i) Crack the Password
ii) exploit the Privileges
iii) execute the Malicious commands / applications
iv) hide the files
v) cover the tracks - delete the access logs, so that there is no trail illicit activity.

2M

12. B. i) Summarize various risks associated with cloud computing environment. [5M] (10)

S.No	Area	What is the Risk	How to Remediate the Risk?
1.	Elevated user Access	Any data Processed outside the organization brings with it an inherent level of risk as outsourced services may by Pass the Physical, logical & Personnel controls and will have elevated user access to such data.	Customer should obtain as much info as he/she can about the service Provider who will be managing the data & scrutiny vendors monitoring mechanism about hiring & oversight of Privileged administrator & IT controls over the access Privileges.
2.	Regulatory compliance.	Cloud computing service Providers are not able and/or not willing to undergo external assessments. This can result into non compliance with various standards like HIPAA, PCI DSS.	The organization is entirely responsible for the security Integrity of their own data.
3.	Location of the data.	The organization that are obtaining Cloud comp. services may not be aware about where the data is hosted & may not even know in which country it is hosted.	org. should ensure that the service Provider is commited to obey local Privacy requirements on behalf of the org. to store & Process the data in the specific jurisdictions.
4.	Segregation of Data.	As the data will be stored encrypted, enc. mechanism should be strong enough to segregate the data from other org, whose data are also stored under the same server.	org. should be aware of the arrangements made by the service Provider about segregation of data.
5.	Recovery of Data.	Business- Continuity In case of any disaster -availability of services & data without any disruption.	organization should ensure the enforcement of contractual liability over the service Provider about complete restoration of data within stipulated time frame.
6.	Information security violation Reports	Due to complex IT encrypted & several customers logging in & logging out of the hosts, it becomes difficult to trace Illegal activity.	org. should enforce the contractual liability toward Providing secure validation logs at Regular Intervals

7.	Long Term viability	In case of any major change in the cloud comp service, the service Provided is at the stake	organization should ensure getting their data in case of such major event.

12. B. ii) Discuss about Social Engineering: [5M]

Social Engineering: [1M]

→ It Involves gaining sensitive Information or Unauthorized access Privileges by building inappropriate trust relationships with Insiders.

→ It is an art of exploiting the trust of people, which is undoubted while speaking in a normal manner.

→ The goal of social Engineer is to fool someone to gain information or access to that information.

Classification of Social Engineering

a) Human Based Social Engineering:

i) Impersonating an employee or ~~valid~~ valid user
ii) Posing as an important user
iii) using a 3rd Person
iv) calling Technical support
v) Shoulder Surfing
vi) Dumpster diving.

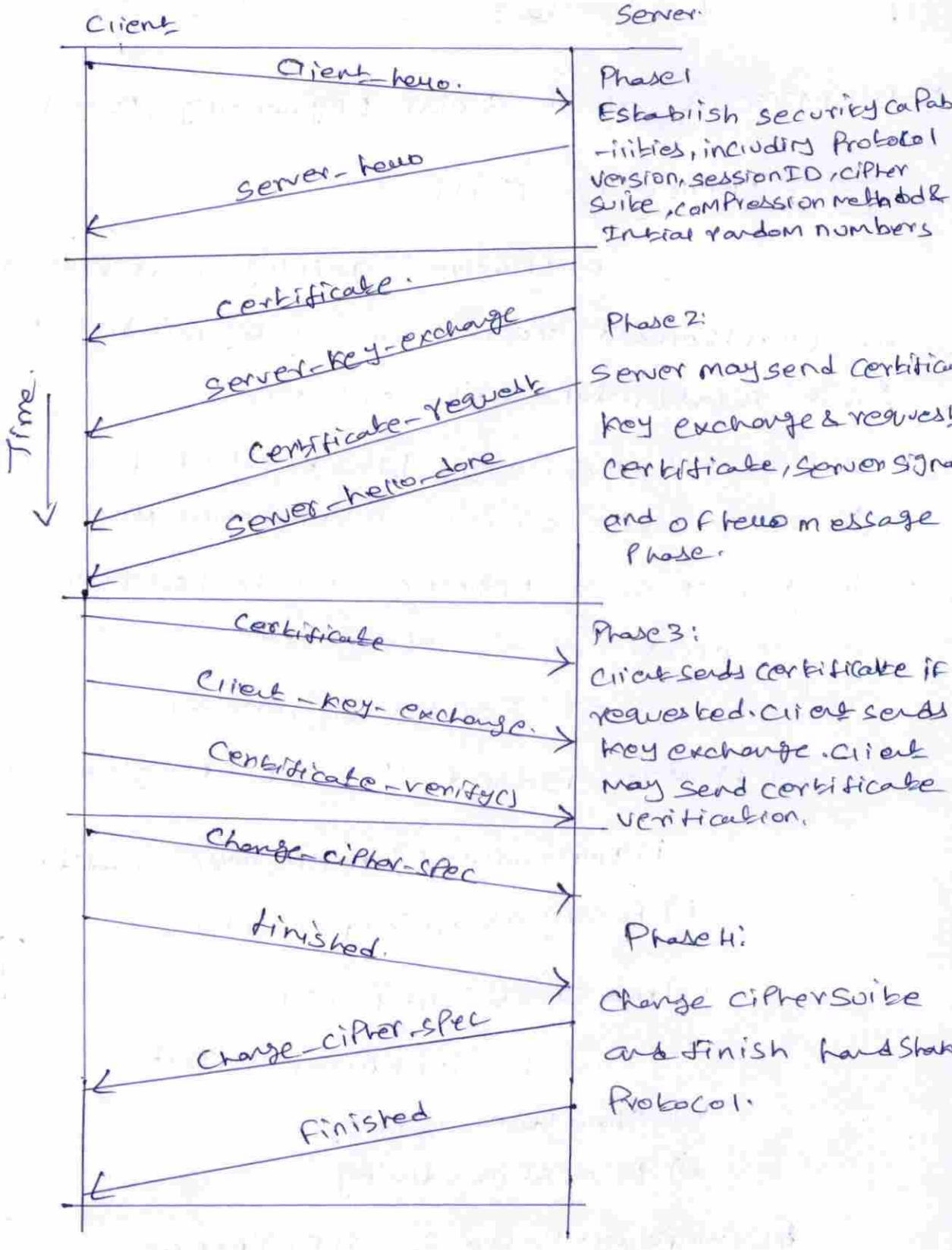
[2M] with explanation

b) Computer-Based Social Engineering

i) fake E Mails
ii) EMail attachments
iii) PopUp windows

[2M] with explanation

13.A. Illustrate with a neat diagram the different Phases in a SSL Handshake Protocol Mechanism. [10M]



HANDSHAKE PROTOCOL ACTION.

HandShake Protocol allows the server & client to authenticate each other & to negotiate an encryption & MAC alg & Cryptographic key to be used. [5M]

The exchange can be viewed as having 4 Phases:

Phase1: Establish security capabilities: [IM]

It sends the client hello message with following parameters: a) version b) Random c) SessionID d) Cipher suite e) Compression method

The following key exchange methods are supported.

a) RSA b) fixed Diffie-Hellman c) Ephermal Diffie Hellman d) Anonymous Diffie Hellman.

Phase2: Server Authentication and Key exchange: [IM]

The server begins this Phase by sending its certificate if it needs to be authenticated. The message contains a chain of X.509 certificate.

A server key exchange message may be sent if required. It includes the following a) Anonymous Diffie Hellman b) Ephermal Diffie Hellman c) RSA key exchange.

The final msg in Phase 2 is server-done-message. This message has no parameters

Phase3: Client Authentication & Key exchange: [IM]

If server has requested a certificate, the client begins this Phase by sending a certificate message. Then client-exchange key-message is sent along with any method: RSA, fixed Diffie hellman, or Ephermal Diffie Hellman is used

Finaly the client may sent certificate_ verify message to Provide explicit veridication of a client ~~certificate~~ certificate.

Phase 4: Finish: [1M]

The client sends a change_cipher_spec Message and copies the pending cipher into current cipher spec. The client immediately sends the finished Message.

---

13. B. Describe various services Provided by PGP in detail. [10M]

There are 4 services Provided by PGP: } 1M.

a) Authentication
b) confidentiality
c) COMPression
d) email compatibility.

Function	Algorithm used	Description
Digital Signature (Authentication)	DSS/SHA or RSA/SHA	A ~~Sh~~ Hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with Sender's Private key
Message Encryption (confidentiality)	CAST or IDEA or TDES with Diffie Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with one time session key is encrypted using Diffie Hellman or RSA with receiffent's Public key & included with message.

Compression	ZIP	A Message may be Compressed for Storage or transmission using ZIP.
Email Compatibility	Radix 64 Conversion	To Provide transparency for email applications are encrypted Message may be converted to an ASCII string using radix 64 conversion.

4M

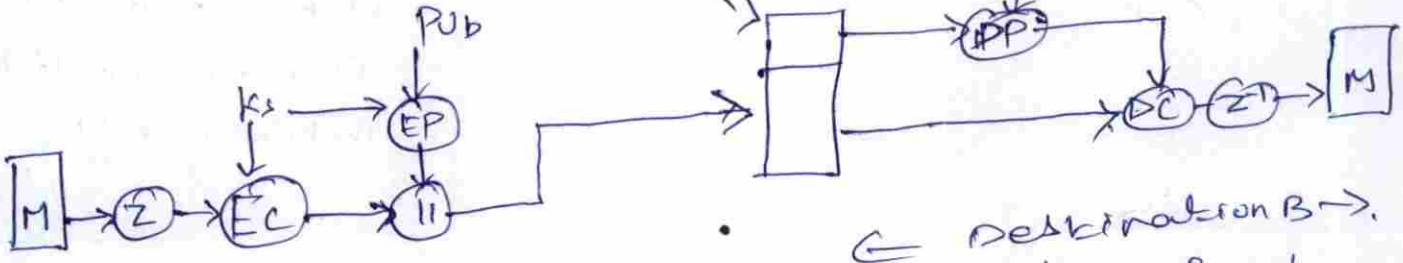
Authentication only:

← Source-A →

← Destination B → with explanation.

Confidentiality:

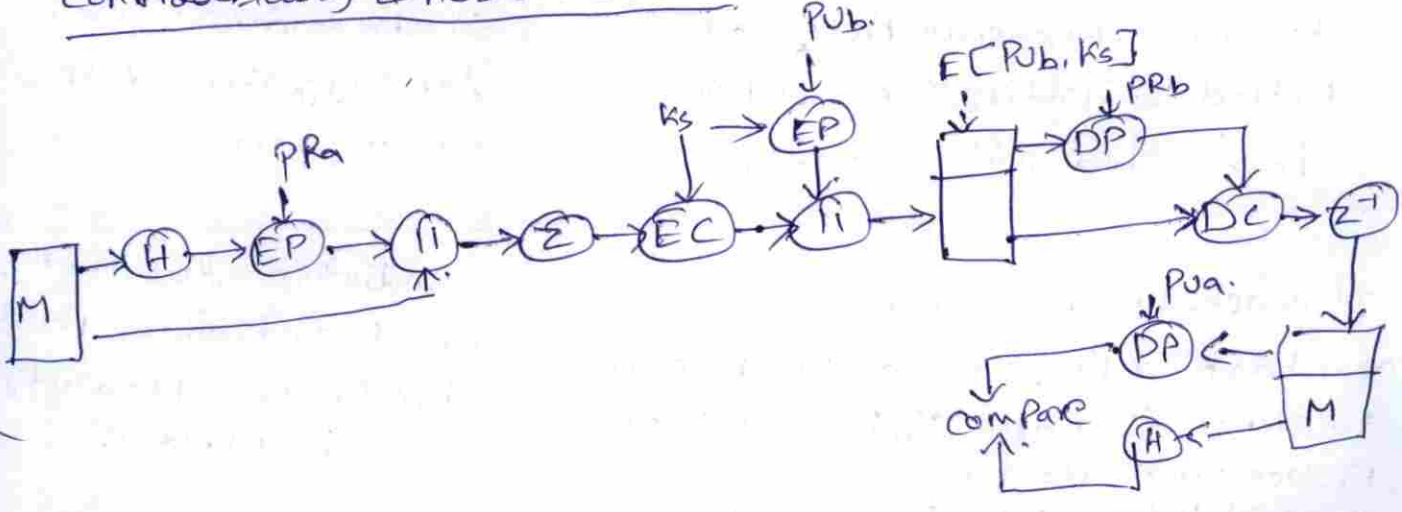
5M



← Source-A →

← Destination B → with explanation.

Confidentiality & Authentication:



with explanation.

14. A-i) Compare and contrast Risk assessment & Risk Management. [5M] (16)

S.NO	Risk assessment	Risk Management.
1.	Risk assessment is a subset of Risk Management.	The Process of taking action to assess risks and avoid or reduce risk to acceptable levels.
2.	Risk assessment to visualize Company's Potential risks	Risk management focuses on everything that needs to be done after risks are identified.
3.	Risk assessment is the Process of Identifying, analyzing & evaluating risks	Risk Management will decide should avoid risk, should Transfer risk or should ~~Mtig~~ mitigate risk
4.	Risk assessment simply means to describe the overall Process or Method to identify risk & Problem factors that might cause harm	It encourage all the Stakeholders & users for suggesting risks at any time.
5.	It is actually a systematic examination of a task or Project that you perform to simply identify significant risk, Problems, hazards & find out ~~to~~ measures you will reduce risk. The Best approach is Prepare Set of Questions.	Conducting Risk Manage-ment activities pools the skills & knowledge of Stakeholders

14. A. ii) Prioritize the necessary steps to be taken for resource recovery. [5M]

→ A cyber security system requires a cyber vault that is both physically & virtually isolated and functions as a data center. It is automated to control the gap b/w a disaster recovery system & a cyber recovery system by leaving the link open or close it when necessary. [1M]

→ The vault storage backup system is immutable, meaning that the data can't modified or compromised by crypto-locking, leaving it safe for you to restore once your NW is clean.

→ Cyber recovery planning can be complex, but it is crucial. Follow the 5 steps below to strengthen your cyber recovery strategy.

- → Go Beyond disaster Recovery
- → Priorize your data
- → Leverage Air-gapped Cyber Recovery vaults & Immutable copies
- → Restore your Data efficiently
- → Remember that your not alone.

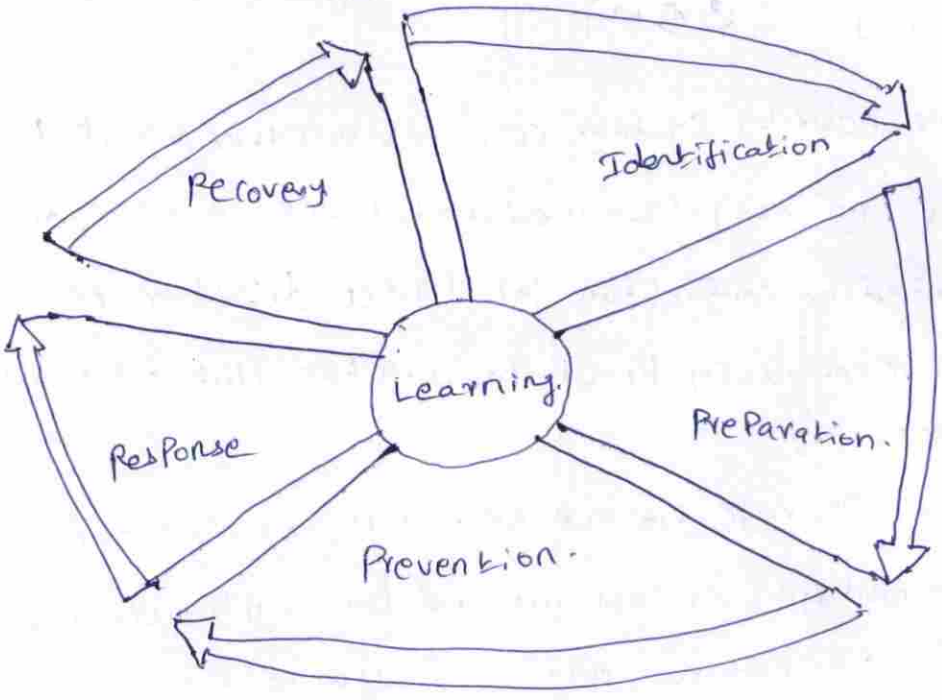
with explanation [4M]

---

14. B. Explain in detail about Crisis Management Plan. [10M]

A Crisis Management Plan outlines how your business will respond if a crisis occurs. The Plan should identify who will take action & what their roles will be. The goal of a crisis management Plan is to minimize damage & restore business operations as quickly as possible. [5M]

Crisis Management Cycle: [SM]



Crisis: It is any event that is expected to lead to, an unstable and dangerous ~~sit~~ situation affecting an individual, group or whole organization.

Crisis Management: It is the process by which organization deals with a major event that threatens to harm the organization, its stakeholders or the general public. [IM]

i) First Stage of Crisis Management is Identifying the Crisis nature:

Crisis can be clusted into

- Natural Crisis
- Organizational misdeed crisis.
- Deception Crisis
- Workspace violence crisis
- Skewed value Crisis
- Rumor Crisis

} with explanation [IM]

ii) Second Stage is Preparing for the Crisis [IM]

Crisis Preparation is done by

- vulnerability assessment: Determine current & Potential areas of operational & communication weakness.

Crisis Planning: are two types

operational : what we do, who does it, & when it is done.

Communication: what do we say, who says it, how do we get the messages out Preparation

iii) Third stage is Preventing the crisis from Planning: [1M]

Crisis Prevention is occured by

→ Anticipate & Have a Plan
→ Respond immediately
→ Do not over talk
→ Always tell the truth.
→ Accept responsibility Prevention

iv) 4th stage is Responding to the Crisis: [1M]

Effective crisis response includes:- set of Planning scenarios- set of response modules, - Preset activation Protocols- Clear Communication channel. Response.

v) Fifth stage is Recovering from the crisis: [1M]

organizations must be able to carry on with their business in the middle of the crisis. while simultaneously Planning for how they will recover from the damage the crisis caused. crisis handlers must engage in the recovery Plan while pursuing the goal, Recovery.

---

15. A. Discuss about Email security Policies & coporate Policies [10]

Email Security policies [5M]

Email Can be used for Communication, transmit information, harass others. Engage in illegal activities and serve evidence against the action.

Email is actually the electronic version of Post card and require special Policy & guidelines

The goal of an email security policy is to ~~ensure~~ secure messages from unauthorized access.

How to Build an effective Email Security Policy?

1. Adopt a Template
2. Modify the Template
3. Identify user Engagement Terms
4. Implement a Tool
5. Train users
6. Enforce user Policy Acknowledgement
7. Develop an incident Response Plan.

} With explanation

Corporate Policy: [5M]

Corporate Policy is formal declaration of Principles & Procedures according to which a company will operates those Principles & guidelines are executed by board of directors, company senior management Policy committee.

A corporate Policy Includes:

-> company mission statement
-> company objective
-> Principles on the basis of which strategic decesions are made.

Importance of corporate Policy:

1. Corporate Policies ~~Includes~~ boost employee's commitment & loyality for the business

2. It helps in dealing with the issues for optimal utilization of limited resources.

3. It helps in analysis of performance by serving as a standard

4. It helps to perform business activities in smooth way

5. Provide steadiness to the action of the members of the organization.

---

15. B.) Explain Information Technology Act, 2000 [8M]

IT Act, 2000:

-> The Information Technology Act also known as IT Act 2000, or the IT Act main aims is to provide the legal infrature in india which deal with cyber crimes & E-commerce.

2M -> Under this law, for any crime invoving a computer or NW located in india foriegn nationals can also be charged.

-> It also gives legal recognision to digital signatures

The IT Act, 2000 has 2 schedules:

First Schedule

Deals with doccments to which the Act shall not apply

2M Second Schedule: Deals with electronic signature or electronic authentication method.

The offences & the punishments in IT ACT 2000:

->Tamperig with comuter source documents.

→ Direction of controller to a subscriber to extend facilities to decrypt information.

→ Publishing of information which is obscene in electronic form.

→ Penalty for breach of confidentiality & privacy.

→ Hacking of Malicious Purpose.

Sections & Punishment under IT Act 2000 are as follows: [GM]

Section	Punishment.
Section 43	This section of IT Act 2000 states that any act of destroying, altering or stealing or deleting data is liable for the payment to be made to owner as compensation for damages
Section 43A	The section of IT Act, 2000 states that any corporate body dealing sensitive information fail to implement reasonable security practices loss of other person is liable for compensation to the affected party.
section 66	Dishonest or fraudulent using passwords → imprisonment upto 3 years / fine of 5 Lakh INR.
section 66 B, C, D	Identity Theft - 3 year imprisonment or 1 Lakh Fine.
Section 66 E	Violation of Privacy by transmitting image of Private area is Punishable - 3 year imprisonment or 200000 Fine or Both.
Section F	Cyber Terrorism affecting unity, Integrity of India is liable for life imprisonment.
Section 67	This section states pornography or transmission of obscene content liable imprisioment 5 years or 10 Lakh or Both.