Rebecca Dias
182027/19

TE CMPN A

Rebecca

CSS - IAT-2

Q2) B)

① The SSL/TLS handshake involves a series of steps through which both the parties client and server, validate each other and start communicating through the secure SSL/TLS tunnel.

② A TLS handshake takes place whenever a user navigates to a website over HTTPS and the browser first begins to query the ~~the~~ websites origin server

③ During the course of a TLS handshake, the client and server together will do the following

i) Specify which version of TLS will be used

ii) Decide on which cipher suites they will use

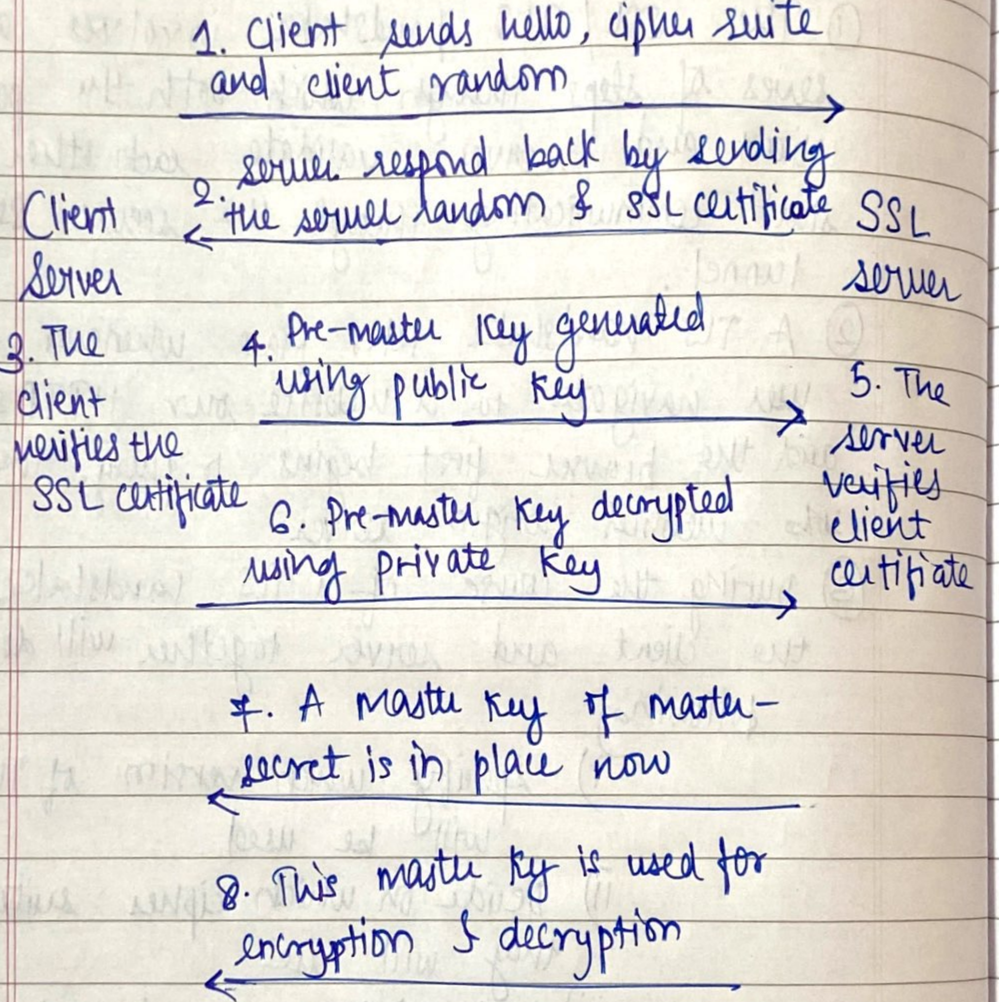
iii) Authenticate the identity of the server via the servers public key and the SSL certificate authoritys digital signature

iv) Generate session keys in order to use symmetric encryption after the handshake is complete.

Rebecca Dias
182027/19

classmate
Date
Page

Rebecca


1. Client sends hello, cipher suite and client random
2. server respond back by sending the server random & SSL certificate
Client Server
SSL server
3. The client verifies the SSL certificate
4. Pre-master key generated using public key
5. The server verifies client certificate
6. Pre-master key decrypted using private key
7. A master key of master-secret is in place now
8. This master key is used for encryption & decryption

SSL HandShake process.