Q1. Enlist all the protocols on SSL

Ans. The protocols on SSL are:-

1. TLS protocol
2. Handshake protocol
3. Alert protocol
4. SSL handshake protocol
5. FTP

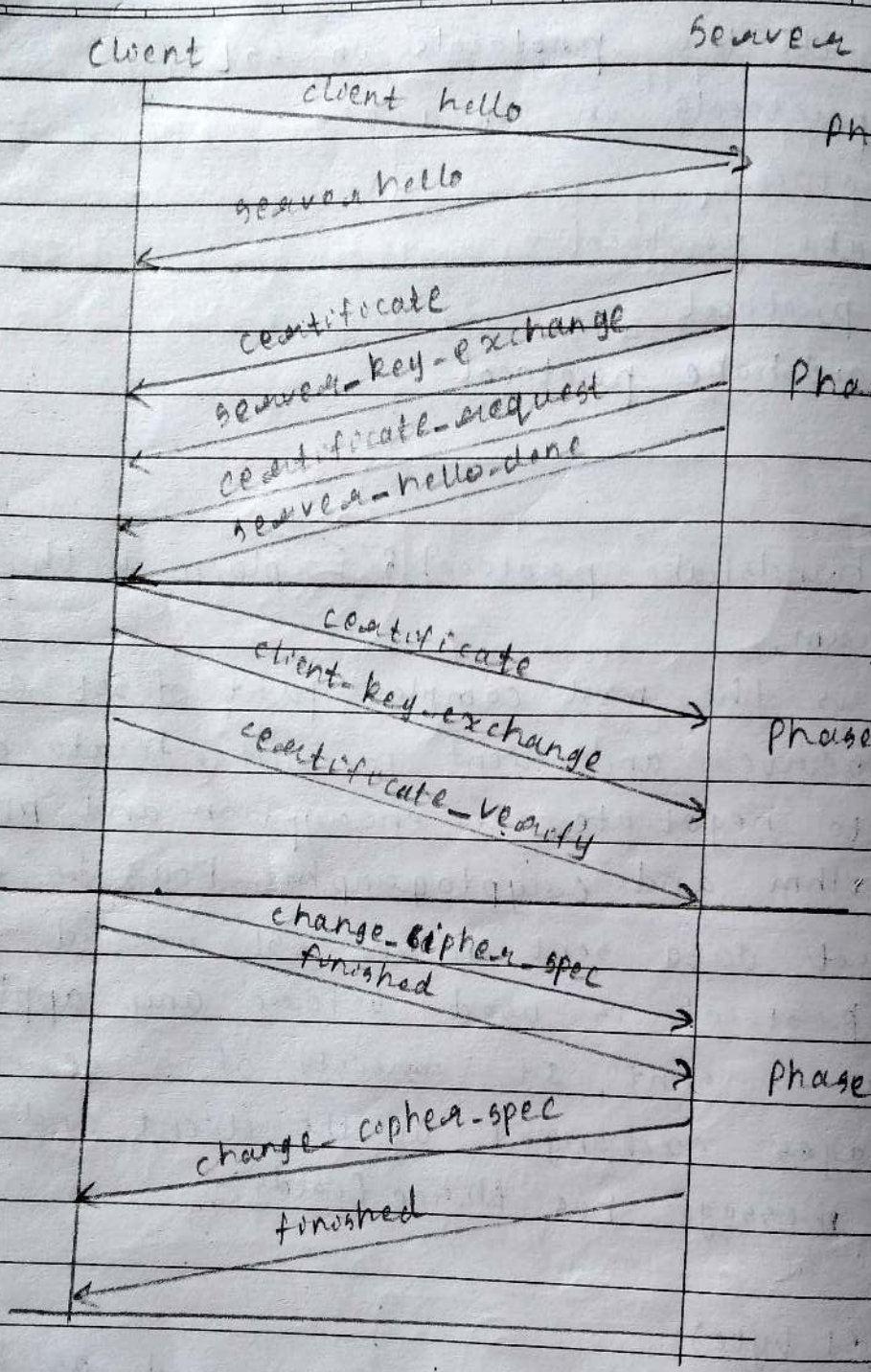
Q2. How handshake protocol? Explain with suitable diagram.

- This is the most complex part of SSL and allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record.
- This protocol is used before any application data is sent. It consists of a series of messages exchanged by the client and server.
- Each message has three fields:-

1. Type (1 byte):
- Indicates one of 10 messages such as "hello request"

2. Length (3 bytes):
- The length of the message in bytes.

3. Content (≥ 0 byte):
- The parameters associated with this message such as version of SSL being used.



Handshake Protocol