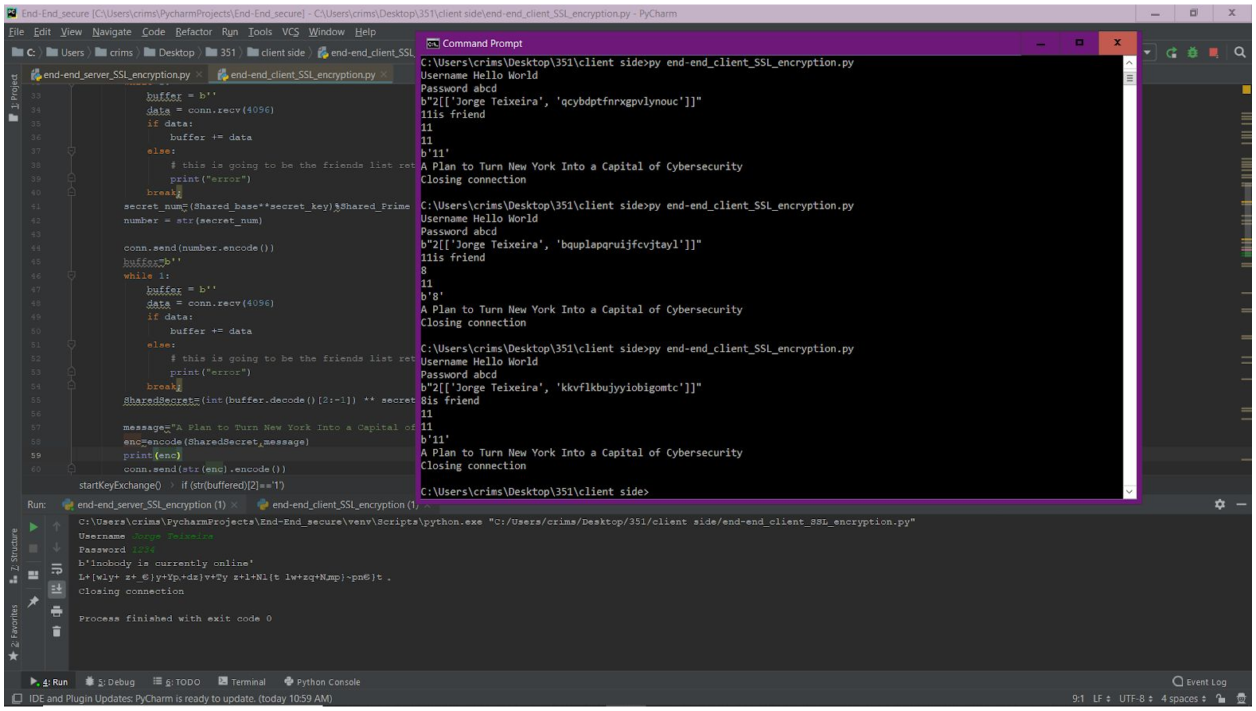
Jorge Teixeira
31385227

So far here is everything I have done. currently the things I have are
1) SSL certificates for clientA and server
2)private keys for the server and clientA
3)salted/hashed passwords in a hardcoded db
4)SSL three way handshake
5)user authentication by using a hashing method that works (check sources for website)
6)server authentication(through ssl certificate)
7) cipher list and support
8) session keys
9) encoding/decoding messages
10)threading
11)friendlist
12)metadata
13)key exchange protocol using simple diffie method
14) manages identities
15)honestly everything that you asked for in the paper
To continue from where the milestone left off. I now have working user input for username and password. It now shows the friends list if any are online. If no are online it tells you that none are online. It only asks for password after the certificate has been verified. The meta data allows me to decide which person I am speaking to and the session ID allows me to confirm that. The entire thing drops if the tls is interrupted which I read in some places is mandatory for a working TLS so that's what I did. I threaded two users at the same time and used spin locks to allow them to work together. I now have the password salted into a file. Iu now have friend lists in a separate file as per your request. The encryption is a simple but effective cipher that does not allow any outsider to enter. And as per your request the sentence to encrypt and decrypt is the same one in the email. The screenshots below will show you the working code and if you wish to check the code for yourself you can do so as you like.
Tutorial on how to get the program working

1) Get https.py working its in the server file and it servers as a host for anyone to grab the server certificate
2) Start the server python file
3) Start the client file one username is Jorge Teixeira and the password is 1234
   The other username is Hello World and the password is abcd

4) from there it should be simple enough. If for some reason it does not work I have it uploaded on my github and it is timestamped so if any error occurs we can use the github and I will show you on my computer

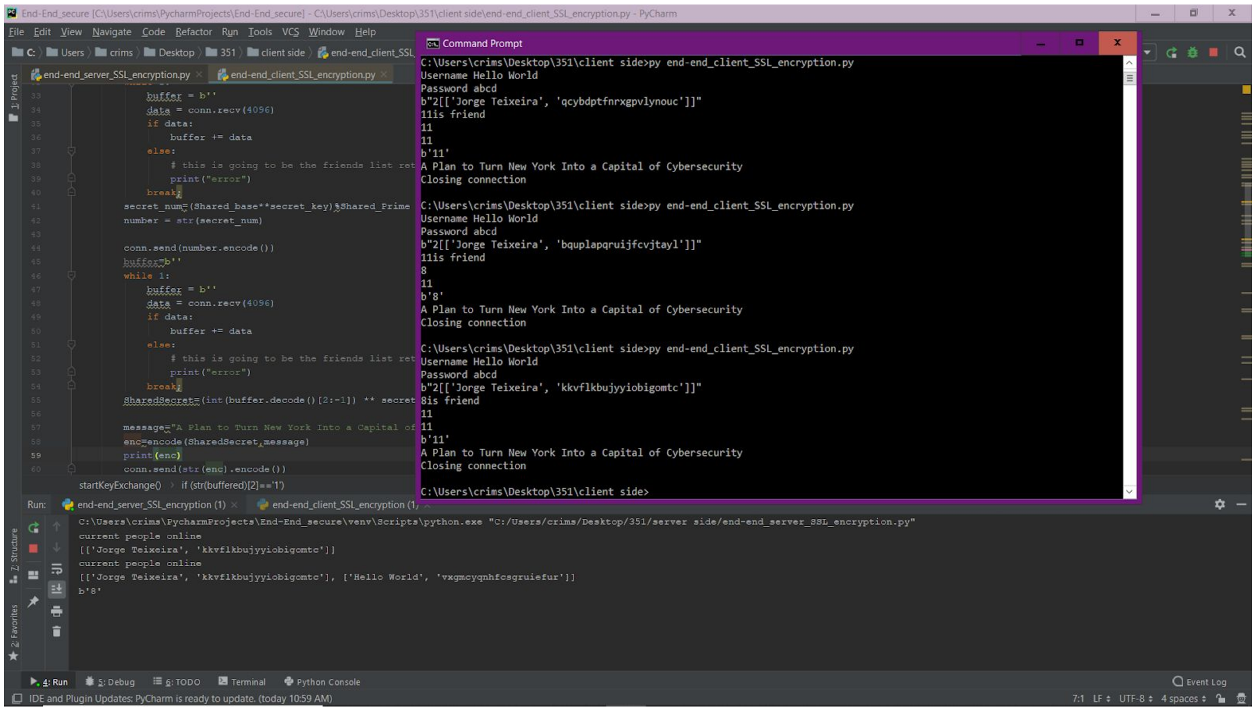
Screenshots of it working



```
        buffer = b''
        data = conn.recv(4096)
        if data:
            buffer += data
        else:
            # this is going to be the friends list ret
            print("error")
        break;
    secret_num=(Shared_base**secret_key)%Shared_Prime
    number = str(secret_num)

    conn.send(number.encode())
    buffer=b''
    while 1:
        buffer = b''
        data = conn.recv(4096)
        if data:
            buffer += data
        else:
            # this is going to be the friends list ret
            print("error")
        break;
    SharedSecret=(int(buffer.decode()[2:-1]) ** secret

    message="A Plan to Turn New York Into a Capital of
    enc=encode(SharedSecret,message)
    print(enc)
    conn.send(str(enc).encode())
```

```
C:\Users\crims\Desktop\351\client side>py end-end_client_SSL_encryption.py
Username Hello World
Password abcd
b"2[['Jorge Teixeira', 'qcybdptfnrxgpvlynouc']]"
11is friend
11
11
b'11'
A Plan to Turn New York Into a Capital of Cybersecurity
Closing connection

C:\Users\crims\Desktop\351\client side>py end-end_client_SSL_encryption.py
Username Hello World
Password abcd
b"2[['Jorge Teixeira', 'bquplapqruijfcvjtayl']]"
11is friend
8
11
b'8'
A Plan to Turn New York Into a Capital of Cybersecurity
Closing connection

C:\Users\crims\Desktop\351\client side>py end-end_client_SSL_encryption.py
Username Hello World
Password abcd
b"2[['Jorge Teixeira', 'kkvflkbujyyiobigomtc']]"
8is friend
11
11
b'11'
A Plan to Turn New York Into a Capital of Cybersecurity
Closing connection

C:\Users\crims\Desktop\351\client side>
```

```
C:\Users\crims\PycharmProjects\End-End_secure\venv\Scripts\python.exe "C:/Users/crims/Desktop/351/client side/end-end_client_SSL_encryption.py"
Username Jorge Teixeira
Password 1234
b'1nobody is currently online'
L+[wly+ z+_€}y+Yp+dz}v+Ty z+l+Nl{t lw+zq+N,mp}~pn€}t .
Closing connection

Process finished with exit code 0
```



```
        buffer = b''
        data = conn.recv(4096)
        if data:
            buffer += data
        else:
            # this is going to be the friends list ret
            print("error")
        break;
    secret_num=(Shared_base**secret_key)%Shared_Prime
    number = str(secret_num)

    conn.send(number.encode())
    buffer=b''
    while 1:
        buffer = b''
        data = conn.recv(4096)
        if data:
            buffer += data
        else:
            # this is going to be the friends list ret
            print("error")
        break;
    SharedSecret=(int(buffer.decode()[2:-1]) ** secret

    message="A Plan to Turn New York Into a Capital of
    enc=encode(SharedSecret,message)
    print(enc)
    conn.send(str(enc).encode())
```

```
C:\Users\crims\Desktop\351\client side>py end-end_client_SSL_encryption.py
Username Hello World
Password abcd
b"2[['Jorge Teixeira', 'qcybdptfnrxgpvlynouc']]"
11is friend
11
11
b'11'
A Plan to Turn New York Into a Capital of Cybersecurity
Closing connection

C:\Users\crims\Desktop\351\client side>py end-end_client_SSL_encryption.py
Username Hello World
Password abcd
b"2[['Jorge Teixeira', 'bquplapqruijfcvjtayl']]"
11is friend
8
11
b'8'
A Plan to Turn New York Into a Capital of Cybersecurity
Closing connection

C:\Users\crims\Desktop\351\client side>py end-end_client_SSL_encryption.py
Username Hello World
Password abcd
b"2[['Jorge Teixeira', 'kkvflkbujyyiobigomtc']]"
8is friend
11
11
b'11'
A Plan to Turn New York Into a Capital of Cybersecurity
Closing connection

C:\Users\crims\Desktop\351\client side>
```

```
C:\Users\crims\PycharmProjects\End-End_secure\venv\Scripts\python.exe "C:/Users/crims/Desktop/351/server side/end-end_server_SSL_encryption.py"
current people online
[['Jorge Teixeira', 'kkvflkbujyyiobigomtc']]
current people online
[['Jorge Teixeira', 'kkvflkbujyyiobigomtc'], ['Hello World', 'vxgmcyqnhfcsgruiefur']]
b'8'
```

Sources

these are my current sources that i used
 and why i used them

How to use simple diffie -
https://sublimerobots.com/2015/01/simple-diffie-hellman-example-python/

How to thread in python- https://docs.python.org/2/library/thread.html

How to make random strings- https://pynative.com/python-generate-random-string/

How to set up key agreement protocol-
https://sublimerobots.com/2015/01/simple-diffie-hellman-example-python/

How to set up
SSl-https://www.electricmonk.nl/log/2018/06/02/ssl-tls-client-certificate-verification-with-pytho
n-v3-4-sslcontext/

salted passwords -
https://stackoverflow.com/questions/9594125/salt-and-hash-a-password-in-python

server preferences and how the ciphers worked -
https://www.programcreek.com/python/example/65033/OpenSSL.SSL.OP_NO_SSLv3

general functions and options - https://docs.python.org/3/library/ssl.html

hwo to open and write to a file -
https://www.guru99.com/reading-and-writing-files-in-python.html

to make sure i signed my certificates correctly -
http://pankajmalhotra.com/Simple-HTTPS-Server-In-Python-Using-Self-Signed-Certs

examples for how to get my certificates over hostnames -
https://www.programcreek.com/python/example/62606/ssl.get_server_certificate

certificate handling - https://docs.python.org/2/library/ssl.html

non secure tcp connection - https://pymotw.com/3/socket/tcp.html

ssl handshake -
https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm

how to decode byte to string -
https://stackoverflow.com/questions/606191/convert-bytes-to-a-string

more salting examples - https://www.vitoshacademy.com/hashing-passwords-in-python/

examples of how to encode and decode-
https://stackoverflow.com/questions/2490334/simple-way-to-encode-a-string-according-to-a-password