How TLS work?

Tags	Tools
Created time	@April 23, 2023 5:21 PM
Last edited time	@April 23, 2023 5:21 PM

here's a step-by-step explanation of how the Transport Layer Security (TLS) protocol works, including the roles of the session key, private key, and public key:

1. Client Hello: The TLS handshake begins with the client (such as a web browser) sending a "Client Hello" message to the server it wants to connect to. This message includes information about the client's capabilities and preferences for the TLS connection.
2. Server Hello: The server responds with a "Server Hello" message, which includes information about the TLS version being used and the security parameters for the connection. This message also includes the server's digital certificate, which contains its public key.
3. Certificate Verification: The client verifies the server's digital certificate by checking its validity and authenticity. This involves checking the certificate's digital signature and verifying that it was issued by a trusted Certificate Authority (CA).
4. Client Key Exchange: The client generates a session key, which is a randomly generated symmetric encryption key that will be used to encrypt and decrypt data transmitted over the connection. The client encrypts the session key with the server's public key from the certificate and sends it to the server.
5. Server Key Exchange: The server receives the client's session key and decrypts it with its private key. The server may also send its own session key, depending on the selected cipher suite and key exchange algorithm.
6. Change Cipher Spec: Both the client and server agree to switch to using the newly established session key for all further communication.
7. Encrypted Data Transfer: From this point on, all data transmitted between the client and server is encrypted using the shared session key. The symmetric encryption

algorithm and parameters are negotiated during the handshake and are agreed upon by both parties.

8. Session Termination: When the TLS session is complete, either the client or server may initiate a session termination by sending a "close notify" alert message. This message indicates that the session is ending and that no further data will be transmitted over the connection.

Overall, the TLS protocol provides a secure means of establishing an encrypted connection between two parties, using a combination of symmetric and asymmetric encryption, and key exchange algorithms. The session key is used to protect the confidentiality of data transmitted over the connection, and the public-private key pair is used to establish a secure channel for exchanging the session key and verifying the authenticity of the parties involved.