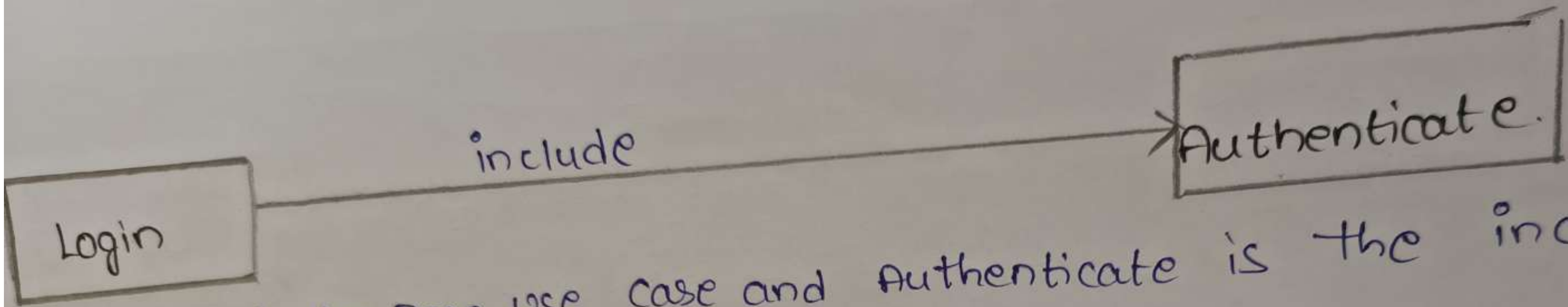
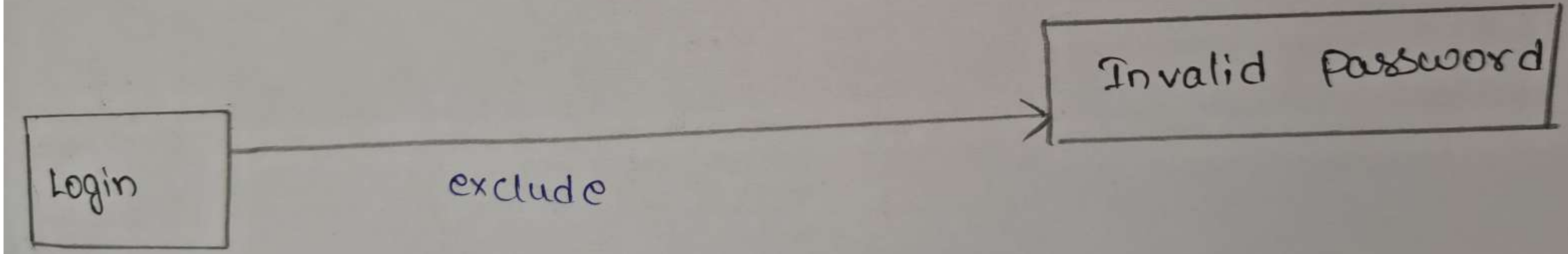


LOGIN is the Base use case and Authenticate is the include use case!



In LoGin is the Base use case and invalid Password is the Extended use CASE

4Q) Recommend session reuse mechanism?

A)

1. TSL- Level session Resumption

- TLS 1.3 uses resumption PSKs to resume previous
- Enable resumption PSK's for performance, but avoid (or) severly
- key management Rotate the resumption PSKs for performance

2. Session Tickets - RFC5077

- Server issue encryption Session tickects to the client
- use strong authentication encryption to protect ticket contents

3. session ID's

- Expiration and inactivity time outs
- Server-side invitation
- Rate limiting for resumption

2Q. If the hand shake adds 500ms delay per session calucu late daily delay for 10,000. sessions

A.

- Hand shake delay = 500ms

  = 0.5 second

- Numbers of sessions per day = 10,000

Total delay = hand shake delay x number of sessions

= 0.5 x10,000

= 5,000 sec

- convert into 8minutes|hours

= 5000/60

= 1 hour 23 minutes

Computer Networks

Assignment - 5

Name : D·Nagababu

code : CSA 0735

Rg No : 19252 5228

Branch : Btech AI & ML

36) SSL Certificates and public key usage.

A.

1. SSL Certificates :-

- An SSL certificate is a digital credential issued by a trusted Authority

- It contain :

→ The server's public key

→ domine name

→ CA digital signature

→ validity period.

2. Public key ussage :

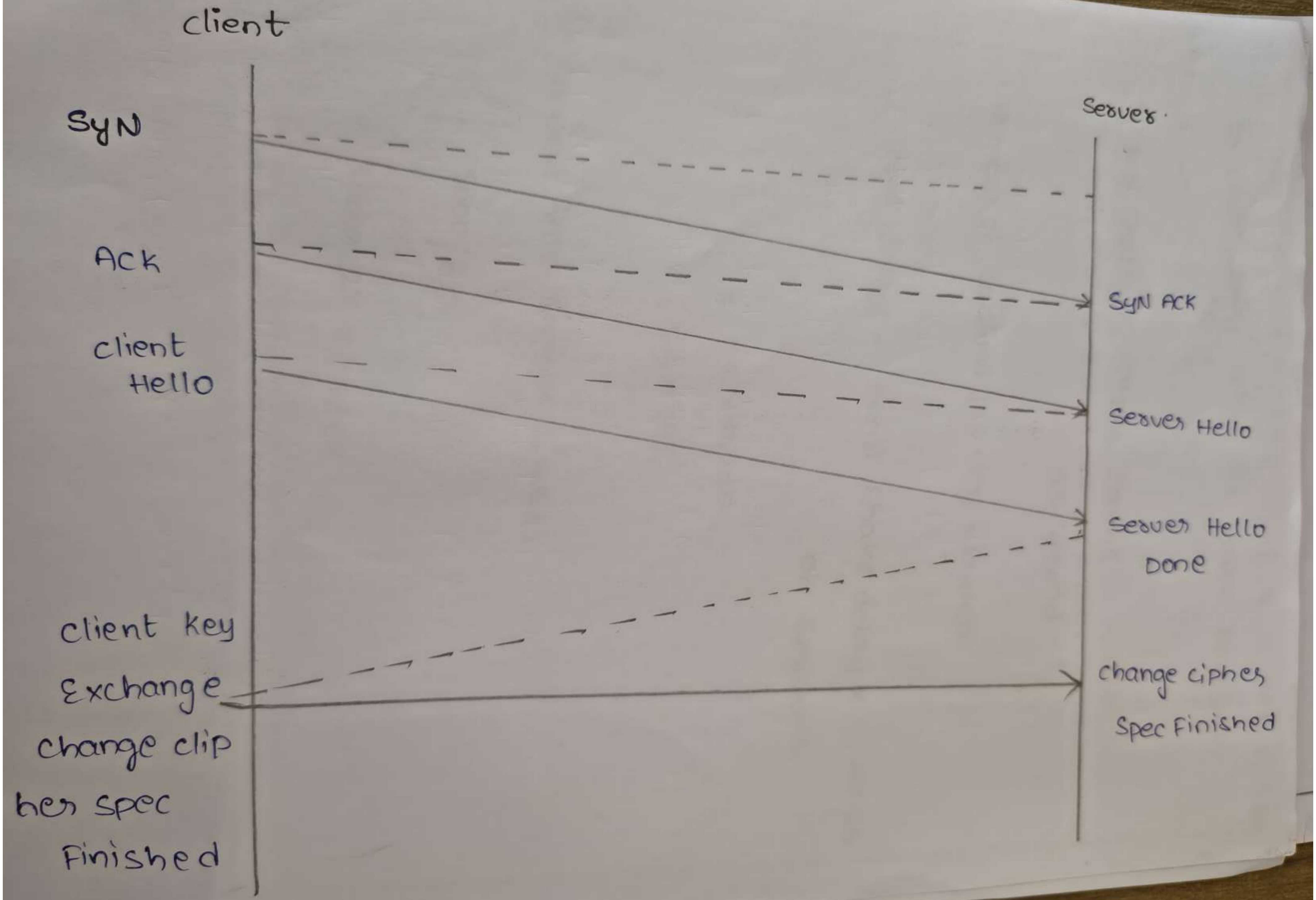
- server sends its SSL
- client verifies the Certificate
- Server's public key

3. why important for Bank :-

- Authentication

- confidentially

- integrity


client
Server.
SyN
Ack
client
Hello
client key
Exchange
change clip
her spec
Finished
SyN ACK
Server Hello
Server Hello
Done
change cipher
Spec Finished

1Q) Describe the SSL hand shake process

A. process :-

1. client Hello :

The client initiates communication

- supported SSL / TLS version
- supported cipher suites
- A randomly generated number

2. server Hello :

- The SSL | TLS version chosen
- selected cipher suite.
- Another random number

3. Certificate verfication :

- checks if it's signed by a trusted certicate
- The browser verifies the certificate

4. key Exchange :

- Depending on the chosen method
- The client and server securely