Client wants to register

Client

Server

1: sendRequest(ID, pubKey);

1.1: random value encrypted with given pubKey

2: decrypts received random value and sends it back encrypted with server pubKey

if returned value is the same as generated, user is registered
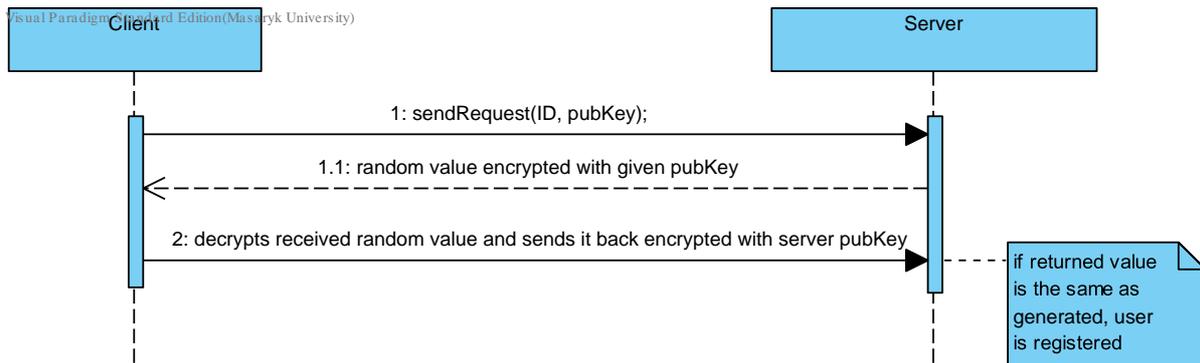
Communication between two clients

Client A

Server

Client B

1: request with own ID

1.1: random value encrypted with client pubKey

2: decrypted value encrypted with server pubKey

3: request with own ID

3.1: random value encrypted with client pubKey

4: decrypted value encrypted with server pubKey

if OK, user
is logged in

5: client list request

5.1: client list (ID, address)

6: connection request with generated half-key encrypted with client B pubKey

6.1: response with generated second half-key encrypted with client A pubKey

7: user communication encrypted with negotiated symmetric key

7.1: