Open PGP Project Report

Project Descrption

This projects serves for better understaning PGP encryption program within university program.

Asymmetric-key algorithm used in this project is RSA with three different key sizes: 1024, 2048 and 4096bits.RSA wil be used for data encryption and digital signing.

Symmetric-key algorithms used in this project is 3DES witi EDE configuration with three keys and CAST5 with key size of 128bits.

For implementation of this project we are using Java programming language,the encrpytion library Bouncy Castle Crypto APIs, Eclipse Window Builder for GUI designing.

Kleopatra software is used as an example of how our app should look and work, the most of our design ideas come from Kelopatra software Analyisis.

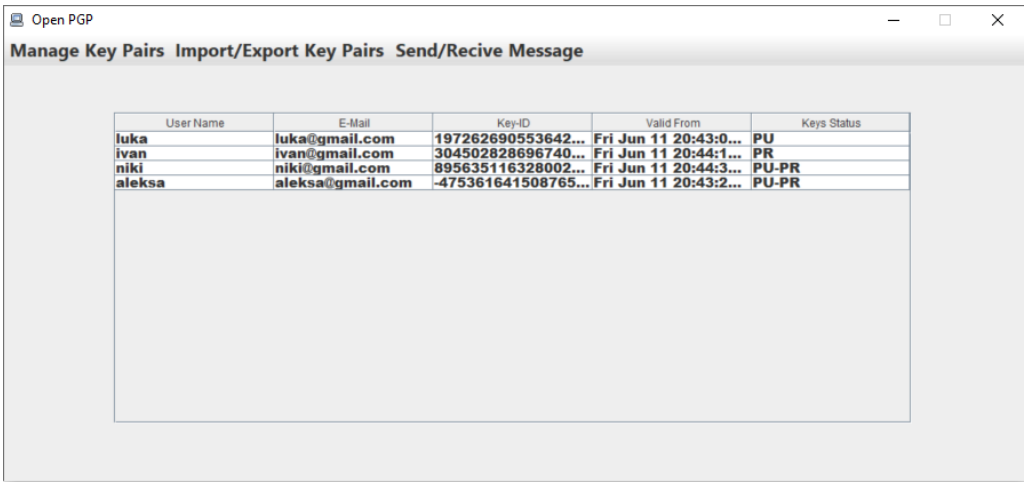
This project will be developed by Živković Aleksa and Matović Luka

Project Features

- New Key Pair generating
- Removing exsiting Key Pair
- Import/Export of public or private keys with necessary infomrations
- Sending message with option of encryption and digital signature
- Reciving message with option of decryption.
- Displaying users key pairs

GUI description

- Main Window



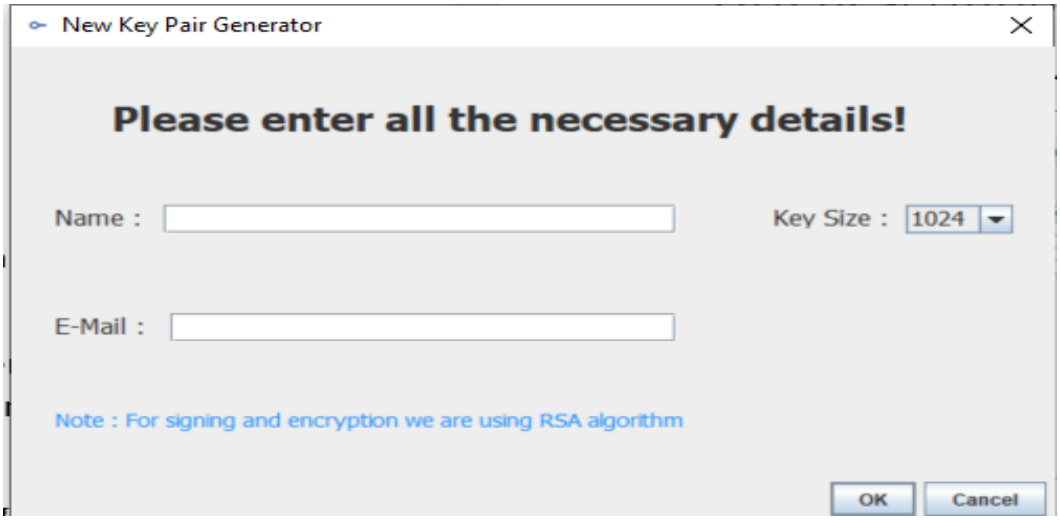
This window shows us all users and their key pair details, with column Key Status which shows us what keys our user have.

PU stands for Public Key and PR stands for private key.

PU-PR means that user has both private and public key.

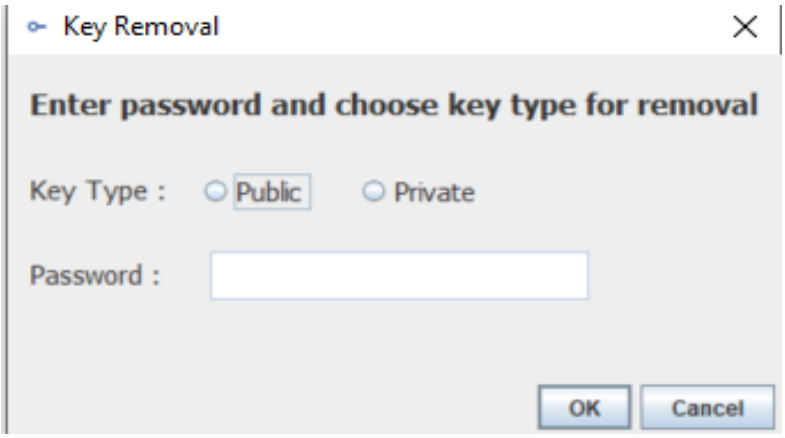
Menu part of the UI offers us options of using our app

- Add New Key Pair



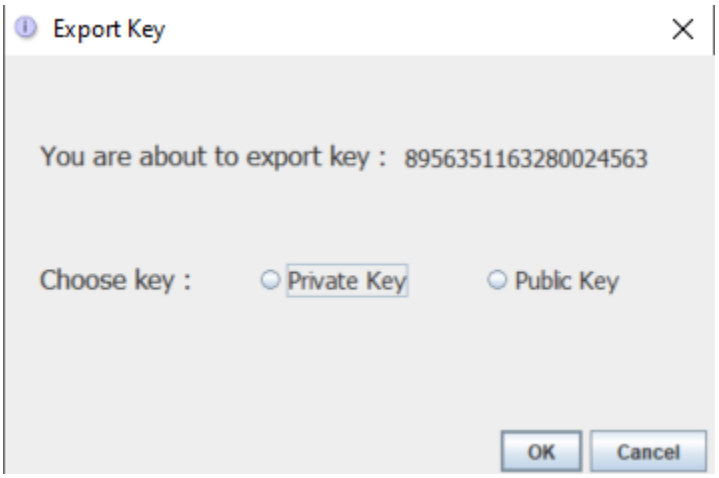
Window for making new Key Pair with desired information user enters. When user enters all data he needs to enter password for private key handling.

- Key Removal



Window for Key Removal is used for deleting particular key, user has to be selected in order to remove key, also if you are removing private key you have to enter private password for that key.

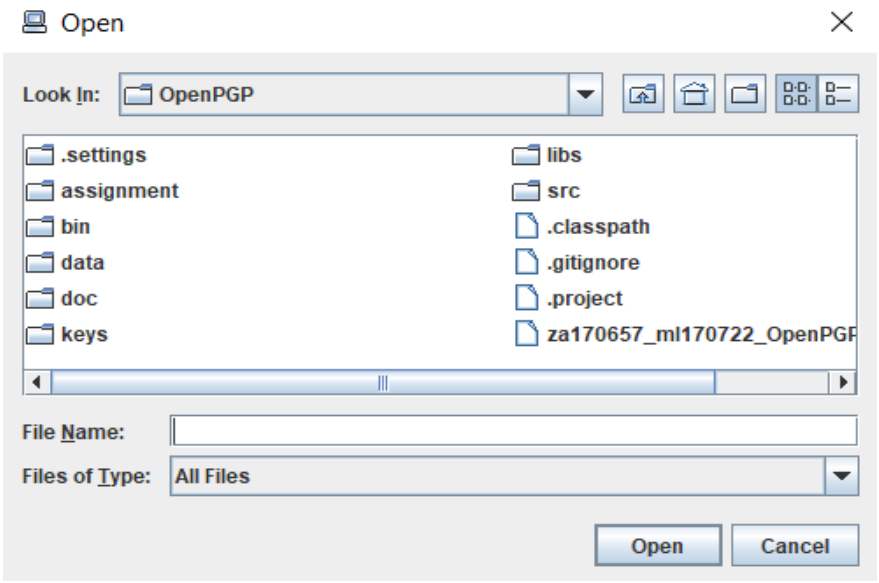
- Export Key



Window for Exporting a Key, you will see Key Id of the key you will export and you can choose what key type of Key Pair you want to export.

Exported file will be called : Key ID + _PUBLIC/_PRIVATE.asc

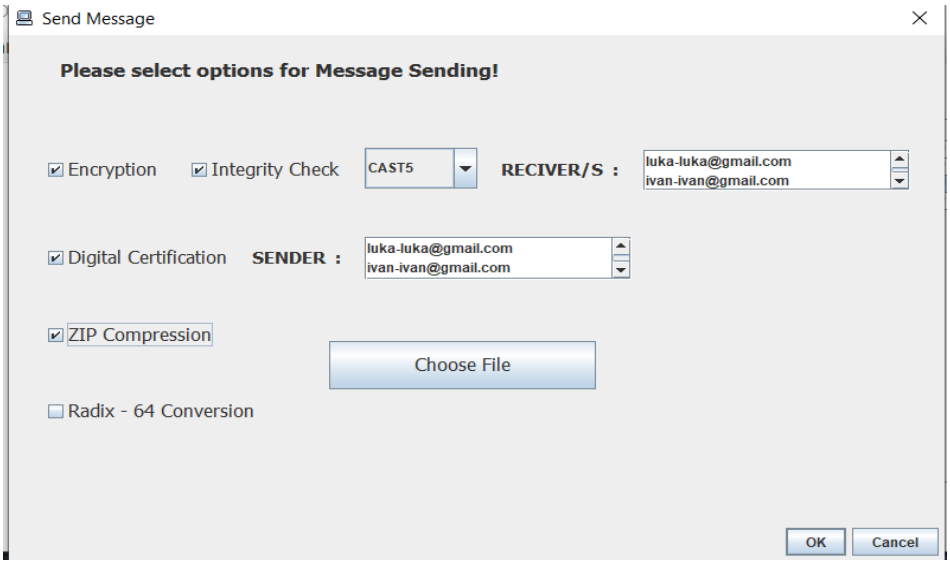
- Import Key



Window for Import Key is used for importing a key from users file system, user has to choose a file from his file system and select it.

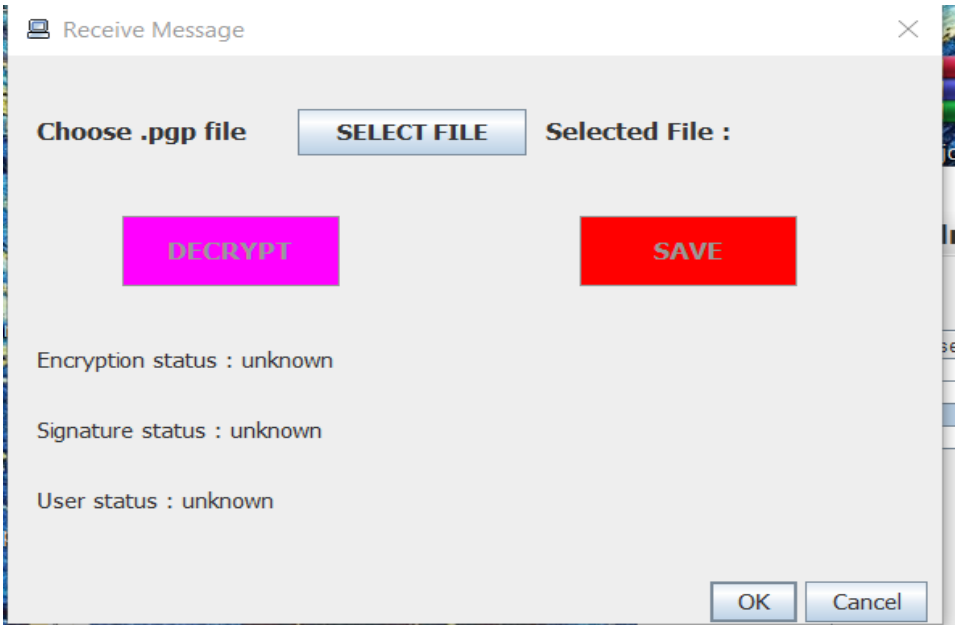
After Key Importing Table of Key Pairs will be updated!

- Send Message



Window for Send Message, is used when user wants to send a message.User can choose wether the Digital Certification, Encryption, ZIP Compression and Radix conversion. User has to select file which he wants to be send to another user.

- Receive Message



Window for Receive Message feature, user can choose a file which is encrypted and after that he can see the details about the message he recived from particular user.

Documentation for Code

We generated Java Doc file which shows you what particular function does and for what is some part code is used for.