Assignment-1

Q1) Name and explain the control categories (with suitable examples) that are essential to handle security issues in an organisation.

Ans → i) Administrative Controls → Focus on the policies, procedures and guidelines that define how security is managed in an organisation.

Examples → a) Security policies → Guidelines for acceptable use of IT resources.

b) Access Control → Rules defining who can access what.

c) Security Awareness Training → Teaching employees how to recognise phising emails or avoid unsafe practices.

ii) Technical Controls → Use technology to protect systems and data from unauthorised access or attacks.

Examples → a) Firewalls → Block unauthorised network traffic.

b) Encryption → Protect data confidentiality during transmission or storage.

c) Antivirus software → Detects and remove malware.

iii) Physical Controls → Protect physical access to facilities and IT systems.

Examples → a) Security guards → Monitor and control entry to buildings.

b) Surveillance cameras (CCTV) → Monitor sensitive areas.

c) Biometric access systems → Control who can enter server rooms.

2) Briefly explain various control types with respect to security concern that help organisers to carry out the operations smoothly at their end.

Ans → i) Preventive Controls → Stop security incidents before they occur. For example, Firewalls, access control systems, encryption, security policies.

ii) Detective Controls → Identify and detect security breaches or anomalies. For example, Intrusion Detection Systems (IDS), audit logs, CCTV, system monitoring.

iii) Corrective Controls → Respond to and fix issues after detection. For example, antivirus remove tools, system patches, incident response procedures.

iv) Deterrent Controls → Discourage attackers or policy violations. For example, warning signs, security awareness training, legal agreements.

v) Compensating Controls → Alternative measures used when standard controls aren't feasible. For example, manual monitoring when automated tools are unavailable, extra logging.

Name: _____ Regd No: _____

3) What is meant by CIA triad? Highlight its significance as a part of information security to work against cyber threat.

Ans → The CIA triad stands for Confidentiality, Integrity and Availability. It forms the foundation of information security and guides the implementation of security policies and controls.

i) Confidentiality → Ensures that data is accessible only to authorised users. Prevent unauthorised access or disclosure. Eg → Encryption, access control, data classification.

ii) Integrity → Ensures data is accurate, consistent and unaltered. Protect against unauthorised changes or tampering. Eg → Hash functions, checksums, version control.

iii) Availability → Ensures that data and systems are accessible when needed. Prevent downtime or denial-of-service. Eg → Redundancy, backups, disaster recovery plans.

Significance in Fighting Cyber Threats →

i) Comprehensive Protection → Covers all aspects of data security.

ii) Risk Mitigation → Helps identify vulnerabilities and apply suitable controls.

iii) Trust Building → Maintains the trust of users, customers and stakeholders.

iv) Compliance → Supports legal & regulatory requirements.

4) State the importance of non-repudiation and discuss its key aspects briefly in digital communication environment.

Ans → Importance of Non-Repudition in Digital Communication → Non-repudition ensures that a sender cannot deny having sent a message, and a reciever cannot deny having recieved it. It is crucial for trust, accountability and legal validity in digit communications.

Key Aspects →

i) Authentication → Verifies the identity of the sender and reciever. Ensures messages come from legitimate sources.

ii) Digital Signatures → Used to sign messages or documents. Provides proof of origin & content integrity.

iii) Timestamps → Record when a message was sent or recieved. Useful in ~~verif~~ verifying the exact time of a transaction.

iv) Logging and Auditing → Maintains records of communication events. Support evidence gathering and dispute resolution.

Name: _____ Regd No: _____

v) Encryption → Though not directly responsible for non-repudiation, it ensures message confidentiality and supports secure communication.

5) State the need of AAA protocol for remote access to the resources in computer network.

Compare and contrast various AAA protocols used in a secured network.

Ans→ Need for AAA protocol in remote access → AAA stands for authentication, authorization, and accounting. It is a framework used to secure remote access to resources in a computer network. AAA ensures that only verified users can access the network, have appropriate permissions and their activities are tracked.

i) Authentication → Verifies the identity of the user or device. Example → Username/password certificates.

ii) Authorisation → Determines what resources or services a user can access. Example → Access to specific files, commands or devices.

iii) Accounting → Tracks user activity for auditing and reporting. Example → Login time, accessed resources, data usage.

Comparison of Common AAA Protocols →

Feature	Radius	TACACS+	Diameter
Full form	Remote Authentication Dial in user service	Terminal Access Controller Access-Control System Plus	- success to RADIUS
Authentication	Combined with authorisation	Separate from authorisation	Supports advanced authentication
Encryption	Encrypts only the password	Encrypts entire packet	Encrypt entire communication
Transport	Uses UDP (connectionless)	Uses TCP (Reliable)	Uses TCP or SCTP.
Usage	Widely used for network access	Used in enterprise networks	Used in next-gen mobile/IP networks
Vendor Support	Open standard, widely supported	Cisco proprietary (but supported widely)	Standardized by IETF.

Name: _____ Regd No: _____

6) Differentiate between the role of Control plane & data plane to ensure a zero trust cyber-security.

Ans →

Aspect	Control Pane	Data Plane
Primary Role	Decision-Making	Data forwarding and execution
Function in Zero trust	Verifies identifies, enforces access policies	Transmits data only after approval from control plane
Processes	Authentication, authorization, policy evaluation	Packet switching, data routing, encryption
Visibility	Manages "who can do what & when"	Handles "how data flow"
Security Focus	Ensures only authenticated and authorized users get access	Secures data in transit, ensures compliance with policy
Example Tools	Identity providers, policy engines	Firewalls, VPNs, proxies, secure tunnels

7) Explain the use of followings associated with deception and disruption technique to strengthen the security in computer networking.

Ans → i) Honeypot →

Ans → A decoy system or server that mimics real services to attract attackers. To detect, deflect or study intrusion attempts. Helps identify new attack methods & gather intelligence without exposing real assets. Example → A fake SSH server set up to log brute-force login attempts.

ii) Honeynet → A network of interconnected honeypots designed to look like a real network. To observe coordinated attacks, study malware behaviour, and analyze attacker strategies. Offer deeper insights than a single honeypot by simulating realistic network interactions. Example → A fake enterprise network with email, database & file servers.

iii) Honeyfile → A deceptive file placed in a system to lure attackers. To detect unauthorised access or insider threats. Trigger alerts when the file is opened, moved or modified. Example → A file named "passwords.txt" on a shared drive with embedded monitoring.

Name: _____ Regd No: _____

iv) Honeytoken → A fake piece of data or credential that has no legitimate use. Acts as a trap to alert administrators when it's used. Detects data breaches or misuse when the token is accessed or sent outside. Example → A fake database entry with an email address - if it's ever used, it indicates data leakage.

8) Briefly highlight the importance of the following to successfully execute the change management process for mitigating the potential disaster effect.

i) Impact Analysis → Evaluates how the proposed change will affect systems, users & operations. Helps identify risks, dependencies and the scope of disruption, allowing better planning & risk mitigation.

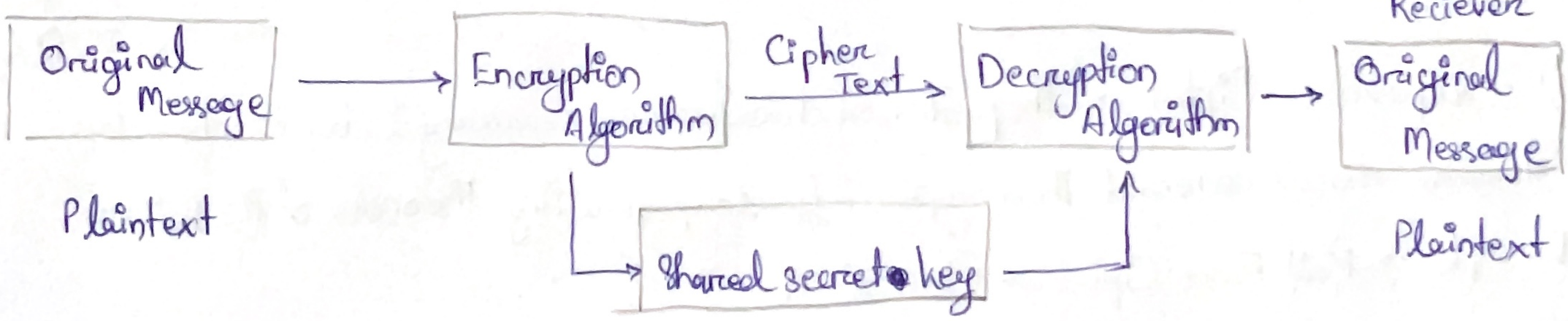
ii) Test Results → Provide evidence of how the change behaves in a controlled environment. Validates that the change works as intended and does not introduce new issues before going live.

iii) Back Out Plan → A predefined process to revert to the previous state if the change fails. Minimizes downtime and limits the impact of a failed implementation.

iv) Maintenance Window → A scheduled time to apply changes with minimal disruption to users. Reduces operational impact & ensures support staff are available in case of issues.

9) Compare symmetric and asymmetric encryption (with the help of a diagram), providing examples of each.

Ans → Sender

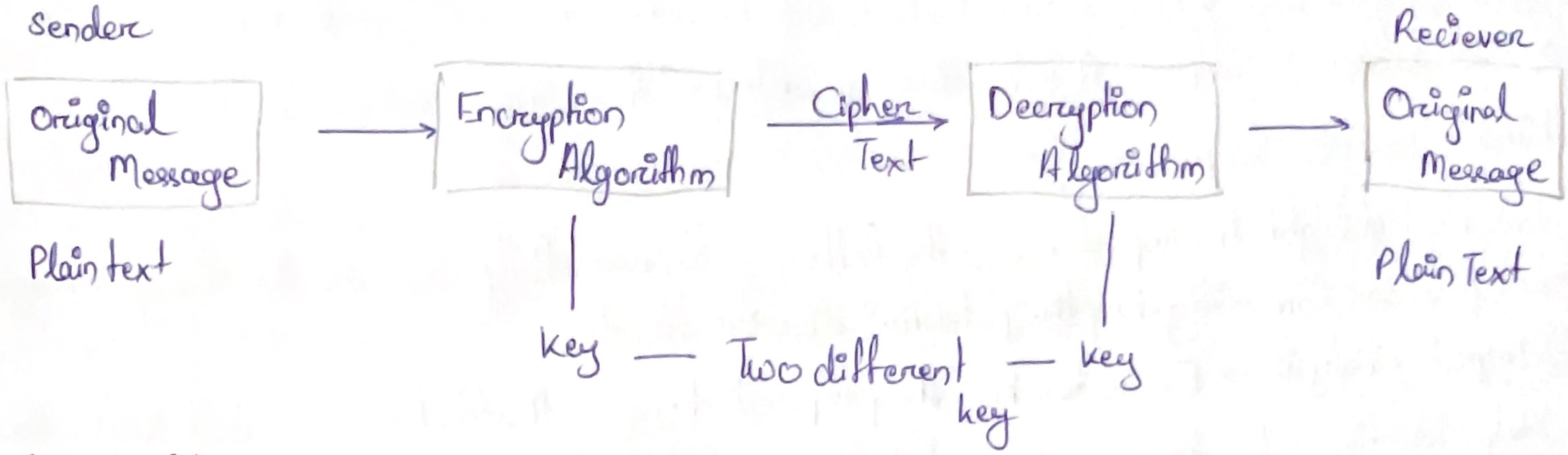


Symmetric Encryption

~~Uses~~ → A single key for both encryption & decryption. Faster, suitable for encrypting large amounts of data. Requires secure way to share the ~~secret~~ secret key.

Use cases → File encryption, secure backups.

Assymmetric key →



A pair of keys - public key (for encryption) and private key (for decryption). Slower, used for securing key exchanges and small data. Public key can be openly shared; private key is kept secret.

Use cases → Digital Signatures, secure email, SSL/TLS(HTTPS).

10) With the help of suitable example elaborate how substitution cipher is different from transposition cipher.

Ans → i) Substitution Cipher → Each character (or group of characters) in the plain text is replaced with another character or symbol. The positions remain the same, but characters are changed.

Eg → Ceaser Cipher (key = 3)

Plaintext → HELLO Encrypted (Shift +3) → KHOOR Explanation → H E LL O
+3 ↓ ↓ ↓ ↓ ↓
K H O O R

ii) Transposition Cipher → The position of characters are rearranged, but the characters themselves remain unchanged. The encryption is based on permutting the order of the letters.

Example → Rail Fence Cipher (key = 2)

Plaintext → HELLO Encrypted → HLOEL Explanation → H L O
E L

11) Encrypt the plaintext "TOMORROW" using the Playfair Cipher with the key "SECRET". Assume the letter I & J shares the same cell in the key matrix.

Ans → Key → SECRET

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

TO MO RX RO WX
EU IU CY EQ XY

Cipher Text → EUIUCYEQXY

Name: _____ Regd No: _____

12) Consider a playfair cipher with keyword "SECRET". Decrypt "ENGBNOHWSTEMEZY" which was formed using this cipher.

Ans→ Key → SECRET

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

Cipher Text → EN GN OH WS IE ME ZY

Decrypted → SO AU NI VE RS IT YX

↳ SOAUNIVERSITYX

13) Encrypt the plaintext "EXAMINATION" using the keyword "KEY", with the help of vignere cipher.

Ans → Plaintext → E X A M I N A T I O N
(4) (23) (0) (12) (8) (13) (0) (19) (8) (14) (13)

Keyword → K E Y K E Y K E Y K E
(10) (4) (24) (10) (4) (24) (10) (4) (24) (10) (4)

$C_i = (P_i + K_i) \bmod 26$

Cipher Text → O B Y W M L K X G Y R
(14) (1) (24) (22) (12) (11) (10) (23) (6) (24) (17)

14) What will be the plain text corresponding to cipher text "DYRYVGKP" if vignere cipher is used with keyword as "KEY"?

Ans → Cipher Text → D Y R Y V G K P
(3) (24) (17) (24) (21) (6) (10) (15)

Key → K E Y K E Y K E
(10) (4) (24) (10) (4) (24) (10) (4)

$D_i = (C_i - K_i) \bmod 26$

Decrypted Text → T U T O R I A L

15) An 8 bit data $(AC)_{Hex}$ is permuted using the permutation table as

7	3	1	5
6	4	8	2

Find the permuted output and the corresponding inverse permutation table which can be used to get the original 8 bit data.

Ans → AC (Hex) = 1010 1100 (Binary)

Permutation table = 7 3 15
6 4 8 2

Name: _____ Regd No: _____

Original 8-bit binary → 10101100

Position → 1 2 3 4 5 6 7 8

Applying permutation →

Output bit → 1 2 3 4 5 6 7 8

From input bit POS → 7 3 4 5 6 4 8 2

Input Bit value → 0 1 1 1 1 0 0 0

Permutated output → $(01111000)_{Binary}$ Hex: 78

Inverse permutation table →

Input → 1 2 3 4 5 6 7 8

Output → 3 8 2 6 4 5 1 7 → Inverse permutation.

16) Given the output of round 16 in DES as "0x0000 0002 0000 0080". Find the respective ciphertext.

Ans→ Given value → 0x0000000200000080

In binary → 00000000 00000000 00000000 00000010
00000000 00000000 00000000 10000000

R16 = 0x00000002

L16 = 0x00000080

So, FP on L16 || R16 = 0x00000002 0000080

So, output after FP = 0x0100000000000080

17) How many S boxes are used in DES? Given the elements of the 2nd row (i.e row no. "01") in a S box used in DES as 14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0 & 7. If the 6 bits input to the S box is "011011", determine the corresponding 4 bit output?

Ans→ DES uses 8 S-boxes, each transforming 6-bit input into 4 bit output.

Input to S-box → 011011

- First & last bits: 0 & 1 → form the row bits 01 (binary) = 1 (decimal)
- Middle 4 bits: 1101 → form the column bits → 13 (decimal)

Row 1 of S-box [14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7]

Value at row 1, index 13 → 9 → 1001 (binary) → 4 bit output.

1) Given the plaintext "SOAUNIVESITY" to AES 128 bit algorithm. If the 128 bit key used for encryption as (0202020202020202020202020202020202)$_{Hex}$, then

a) Show the original contents of state array, displayed as a 4x4 matrix.

Ans→ Plaintext → "SOA UNIVERSITY" → 13 characters → Pad with 3 null characters (00) to make 16 bytes.

ASCII values → SOA UNIVERSITY 0 0 0

53 4F 41 20 55 4E 49 56 45 52 53 49 54 59 00 00 00

Arrange column-wise (4x4 matrix)→

[53 55 45 54] ← Column 0
[4F 4E 52 59] ← Column 1
[41 49 53 00] ← Column 2
[20 56 49 00] ← Column 3

State array →
| 53 4F 41 20 |
| 55 4E 49 56 |
| 45 52 53 49 |
| 54 59 00 00 |

b) Show the value of state array after ~~round~~ initial Add Round key transformation.

Ans→ Key rewritten as bytes → All bytes are 0x02.

Perform bitwise XOR with 0x02→

53^02 = 51 4F^02 = 4D 41^02 = 43 20^02 = 22
55^02 = 57 4E^02 = 4C 49^02 = 4B 56^02 = 54
45^02 = 47 52^02 = 50 53^02 = 51 49^02 = 4B
54^02 = 56 59^02 = 5B 00^02 = 02 00^02 = 02

State array →
| 51 4D 43 22 |
| 57 4C 4B 54 |
| 47 50 51 4B |
| 56 5B 02 02 |

c) Show the value of state array after SubBytes transformation.

Ans→ AES S-box reference →

51 = row 5, column 1 → S-box[5][1] = E0

4D → BF 43 → 85 22 → 6B
~~49~~ 57 → F9 4C → B0 4B → A4 54 → F1
47 → B5 50 → C0 51 → E0 4B → A4
56 → F8 5B → FA 02 → 6F 02 → 6F

Name: _____ Regd No: _____

State Analysis → | EO BF 85 6B |
| F9 BO A4 F1 |
| B5 C0 E0 A4 |
| F8 FA 6F 6F |

d) Show the value of state arrray after ShiftRows transformation.

Ans → |EO BF 85 6B| ← Row 0 (No shift)
|F9 BO A4 F1| ← Row 1 (Shift left by 1 byte)
|B5 C0 E0 A4| ← Row 2 (Shift left by 2 byte)
|F8 FA 6F 6F| ← Row 3 (Shift left by 3 byte)

After shiftrows → |EO BF 85 6B|
|BO A4 F1 F9|
|E0 A4 B5 C0|
|6F F8 FA 6F|

19) What is meant by the term "hashing" in the field of cryptography? Justify, how hashing ensurees both data integrity and password security?

Ans → Hashing is a cryptographic process that converts input data (of any size) into a fixed-size string of characters, typically a sequence of hexadecimal digits. This output is called a hash value or digest. This output is called a hash value or digest.

How Hashing Ensurce →

i) Data Integrity → When data is sent or stored, its hash can be calculated. Later, the same hash function is applied again to the recieved or retrieved data. If the hash values match, the data has not been tampered with.

ii) Password Security → Instead of storing passwords in plaintext, systems store the hash of the password. During login, the entered password is hashed and compared to stored hash. Even if someone steals the database, they get only the hashes - not the actual passwords.

20) Discuss the role of blockchain as a modern technique to ensure a secure mode of data communication and recording highlighting the benefit of it.

Name: _____ Regd No: _____

Ans → a) Decentralisation →

i) No single point of failure; data is distributed across multiple nodes.

ii) Prevents unauthorised data manipulation or attacks on a central server.

b) Immutability →

i) Once data is recorded in a block and added to the chain, it cannot be altered or deleted.

ii) Ensures data integrity & trust.

c) Cryptographic Security →

i) Every block contains a cryptographic hash of the previous block, forming a secure chain.

ii) Unauthorized changes in any block break the chain, making tampering detectable.

21) State the significance of Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) associated with certificate validity process ensuring a secure interaction over internet.

Ans → i) Certificate Revocation Lists (CRLs) → A CRL is a digitally signed list, issued by a Certificate Authority (CA), that contains the serial numbers of certificates that have been revoked before their expiration date.

Significance → i) Prevents the use of compromised, misused or expired certificates.

ii) Provides a centralised method to check certificate revocation status.

iii) Enhance trust by ensuring only valid certificates are used in secure communications.

Limitations → It needs to be downloaded periodically, may not reflect real-time revocation status.

ii) Online Certificate Status Protocol (OCSP) → OCSP is a real-time protocol used to check the revocation status of a single certificate by querying the CA's OCSP responder.

Significance → i) Provides faster and more current certificate validation than CRLs.

ii) Reduces bandwidth and processing overhead by checking status individually.

iii) Enhances performances and responsiveness in secure systems.

Limitations → Depends on the availability and ~~reliability~~ reliability of the OSCP server.

22) How does the level of resources and level of sophistication influence the threat actor?

Ans→ i) Level ~~Re~~ of Resources → This includes financial backing, access to tools, man power & infrastructure.

a) Low Resources → • Use freely available tools or simple malware.
• Often script kiddies or amateur hackers.
• Perform basic attacks like phising, password guessing or defacement.

b) High Resources → • May have access to zero-day exploits, advanced malware or custom-built tools.
• Can afford long-term campaigns, infrastructure & expert personnel.
• Often associated with state-sponsered actors or organised cybercriminal groups.

ii) Level of Sophistication → This refers to technical expertise, planning, stealth and ability to adapt.

a) Low ~~Resources~~ Sophistication → • Use known vulnerabilities or publicly available exploits.
• Attacks are noisy and easily detected.
• Lack persistence or evasion techniques.

b) High Sophistication → • Conduct stealthy, targeted and well-known attacks.
• Employ techniques like Advanced Persistent Threats (APTs), polymorphic malware or lateral movement.
• Can evade detection and sustain long-term access.

23) Briefly describe the following concepts considered as motivations to build defence against cyberthreats.

a) Data Exfiltration → Unauthorised transfer or theft of sensitive data from a system or network. Attackers may steal personal, financial, or confidential business data for espionage, resale or competitive advantage. To protect privacy, intellectual property and comply with data protection laws.

b) Service Disruption → Intentional interruption or degradation of services. Disrupt business operations or create public embarrassment (often via DDoS attacks). To ensure availability & maintain customer trust & service continuity.

c) Blackmail → Extorting money or actions by threatening to ~~re~~release stolen or sensitive information. Financial gain (e.g. ransomware attacks demanding payment). To prevent financial

losses, reputational damage and legal complications.

d) Revenge → A personal or emotional motive, often by insiders or former employees. To harm or retaliate against an individual or organisation. Insider ~~threats~~ threats can be highly damaging and are often harder to detect.

24) Define "supply chain" in the context of cybersecurity with a comparison among different parties involved in this & explain why its important.

Ans→ In cybersecurity, a supply chain refers to the entire network of external vendors, service providers, contractors, software suppliers and partners that interact with an organisation's systems, software ~~suppliers~~ or data. Each party in this chain can pose a potential security risk if not properly managed.

Key parties involved & Comparison →

Party	Role in Supply Chain	Risk levels	Example Threats
Manufacturers	Provide hardware components	Moderate to high	Malicious chips, firmware vulnerabilities
Software vendors	Provide apps, OS, plugins, etc.	High	Infected updates, backdoors
Service Providers	Offer IT, cloud or security services	High	Misconfigurations, insider threats
Distributors/ Resellers	Handle storage and delivery of tech products	Medium	Tampering during shipping
Third-Party Contractors	Temporary staff or outsourced teams with system access	High	Unauthorised access, data leaks

Why its important →

i) Expanded Attack Surface → Each third-party increases the number of potential entry points for attackers.

ii) Trust doesn't equal security → Even trusted vendors can be compromised - security must extend beyond your own perimeter.

iii) Regulatory Compliance → ~~Organisers~~ Organizations are often held accountable for data breaches caused by their suppliers.

25) Briefly explain the following techniques associated with attacks made using human psychology.

i) Phising → A deceptive attempt to trick individuals into revealing sensitive information (like passwords or credit card numbers) by posing as trustworthy entity, usually via email or messages. Plays on urgency, fear or curiosity to manipulate victims. For e.g., an email claiming to be from a bank asking to verify your account.

ii) Misinformation → The deliberate spread of false or misleading information to influence opinions or cause confusion. Exploits trust in sources or social proof to manipulate behaviour or beliefs. For e.g., fake news shared on social media to sway public opinion or cause panic.

iii) Brand impression → Attackers mimic a legitimate company's brand (logo, emails, websites) to trick users into interacting with malicious content. Leverages trust in well-known brands to lower skepticism. For e.g., a fake login page that looks like a real microsoft or Google portal.

iv) Typosquatting → Registering misspelled or similar-looking domain names of popular websites to trick users who mistype URLs. Relies on user error and assumptions that a familiar-looking site is genuine. For e.g., a site like amazOn.com that imitates Amazon to steal login details.

Name: _____ Regd No: _____