① There are two main protocols :

1) The handshake protocol

Hand shake protocol is used to establish seassions. This protocol allow client & servers to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle :

1) Client & server sends hello packets to each other.
2) Server sends his certificate and server key.
3) Client reply by sendig its certyficate and client enchange key.
4) Change cipher suit, after the handshake protocol ends.

2) The record layer protocol

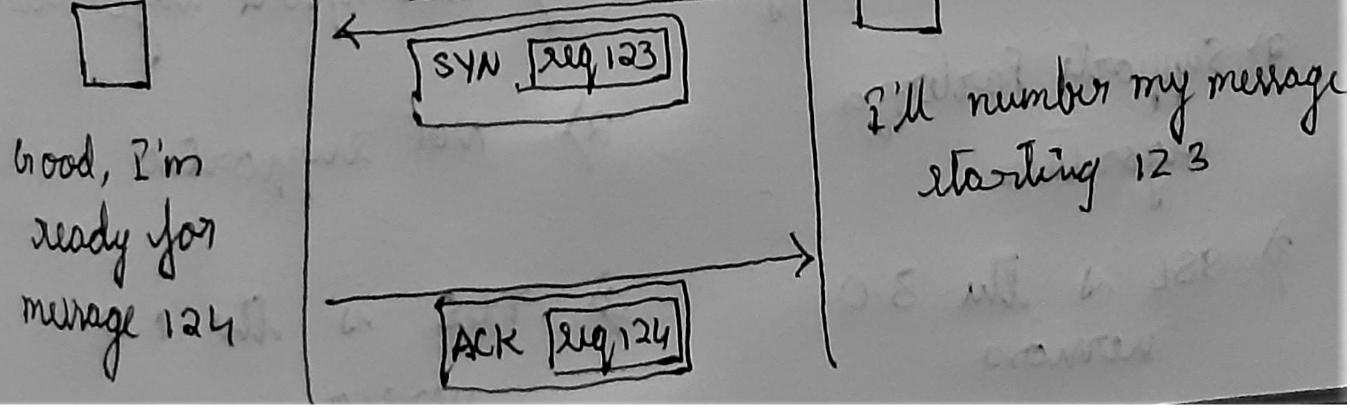
SSL record provides two services

- Confidentiality
- Message integrety

Here, data is divided into fragments. The fragments is compressed and the encrypted MAC generated by algorithms like SHA & MD5 is appended.

After the encryption is done ~~and~~, SSL header is appended to the data.

② Three way hondshaking



Lets connect, my message starting at 465
①
SYN
seq 465
Got it
ACK
seq 456
SYN
seq 123
I'll number my message starting 123
Good, I'm ready for message 124
ACK
seq 124

Two way handshaking only allow one party to establish initial sequence number and other party ACK it. Which means only one party can send data reliably.

But TCP wants to be able to send data reliably in both directions. Hence both parties need to establish an initial sequence number and ACK respectively.

③

SSL	TLS
1) Secure Socket Layer	1) Transport layer Security
2) Supports Fortezza algorithms	2) Not supported
3) SSL is the 3.0 version	3) TLS is the 1.0 version

4) Digest is used	4) Pseudo random functions is used
5) MAC protocol is used	5) Hashed message auth. protocol is used
6) complex	6) simple