Exercise Public Key Cryptography

Emmanuel Benoist

Herbst Semester 2023-2024

This exercise is to be done inside the Linux Virtual machine or a Mac.

1 Install

Install both softwares `gpa` and `gnupg2`
For Linux

```
sudo apt install gpa gnupg2
```

For Mac

```
brew install gpa gnupg2
```

Generate a key pair (private and public key):

```
gpg --full-generate-key
```

Chose the option **RSA and RSA**.
Length of the key 4096.
Key does not need to have an expiration date.
You have to do things to generate "entropy" to generate the keys.
The key pair has been created!

2 Communication

Start the software `gpa`.

```
gpa
```

- Select the key you have just created in the list.
- Export the public key.
- Send the key to your neighbors

Import the key of your neighbors

- in gpa you can import the keys.

Use the keys to write a message to your friends. Encrypt with the corresponding public key.

Once received. Copy paste the message in gpa to decrypt it.