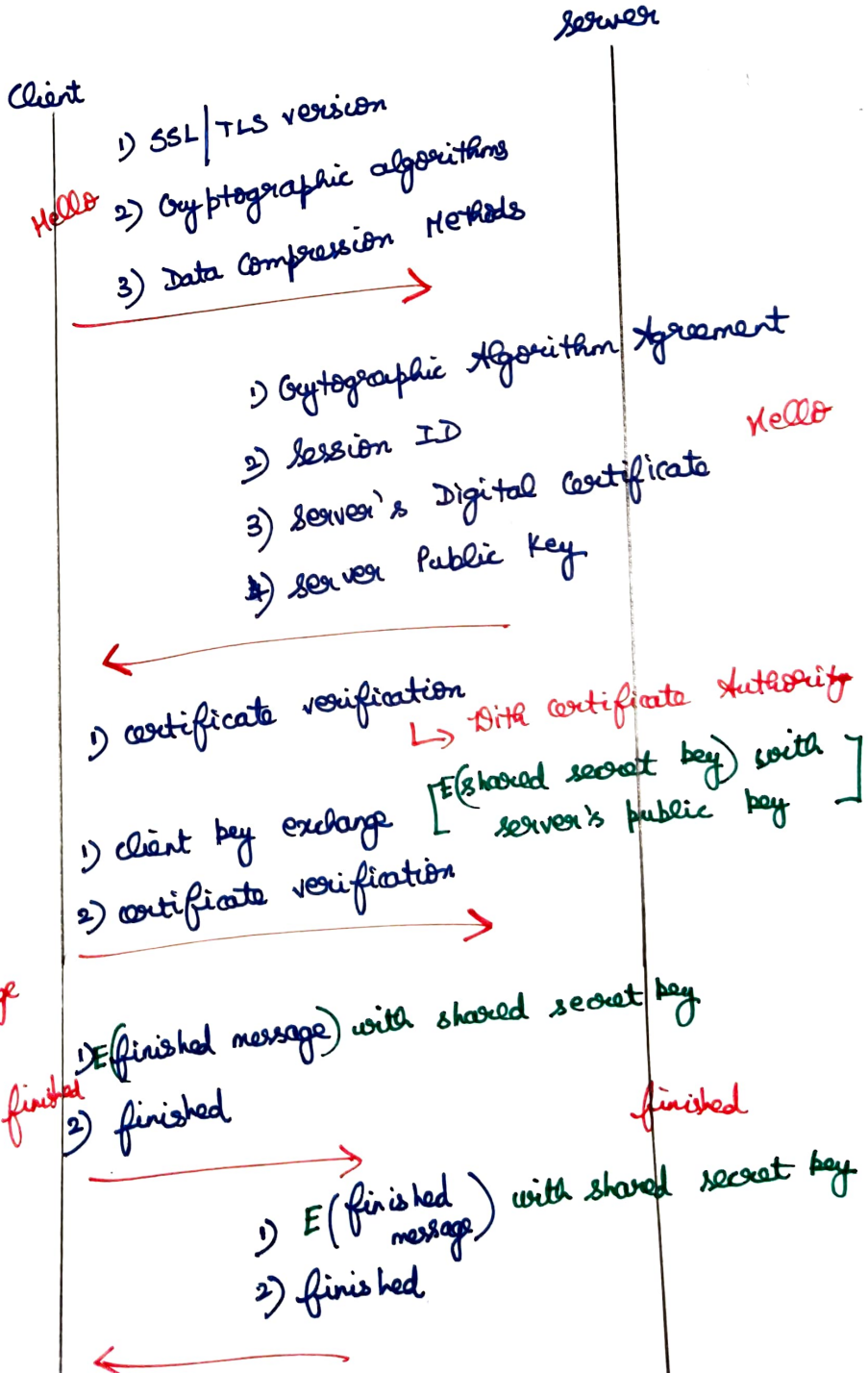
SSL Handshake Protocol

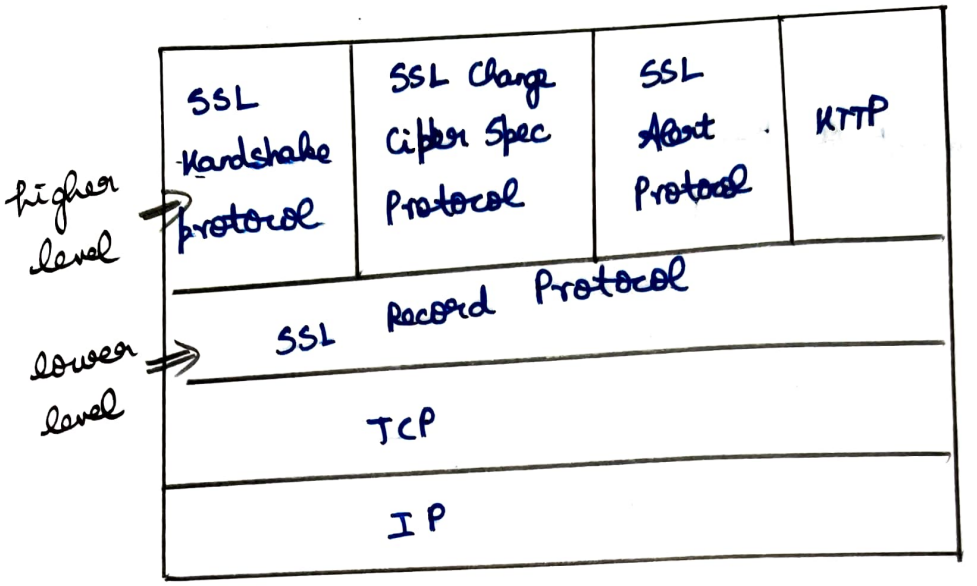
*) Most complex part of SSL

Allows server & client } to authenticate each-other and negotiates
- ↳ encryption
- ↳ MAC Algorithms
- ↳ Cryptographic Keys

*) This is used before an application data is sent.



SSL Protocol Stack



SSL Change Cipher spec Protocol } Notifies the receiver that all the subsequent packets are to be protected based on negotiated cipher suite & key

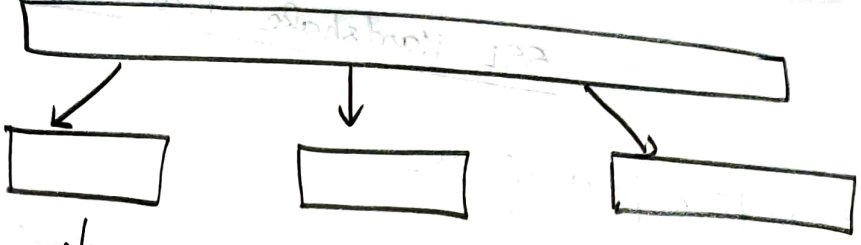
SSL Alert protocol } *) ~~Sends~~ Sends the alert messages to the receiving party.

*) Alert Message
↓ contains
Alert security level & a description

SSL Record Protocol

- Confidentiality
  - Conventional Method
- Message Integrity
  - MAC Address

Application Data



Fragments

Compress

Add MAC

MAC is added using secret key.

Encrypt

Encryption via Symmetric Encryption

Append

SSL Record Protocol