This is your final lesson, which means you must write a really complex program. This program must take you approximately 4-6 months to complete. This is the program that is supposed to force you to learn programming for good. This program is also supposed to force you to use everything you’ve learned so far, and learn new things while at it.

You will learn a lot from this project. At first this project will seem impossible but the more you continue to work on the easier it will become for you.

READ THE TOP OF SECOND PAGE BEFORE STARTING ANYTHING

Requirements:

1. Your program must use threading in some way.
2. Your program must use GUI instead of a console.
3. Your program must have multiple classes, each class in its own file, each file in a lib folder
4. Your code must be well-documented, don’t over document it please.
5. Your code must be well-written; easy to read, follow, and understand.
6. Your code should have a few error handlers, so, the user doesn’t crash it when it’s compiled into a portable executable using something like PyInstaller.
7. Your GUI must look neat and professional, like a group of people did it together.
8. A user must be able to login into their account and see the friends that are online.
9. Don’t stop until you get it to work as intended. Have fun.

Your final program is the following:

A program that allows two users to communicate in privacy.

Your program should have main server where the users will connect to and have their messages relied to the intended person, that way both of the users don’t have to online simultaneously to send each other messages. Your program should be designed in a way that prevents the server program view the messages that are being sent and received, also known as End-to-End Encryption. You can achieve this generating a random key (AES) and using that key to encrypt the message, then use the recipient’s public key (RSA) to encrypt the random key (AES). That way only the other user that has the private key to that public key can decrypt the AES key that was encrypted with the public key and use that key to decrypt the message that was encrypted with the AES key.

By the way, the RSA key pair must be generated only once; the public key saved on to the server and the private key saved on to the user’s device. That will allow the server to know the recipient’s public key at all times, even when that user is offline.

Your program must use the following:

1. Sockets; so, the computers can communicate.
2. RSA/AES; so, the server can’t intercept the users’ communication.
3. SSL; so, the user can communicate with the server in private.
4. Databases; databases can be useful for keeping track of account data.

How have about six months to do this, spend about two months learn each section, and learn each section very well. After that start the project

Things to learn before starting project:

Python:

[How to make GUI in PyGt5?](https://www.youtube.com/watch?v=ksW59gYEl6Q)

[How to make modern GUI in Python?](https://www.youtube.com/watch?v=627VBkAhKTc)

Hashing:

[What is hashing?](https://www.youtube.com/watch?v=2Cg2So2js5k)

[Why use hashing?](https://www.youtube.com/watch?v=b4b8ktEV4Bg)

[What is SHA?](https://www.youtube.com/watch?v=DMtFhACPnTY)

Salting:

[What is a salt?](https://en.wikipedia.org/wiki/Salt_(cryptography))

[What is salting?](https://www.youtube.com/watch?v=sjEeqtZ7Tw4)

[What is bcrypt?](https://en.wikipedia.org/wiki/Bcrypt)

Communication:

[What is TCP/UDP?](https://www.youtube.com/watch?v=qs5X0-x209M)

[How to create a server in Python?](https://www.youtube.com/watch?v=2P8s_KV51rM)

[How to create a client in Python?](https://www.youtube.com/watch?v=xbeNk-UQ0kE)

[How to have multiple clients?](https://www.youtube.com/watch?v=ZwxTGGEx-1w)

Cryptography:

[What is AES?](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

[What is RSA?](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

[What is SSL?](https://www.youtube.com/watch?v=iQsKdtjwtYI)

[What is asymmetric encryption?](https://www.youtube.com/watch?v=AQDCe585Lnc)

[What is the difference between symmetric and asymmetric key encryption?](https://www.youtube.com/watch?v=-9rK3EZop_M)

[What is E2EE?](https://www.youtube.com/watch?v=jkV1KEJGKRA)

Database:

[How to program in SQL?](https://www.youtube.com/watch?v=HXV3zeQKqGY)

[What is SQL injection?](https://www.youtube.com/watch?v=_jKylhJtPmI)