

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.

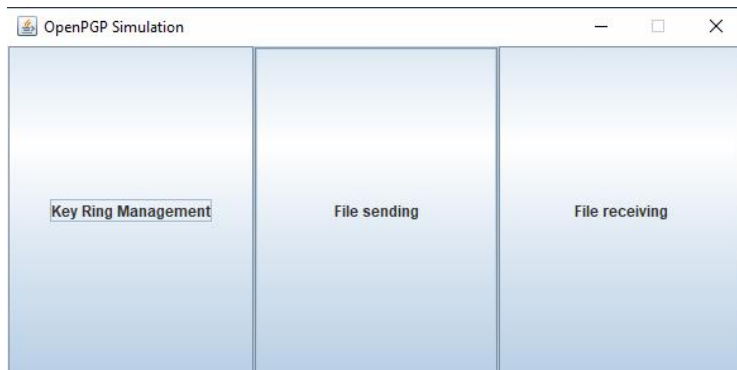
PGP (*Pretty Good Privacy*) is widely used security protocol that enables authentication, integrity and privacy of data.

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, signing, compression and radix-64 conversion)
- Message receiving (decryption and signature verification)

2. GUI

2.1. Start Menu



2.2. Key Management

Key ring management

Public Key Rings			
Username	Email	Key ID	Creation time
paja	paja@gmail.com	10B68F96448CA2FE	Fri Jun 03 22:29:47 CEST 2022
dule	dule@dule.com	598B7A9D1859BF65	Thu Jun 09 03:47:49 CEST 2022
Kosta	leko.matijevic@gmail.com	115772E11320A993	Tue May 31 20:29:57 CEST 2022
kosta	kosta@kosta.com	B9EBEB3A24A2F4FE	Thu Jun 02 03:13:28 CEST 2022
Jojan	jojan@bankovic.com	74F09986580C955D	Fri Jun 03 15:42:54 CEST 2022

Import Export Delete

Private Key Rings			
Username	Email	Key ID	Creation time
paja	paja@gmail.com	10B68F96448CA2FE	Fri Jun 03 22:29:47 CEST 2022
dule	dule@dule.com	598B7A9D1859BF65	Thu Jun 09 03:47:49 CEST 2022
Kosta	leko.matijevic@gmail.com	115772E11320A993	Tue May 31 20:29:57 CEST 2022
Jojan	jojan@bankovic.com	74F09986580C955D	Fri Jun 03 15:42:54 CEST 2022

Import Export Delete

Generate new KeyPair

Main Menu

Enter the password for secret key: X

Password?

Confirm

Abort

New Keypair data X

User name

User email

Passphrase

RSA Encryption Key size

1024

RSA Signing Key size

1024

Confirm

2.3. Message sending

The screenshot shows a window titled "Encrypt/Sign Files" with standard Windows window controls (minimize, maximize, close). The interface is divided into several sections by horizontal lines. At the top, there are two buttons: "Choose input file" and "Choose output directory". Below these, the text "No file chosen" and "No output dir chosen" is displayed. The next section contains a checkbox labeled "Encrypt". Below the checkbox, it says "Select encryption algorithm:" followed by two radio buttons: "Triple DES" (which is selected) and "AES". Below this, there is a label "Choose receiver public key" and a dropdown menu showing the value "10B68F96448CA2FE". The following section has a checkbox labeled "Sign". Below it, the text "Password for unlocking private key:" is followed by an empty text input field. Below the input field, there is a label "Choose sender secret key" and a dropdown menu showing the value "10B68F96448CA2FE". The next section contains two checkboxes: "Compression" and "Radix conversion". At the bottom of the window, there are two buttons: "Start Encrypt/Sign" and "Main menu".

Encrypt/Sign Files

Choose input file Choose output directory

No file chosen
No output dir chosen

☐ Encrypt

Select encryption algorithm: ☒ Triple DES ☐ AES

Choose receiver public key 10B68F96448CA2FE ▼

☐ Sign

Password for unlocking private key:

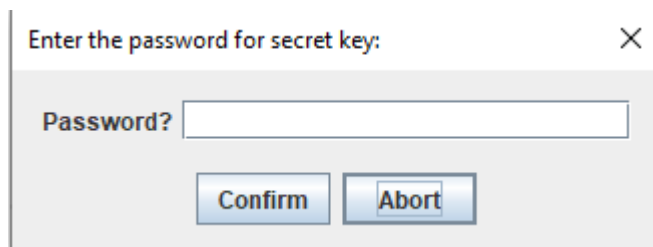
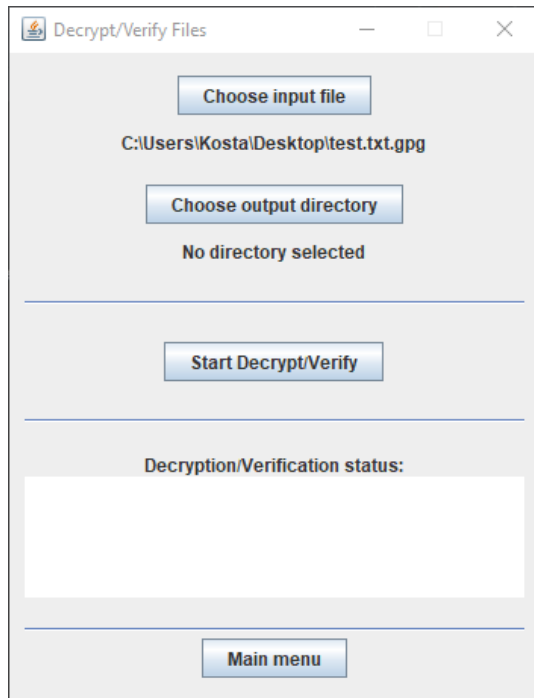
Choose sender secret key 10B68F96448CA2FE ▼

☐ Compression
☐ Radix conversion

Start Encrypt/Sign

Main menu

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.