

RSA GUI

Boise Cryptology Conference Fall 09

Thomas Castona

Overview

1. Motivation
2. Application Design
3. Uses
4. Security
5. Implemented and Used Algorithms
6. Performance
7. Future Modifications

Motivation

- Create an application that is user friendly and does not require in-depth knowledge of the mathematics behind RSA and other algorithms used to implement a secure and fast RSA encryption system.

RSA Application Design

- A GUI application that uses the RSA asymmetric encryption algorithm.
- Open files and encrypt and then save the file.
- Save and load RSA keys. Have a tool for generating an RSA key.

Uses

- Encrypted files can be passed in emails and other “insecure” communication channels.

Security

- Use the RSA algorithm to encrypt and decrypt data.
- Generate and use keys of substantial number of bits, (several thousand bits). RSA keys with “length of 1024 bits are considered insecure” Arjen Lenstra. The application has been tested with keys of 4094 bits, with minor performance decrease.
- (not implemented) A module that checks the strength of a generated or opened key private key.

Implemented and Used Algorithms

- RSA Rivest Shamir and Alderman algorithm.
- Miller Rabin
- Euler's Algorithm for finding modular inverse

Performance

- Current Key Generation With Bit Lengths
 - $p \& q(1024) m(2042)$: 35 seconds
 - $p \& q(2048) m(4094)$: 1 minute – 1 minute and 45 seconds
- Current Encryption/Decryption time
 - 2042 bits: 2 seconds
 - 4094 bits: 5 seconds

Future Modifications

- Expand on the current key generator to not use pseudo random number, but use large numbers generate with mouse movements (similar to PGP) or another method. Increase the speed of the key generation.
- Get the strength checking module working and implement it in the current code.
- Add functionality for using a list of keys, currently several methods have been designed for this.
- Add functionality for signatures

A decorative border surrounds the central text, featuring a repeating pattern of stylized, overlapping letters and symbols in shades of blue and green. The border is thicker at the corners, creating a rounded rectangular frame.

The End
Now to the RSA application.