***TLS / SSL Handshake process***

***Step 1:***

***Client messaging: Client sends a message to server.***

* ***List of crypto ciphers***
* ***Client random number and data compression methods***

***Step 2:***

***Server Messaging: Server replies with the below information***

* ***Supported crypto ciphers***
* ***Public Key***
* ***Server certificate***

***Step 3:***

***Certificate validation and authenticity check:***

* ***Client checks the validity of certificate from the server***
* ***Generates a pre-master key***
* ***Pre-master key encrypted with server public key (step 2)***
* ***Sent to server***

***Step 4:***

***Key Exchange:***

* ***Server decrypts premaster key using private key (default in server)***
* ***Using premaster key -> server generates (computes) the master key***

***Step 5:***

***Finishing the handshake***

* ***Server sends a finished message encrypted with the master key***
* ***Client decrypts the message using its own computed master key***
* ***Symmetric encryption happens from here***
* ***Both client and server use same master key.***

***(Note: Client also generates the master key on its own using the premaster key)***

***Type of encryption used:***

1. ***Asymmetric encryption -> During Key exchange process***
2. ***Symmetric encryption -> After master key generation***

***(Master key computed by client and server using same computation methods, but master key is not exchanged )***