# CS 5770: PROJECT PROGRESS REPORT

Team Members: Akshay Kulkarni, Aravind Eswaran, Karthik Sambamoorthy

ACCOMPLISHED STEPS:

1. For the RSA key generation toolbox, we have made significant progress on the backend part. We have developed (in java 8) the functions for randomly generating two primes p and q. We also coded the parts for calculating e and d given p and q, encrypting a message m with a given public key, and decrypting an encrypted message given a private key. All that is left for this portion of the project to develop a front end GUI, map the slots and buttons in the GUI to their corresponding mathematical values.

OBSTACLES ENCOUNTERED

1. We have used an in built modular arithmetic library for the purposes of this project. That library has functions for probable prime generation. Ideally we would like to have such functions be deterministic, as in real world situations it would be fatal even to have a small degree failure. So we have been researching more about the mathematics behind this prime generation and how to make it more secure. As of now it seems like the best approach out there is still probabilistic.

HARDER STEPS AND POTENTIAL CHALLENGES

1. One potential challenge that we foresee in this project is the testing of our encryption and decryption systems. Testing includes many facets like checking whether the huge number that was generated was a prime or not, did the encryption and decryption that happened was correct mathematically. Since we would be dealing with exceedingly large numbers(~ 10300), even checking for additions would be tedious what to speak of complicated operations like gcd, modulo etc.