Computer Science Project Proposal

Neil Nie

April 28, 2017

Introduction:

RSA, which stands for Ron Rivest, Adi Shamir and Leonard Adleman, is a computer algorithm used for encrypting and decrypting messages. This is also called a public key cryptography, because one key is given to everyone. RSA is widely used in SSH (Secure Shell), HTTPS (Hyper Text Transfer Protocol Secure) and other data transfer protocols. The algorithm is also very powerful in that it has been around for more than 30 years and have not been compromised.

The project:

During the end of the spring term, I will develop an encrypted iOS messenger with RSA algorithm. First, I will write a console program that can encrypt and decrypt data. Then, I will apply this to the iOS app.

The iOS app will use Firebase as its mobile backend, which is a real-time database with push notification support. This tool will allow me to develop a professional messaging app without developing my own web backend.

Timeline:

During the first week of the project (May 1st – May 5th), I will research and learn about RSA algorithm and also begin some coding. During the second week, (May 8th – May 12th), I will finish the console program for RSA. From May 15th to 26th, I will finish the encrypted messenger. With the time left, I will write about the development process.

Final deliverable:

The final deliverable for the project should be two Xcode project. One is a console program that uses RSA to encrypt and decrypt data. The second program should be an encrypted iOS messaging app with RSA algorithm.