RSA Group Project

Andrew Farmer, [Clayton McEntire](mailto:cmcentire@cub.uca.edu), Chandler Richmond

University of Central Arkansas

Algorithms CSCI 3330

Dr. Hu

Date: 2/16/2022

# Introduction

For this project the use of several algorithms is required for it to correctly Encrypt and Decrypt user input strings. Starting out with generating two large integers and determining if they are pseudo prime through the use of Fermat’s test. Then a relatively prime is found from the pseudo primes using Euclid's gcd and d is found from the Extended Euclid algorithm. From these elements we have found, RSA encryption and decryption is now possible.

**Member Contributions / Responsibilities**

| Andrew Farmer | Clayton McEntire | Chandler Richmond |
| --- | --- | --- |
| Responsibilities:  Git Hub Creation | Responsibilities:  Group Communication | Responsibilities: |
| Contributions:  Key Generation  Euclid’s GCD  RSA Encryption  RSA Decryption | Contributions:  Rand Prime Generation  Fermat’s Test  UI Elements  Project Report | Contributions: |

**Solution Design**

**Problem Analysis and Algorithm Identification**

**Implementation**

The project was Implemented using Spyder Python,

**Testing**

**Summary**