**Cryptographically Secure Version of Facebook Prototype**

Nikhil Tiwari UFID 91507670 ([nikhiltiware@ufl.edu](mailto:nikhiltiware@ufl.edu))

Parikshit Tiwari UFID 79218564 ([pariksh1tatiwari@ufl.edu](mailto:pariksh1tatiwari@ufl.edu))

**How to run:**

To run the application the Server needs to be run first. Followed by the Client.

**Running the Server (No arguments need to be passed)**

Navigate to the FacebookServer folder in terminal/commandline

For example navigate to “/home/Documents/ project4\_part1 /FacebookServer” or “C:\Desktop\ project4\_part1 \FacebookServer”

Run the command: sbt compile

Run the command: sbt run

**Running the Client (Number of users need to be passed)**

Navigate to the FacebookClient folder in terminal/commandline

For example navigate to “/home/Documents/ project4\_part1 /Facebook Client” or “C:\Desktop\ project4\_part1 \Facebook Client”

Run the command: sbt compile

Run the command: sbt “run number\_of\_users”

For example if you want to run 100 users the command would be

sbt “run 100”

**Working**

**Authentication**

1) The user first registers and deposits his public key at the server

2) When login request is sent to the server. Thee server generates a random number and encodes it with the user's public key and sends this cipher text back to the user

3) The user then decrypts the message with his private key and sends back across to server. Thus iauthenticating himself.

**Encryption**

1) Every post and picture , posted by a user is encrypted with a unique AES symmetric key. The symmetric key is encrypted by the receiver's public key. This combination is stored at the server.

2) The intended recipient retrieves this data from the server. Uses his private key to decrypt the AES symmetric key and then uses the symmetric key to decrypt the message or picture.