1. What are the three goals of cybersecurity?

i. Confidentiality: Cybersecurity ensures that sensitive information is accessed only by authorized individuals or systems. it involves protecting data from unauthorized access or disclosure through measures like encryption and authentication.

ii. Integrity: Cybersecurity maintains the accuracy and consistency of data over its entire lifecycle. It means preventing unauthorized modification, deletion, or corruption of data.

iii. Availability: Cybersecurity ensures that information and resources are accessible to authorized users when needed. This involves protecting systems from disruptions, such as cyberattacks, hardware failures etc through measures like backups and disaster recovery plans.

2. Explain social engineering as a form of security breach

Social engineering is a form of security breach that relies on manipulating human psychology rather than exploiting technical vulnerabilities. It involves tricking individuals into releasing sensitive information, granting unauthorized access, or performing actions that compromise security. These attacks exploit natural human traits such as trust, curiosity, fear, or a \*\*desire to help\*\*, making them highly effective and difficult to detect.

Characteristics of Social Engineering:

1. Human-Centric

2. Deceptive

3. Exploits Emotions

4. Highly Adaptable

3.What is MFA

MFA is a security system that requires users to provide two or more forms of verification before granting access to an account, system, or application. It adds an extra layer of security beyond just a username and password, making it significantly harder for attackers to gain access.

4. what is the difference between symmetric and asymmetric key encryption?

1. Symmetric key encryption uses one key for both encryption and decryption while Asymmetric key encryption uses a public key for encryption and private key for Decryption.
2. In symmetric key encryption, the same key must be shared between the sender and receiver while in Asymmetric, key The public key can be shared openly, while the private key must remain secret.
3. Symmetric key encryption is faster and more efficient for encrypting large amounts of data while Assymetric key encryption is slower and computationally more intensive than symmetric encryption.

5. What is a hashing function?

A hashing function is a mathematical algorithm that takes an input (or "message") and produces a fixed-size string of characters, which is typically a hash value or digest. The output is unique to the input data, meaning even a small change in the input will produce a significantly different hash. Hashing functions are widely used in cryptography, data integrity verification, and data indexing.