**Assignment for module 1**

1. Encryption is the process of encoding data to be read only by someone with the means to return it to it’s original state.
2. Encryption is daily used when we are on the internet to provide secure communication or shopping online.
3. If encryption is not used, there can be data theft, privacy violations, identity theft, data tampering, financial loss, compromised communication channelsetc.
4. **Advantages of symmetric encryption:**

i. Symmetric encryption is generally faster and requires less computational resources compared to asymmetric encryption.

ii. Symmetric encryption involves using the same key for both encryption and decryption, simplifying the encryption process.

iii. Symmetric encryption can scale efficiently to secure communication between multiple parties.

iv. Symmetric encryption algorithms often include features to ensure data integrity, meaning that any tampering with the encrypted data can be detected.

1. **Advantages of asymmetric encryption:**
2. Uses a public key and private key
3. Solves the problem of secure key exchange
4. Most often used to establish a secure internet connection.
5. End-to-end encryption (E2EE) is a method of secure communication that ensures that only the communicating users can read the messages. In E2EE, data is encrypted on the sender's device, remains encrypted as it travels across the communication channel, and is decrypted only on the recipient's device. This means that the communication service provider (such as a messaging app) cannot decrypt the messages, ensuring that even if the provider's servers are compromised, the messages remain unreadable to anyone except the intended recipients. End-to-end encryption is considered a safe method for security and privacy because it provides strong protection for sensitive data and communications, ensuring confidentiality, data security, trust, compliance, and protection against surveillance.