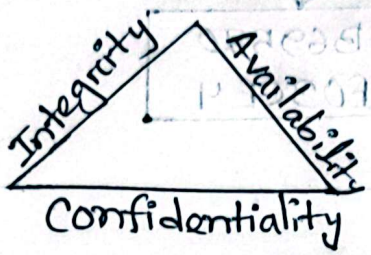
1. CIA Security Goals :

The goals of CIA Triod are Confidentiality, Integrity, and availability which are basic factors in information security.



Confidentiality :

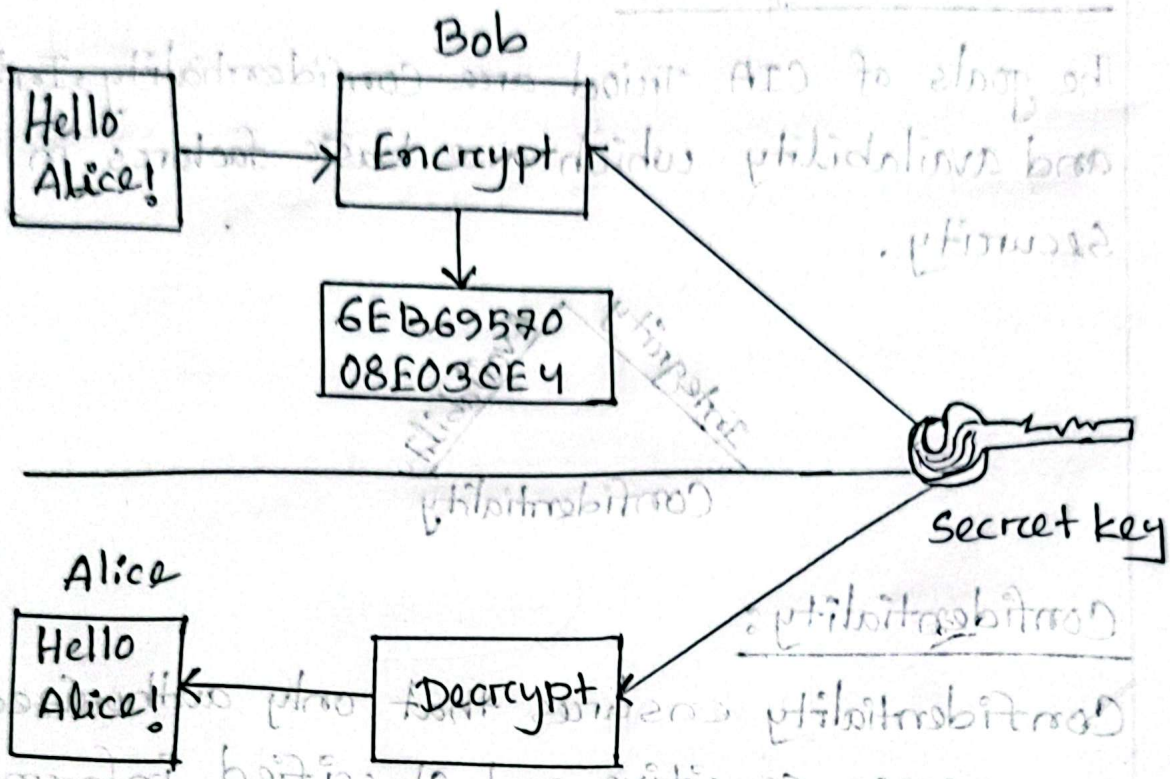
Confidentiality ensures that only authorized individual can access sensitive and classified information.

Data transmitted over a network must be protected from unathorized access.

Attackers may attempts to intercept this data using various tools available on the internet.

To prevent this, a key strategy is to use encryption Techniques. Encryption helps secure data so that, even if an attacker gain access, they will not be able to understand or misuse it.

Another way to protect our data is through a VPN tunnel.



Integrity:

The concept of integrity ensures that data has not been altered or tampered with. If data is corrupted or modified without authorization, it indicates a loss of integrity.

To verify whether data has remain unchanged, we use hash functions. These functions generates a unique value for the original data. If the data is changed, even slightly, the resulting hash will be changed.

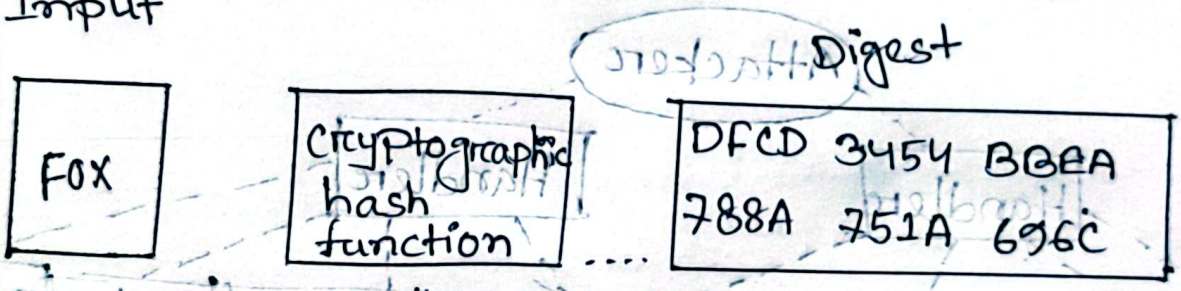
Two commonly used hash functions are:

i. SHA (Secure Hash Algorithm)

ii. MD5 (Message Digest 5)

MD5 generates a 128 bit hash value and widely used to vercify data integrity.

and SHA is a 160-bit hash if we're using SHA-1.



Availability:

Availability means that the network and its resources should always be accessible to authorized users. This applies to both systems and data.

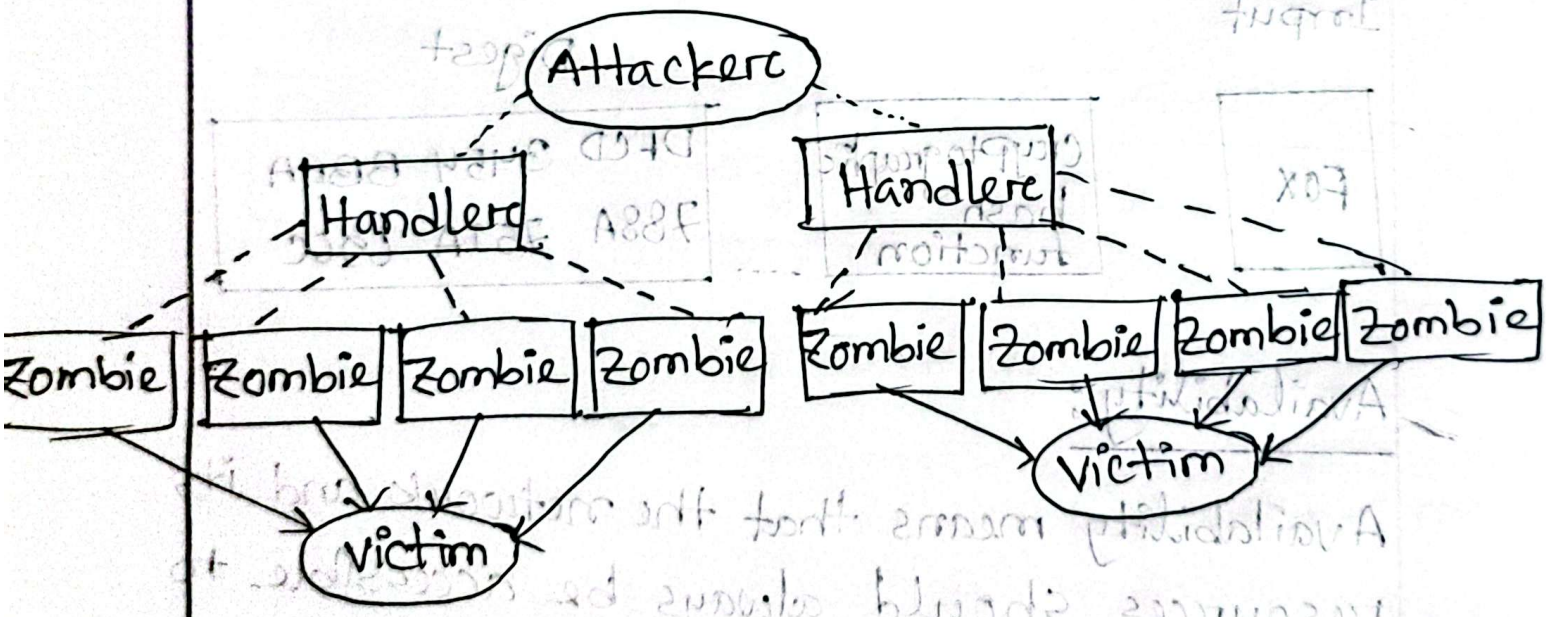
To maintain availability, network administrators should:

i. Regularly maintain hardware.

ii. Perform timely upgrades.

iii. Have contingency plans for available failover situation.

iv. Eliminate or minimize network bottlenecks. Threats like DoS (Denial of service) or DDoS (Distributed Denial of service) attacks can disrupt availability by overwhelming the network, leading to exhaustion of resources and denial of access to legitimate users.



Types of cyber attacks:

1. Malware:

- Malicious software like viruses, worms, trojans, ransomware and spyware.
- Can steal, delete or encrypt data or damage system.

2. Phishing:

- Fake emails or messages that trick users into giving away sensitive info (like passwords or credit card numbers).

3. Denial of service (DOS/Distributed Dos (DDoS)

- Overwhelms a system, servers, or network with traffic to make it unavailable.

4. Man in the middle Attack (Mi+M):

- An attackers intercepts communication between two parties to steal or manipulate data.

5. SQL injection :

- Attackers insert malicious SQL code into a database query to access or modify data.

6. Zero-day-Exploit :

Attacks that exploit unknown vulnerabilities before a patch or fix is released.

7. Credential stuffing :

Using stolen usernames/passwords from one service to break into other accounts.

8. Brute force Attack :

Trying many password combinations until the correct one is found.

9. Cross-site Scripting (XSS) :

Injecting malicious scripts into webpages viewed by others, often used to steal session cookies.

10. Ransomware :

A type of malware that encrypts data and demands or ransom for its release.

Symmetric key Encryption:

Symmetric key encryption is a type of encryption where the same key is used to both encrypt and decrypt the data.

How it works:

1. The sender encrypts the message using a secret key.
2. The encrypted message (ciphertext) is sent to the receiver.
3. The receiver users the same secret key to decrypt the message back to it's original form.

Asymmetric key Encryption:

Assymmetric key encryption is a type of encryption that uses two different keys: a public key & a private key.

How it works:

1. The public key is shared with everyone.
2. The private key is kept secret by the owner.
3. If someone encrypts a message with the public key.