Lab #4 - Public Key Encryption

Léo Gabaix

Francesco Mosanghini

To solve this lab we developed different scripts:

1. To simulate a message exchange between Alice and Bob:

- `generator.sh`
- `encryptor.sh`
- `decryptor.sh`

2. To send a message to someone using its public key:

- `send_message.sh`

Usage

The message exchange simulation works with 3 scripts illustrating the 3 different parts. They can be used as follow:

```
$ ./generator.sh
...
$ ./encryptor.sh "<message>" <output_file.pem>
...
$ ./decryptor.sh <encrypted_file.pem>
...
```

or in a chained way:

```
$ ./generator.sh && ./encryptor.sh "<message>" <output_file.pem> && ./decryptor.sh <en
crypted_file.pem>
...
```

Working example:

```
$ ./generator.sh && ./encryptor.sh "ABC123" output.pem && ./decryptor.sh output.pem
```

To send a message to someone you will need only one script:

```
$ ./gen_msg.sh "<message>" msg_encrypted.pem
```

It will generates a `msg_encrypted.pem` file containing all the needed information for the receiver.