CSA0735

COMPUTER NETWORK

UNIT - 5

ASSIGNMENT 5

S. MOHAMED SEED THOWFIQ
192511178
COMPUTER NETWORK
DR. RAJARAM.

Scenario : An e-commerce site enforces HTTPs on all user transcantion

Parameter : 10,000 session/day, 0.2 SSL.

Question:

a) Describe SSL/TLS hand shake Steps.

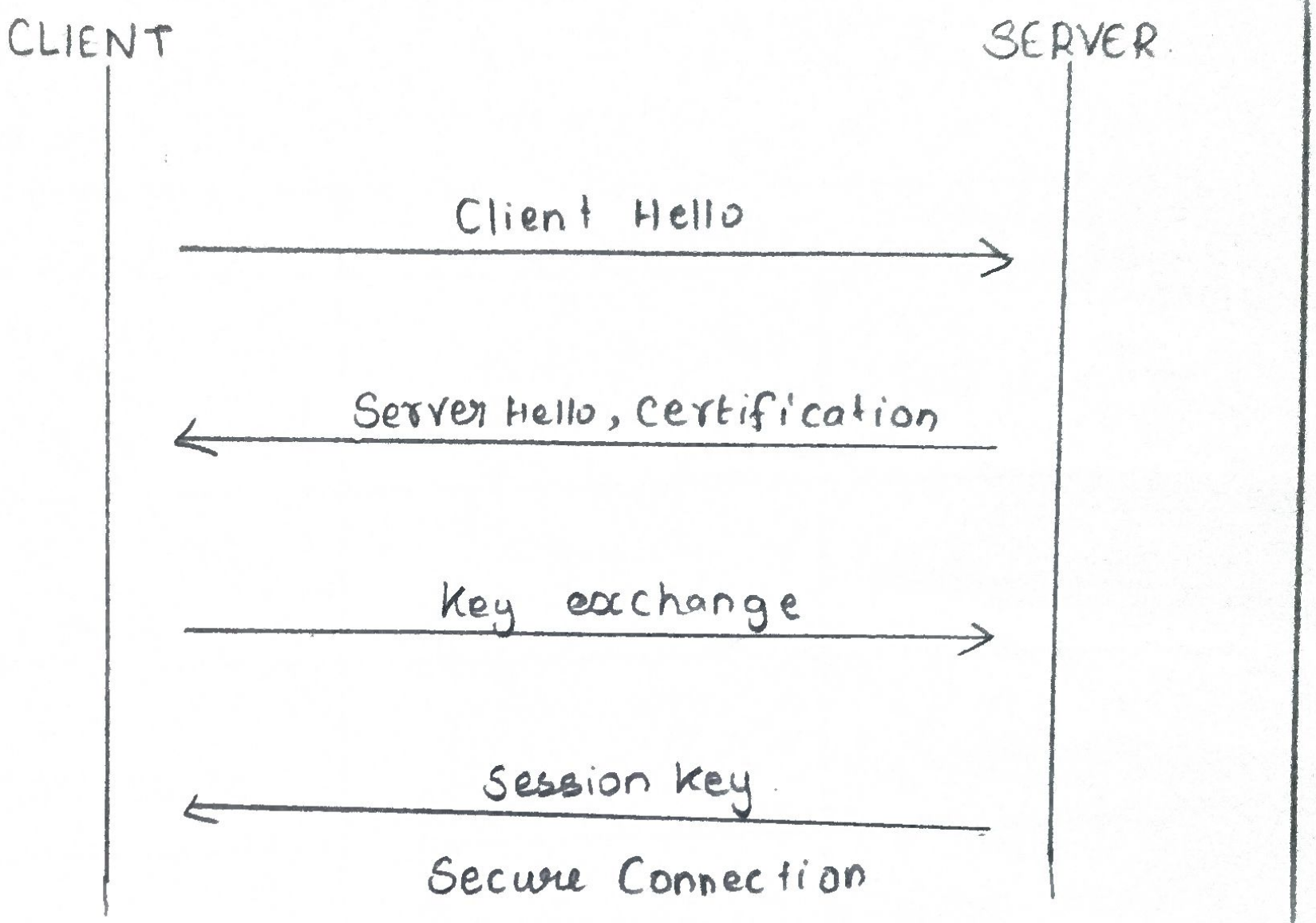
Ans: ↳ Client Hello : Browser says hello, I Shares encryption option.

↳ Server Hello : Server replies, Shares its certificate (identity).

↳ Key Exchange : Browser send a Secret (encrypted)

↳ Session key : Both Sides Create by the same secret key.

↳ Secure Connection : They Confirm, and Secure Communitcation begins.



b) Total Hand Shake Time per day.

↳ 10,000 Sessions x 0.2 Seconds

= 2000 Seconds.

↳ 2000 Seconds = 33.3 minutes.

The Server spends about 33.33 minutes/day on SSL Hand Shake.

c) Full Hand Shake VS Session Race.

Ans:

Feature	Full Hand Shake	Session Reuse.
Time	0.2 sec	~ 0.02 sec
Speed	Slower	Much faster
CPU usage	High	Low
Use Case.	New user	Repeat user.

Session reuse is faster because it skips full steps and reuse. earlier session info.

d) How to improve SSL Performance.

↳ Use session reuse (makes hand shakes faster).

↳ USE TLS 1.3 (faster and safer)

↳ Enable OCSP stapling (speeds up Certificate checks).

↳ Use hardware SSL offloading (less load on server)

↳ Use CDNs or edge servers (closer to user).

↳ Use faster Certificates (like ECC)