RSA Group Project

Andrew Farmer, Clayton McEntire, 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 using 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 Decryption | Contributions:  Rand Prime Generation  Extended Euclid  Fermat’s Test  UI Elements  RSA Encryption  Project Report | Contributions: |

**Solution Design**

**Problem Analysis and Algorithm Identification**

The project was divided into 3 main tasks, Key Generation, RSA Encryption/Decryption, and Digital Signature and Digital Signature authentication.

Key generation used the Fermat’s test to determine if the p and q generated were pseudo primes. The Fermat’s test was run 40 times to ensure accuracy, If the number was determined to not be a pseudo prime they were regenerated. Euclid’s gcd and extended gcd were called to generate e and d for encryption. From there we have our Public and Private keys.

RSA Encryption received the keys e, d, and n = (P\*Q), from there the RSA encryption algorithm can be completed by

**Implementation**

The project was Implemented using Spyder Python, and the course materials.

Clayton worked on Key Generation in the project along with encryption of the input text. He implemented the Extended Euclid’s algorithm and determining the pseudoprimes with the Fermat’s test. To better understand proper implementation of the algorithms he went to tutoring with Tarrant at the UCA Library as well as Office hours to understand finding d.

Andrew worked on ……. ADD LATER

Chandler worked on ????

**Testing**

**Summary**