Information Security lab Assignment

Raja Umer Saleem (2023-cs-609)

Q#1

**End-to-End Encryption:**

This is a security method that can be written as E2EE. In this method, the message encryption occurs before sending it to the receiver. On the receiver side, the encrypted message is decrypted into original form. So, in this condition data is encrypted and inaccessible to the attackers.

Q#2

**Public Key:**

It is openly shared in public for data encryption. Anyone can use this to encrypt their data by this key.

**Private Key:**

It is private and remains secret by the organization and person. The encryption where takes place by the public key.

Q#3

**Different methods of encryption:**

**There are numerous methods some are:**

* Hash Functions
* Stream Ciphers
* Block Ciphers
* Asymmetric Key Encryption
* Symmetric Key Encryption

Q#4

**Software in real life?**

**There are several types of apps examples:**

* **Messaging Apps:** WhatsApp –use EE2E
* **Email Apps:** Proton mail –use EE2E
* **File Storage Apps:** Google Drive

Q#5

**Popular techniques of Encryption:**

* Advanced Encryption Standard (AES):
* Secure Hash Algorithm (SHA)
* ChaCha20
* Blow Fish