#6

1.TLS, or Transport Layer Security, secures web communication by encrypting data transmitted between a client (like a web browser) and a server, ensuring confidentiality and integrity. It also verifies the identity of the server, preventing man-in-the-middle attacks. This is achieved through a handshake protocol that establishes a secure connection using digital certificates, cryptography, and public key infrastructure (PKI).

Its importance is in prevention of data interception, verification of server identity and maintaining data integrity.

2. The TLS handshake is a process that establishes a secure communication channel between a client and a server, typically used to secure web traffic (HTTPS). It involves several steps where the client and server exchange messages to authenticate each other and agree on encryption algorithms and session keys. This process ensures that only the intended parties can communicate securely, preventing eavesdropping and tampering.