OPENPGP SIMULATION

Authors:
Kosta Matijević
Dušan Gradojević

1. Introduction

Goal of this project is implementation of Swing based Java application that demonstrates usage of PGP protocol in data sending and receiving.

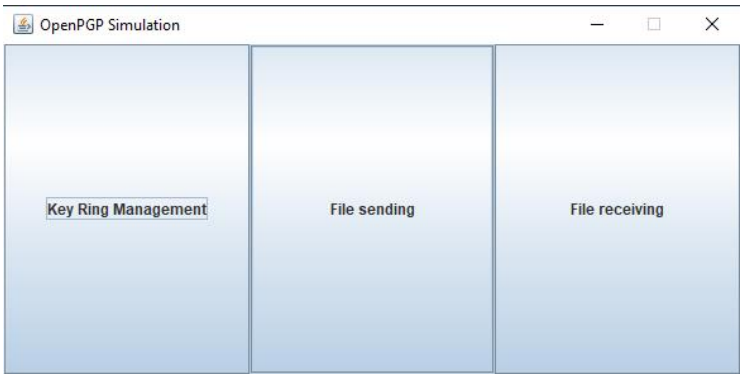
PGP (*Pretty Good Privacy*) is widely used security protocol that enables authentication, integrity and privacy of data.

Functionalities:

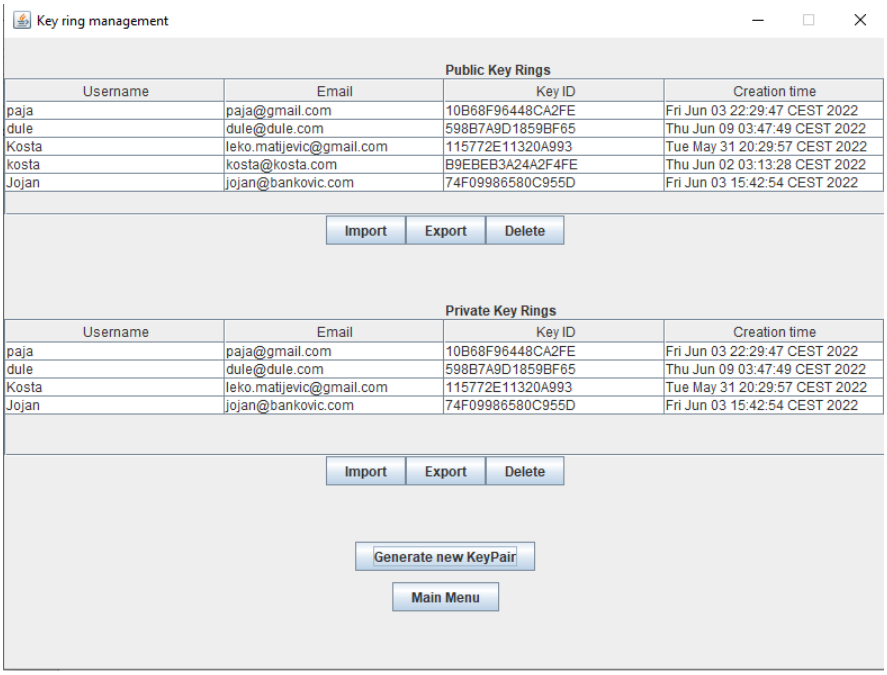
- Reviewing collections of private and public keys
- Import and export of key rings into .asc files
- Generating new and deleting existing key rings
- Message sending (encryption, singning, compression and radix-64 conversion)
- Message receiving (decryption and signature verification)

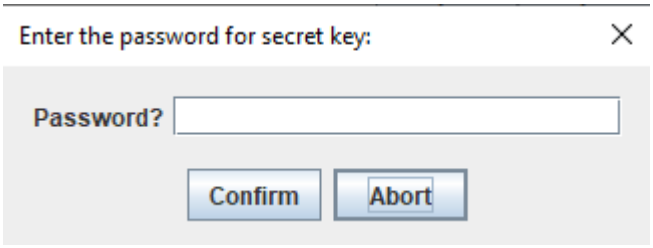
2. GUI

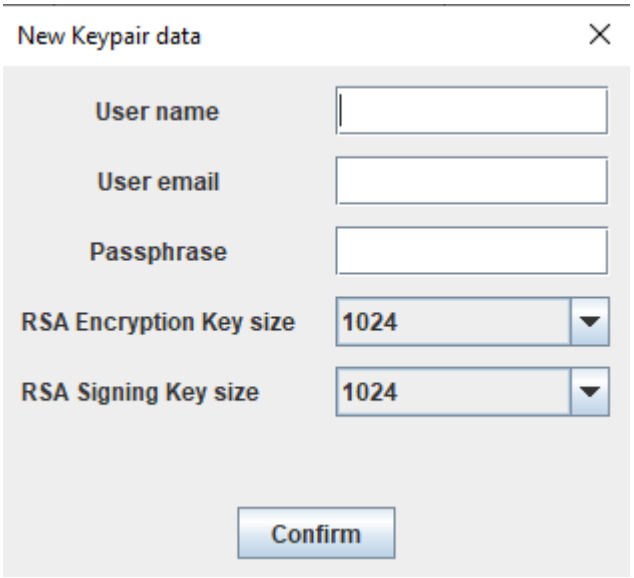
2.1. Start Menu



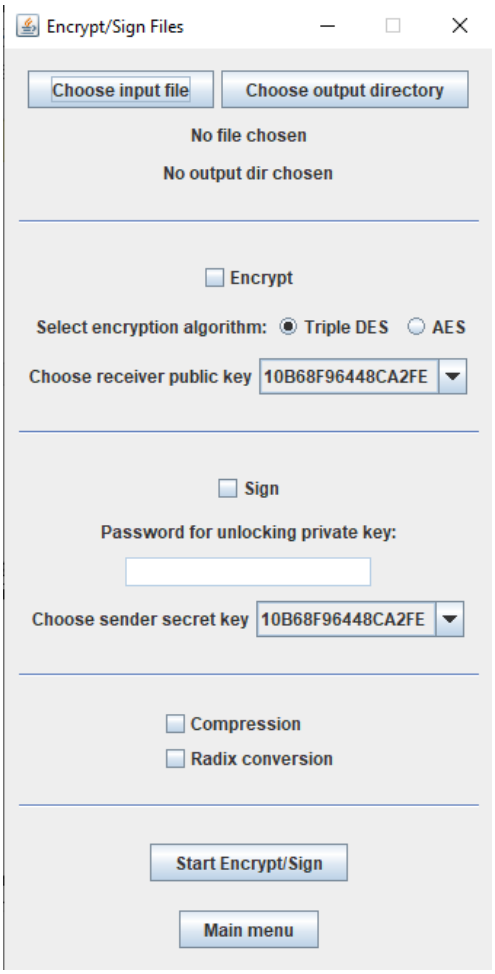
2.2. Key Management



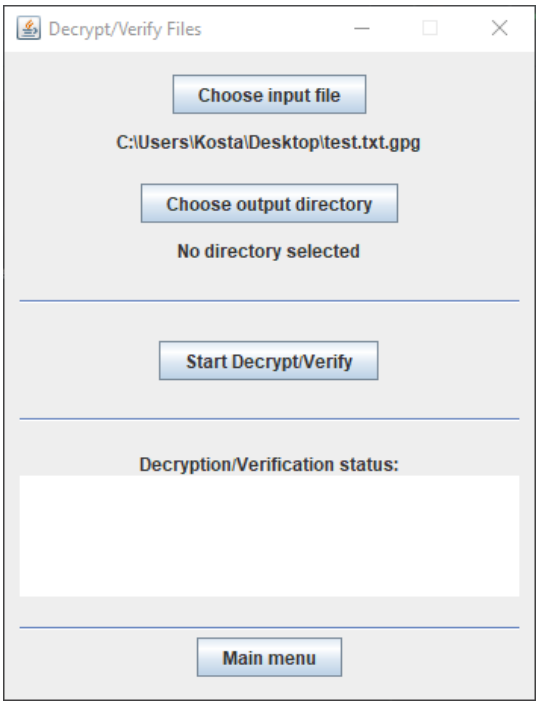


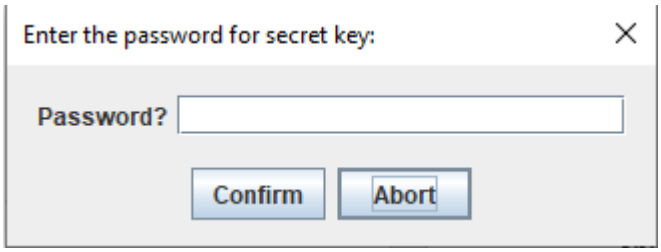


2.3. Message sending



2.4. Message receiving





3. Used Algorithms

Asymmetric: RSA for signing and encryption.
Symmetric: 3DES with EDE configuration and AES.

3.1. Asymmetric algorithms

RSA (Rivest-Shamir-Adleman) is the best known and most widely used public key encryption algorithm. It is a block algorithm where the original data and encrypted data are integers between 0 and n-1 for some n. The message is encrypted with the receiver's public key while the receiver decrypts the message with his private key. This ensures that only the recipient can decrypt the message. The sender signs the data he sends with his private key,

which provides a unique signature for the user, while the receivers use the sender's public key to verify who the message came from.

3.2. Symmetric algorithms

The 3DES algorithm is a symmetric key algorithm used to encrypt block data. 3DES is a variation of the DES algorithm where the algorithm itself is repeated three times. This particular implementation uses a three-key EDE (Encrypt-Decrypt-Encrypt) configuration.

AES (Advanced Encryption Standard) is a block algorithm intended to replace DES in commercial applications. It uses 128 bits for the block size and 128, 192 or 256 bits for the key size. AES does not use the Feistel structure.