Pir Mehr Ali Shah

**Arid Agriculture University, Rawalpindi**

**University Institute of Information Technology**

Course Code.: **CS-597** Course Title: **Cyber Security**

Degree: **BSIT** 8B (Evening) Date: **05-May-2023**

**Class Task**

You work for a company that handles sensitive information, such as financial data and personal information of clients. The company wants to implement a secure communication system between its employees and clients, to ensure the confidentiality and integrity of the information exchanged. The company's IT department recommends using symmetric and asymmetric cryptography to secure the communication.

**Questions:**

1. Explain how symmetric cryptography can be used to secure the communication between employees and clients.
2. What is the key difference between symmetric and asymmetric cryptography?
3. How can asymmetric cryptography be used in addition to symmetric cryptography to enhance security?
4. What is the process of creating a secure communication channel using symmetric and asymmetric cryptography?

**Solution:**

Symmetric cryptography can be used to secure the communication between employees and clients by encrypting the data using a shared secret key that is only known to the parties involved in the communication. The encrypted data can only be decrypted using the same key, which ensures the confidentiality and integrity of the data.

The key difference between symmetric and asymmetric cryptography is that symmetric cryptography uses the same key for both encryption and decryption, whereas asymmetric cryptography uses two different keys, a public key and a private key.

Asymmetric cryptography can be used in addition to symmetric cryptography to enhance security by using the public key to securely exchange the shared secret key used in symmetric encryption. This process is called key exchange, and it