

# Exercice 1

## Question 1

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 110x10
$ openssl genrsa -des3 -out alice-privatekey.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x010001)
Enter pass phrase for alice-privatekey.pem:
Verifying - Enter pass phrase for alice-privatekey.pem:
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 <master*>
$
```

Pass phrase: password

## Question 2

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 110x6
$ openssl rsa -in alice-privatekey.pem -pubout -out alice-publickey.pem
Enter pass phrase for alice-privatekey.pem:
writing RSA key
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 <master*>
$
```

## Question 3

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 110x14
$ openssl genrsa -des3 -out bob-privatekey.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x010001)
Enter pass phrase for bob-privatekey.pem:
Verifying - Enter pass phrase for bob-privatekey.pem:
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 <master*>
$ openssl rsa -in bob-privatekey.pem -pubout -out bob-publickey.pem
Enter pass phrase for bob-privatekey.pem:
writing RSA key
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 <master*>
$
```

Pass phrase: password

## Question 4

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 110x4
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 <master*>
$ echo "Corentin GIRAUD" > message.txt
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 <master*>
$
```

## Question 5

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 110x5
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 <master*>
$ openssl dgst -sha1 -sign alice-privatekey.pem -out message.sha1-signed message.txt
Enter pass phrase for alice-privatekey.pem:
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 <master*>
$
```

## Question 6

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 110x5
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 <master*>
$ openssl dgst -sha1 -verify alice-publickey.pem -signature message.sha1-signed message.txt
Verified OK
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3 <master*>
$
```

## Question 7

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q7
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q7 115x21
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q7 <master*>
$ ls -l
total 8
-rw-rw-r-- 1 corentin corentin 451 Nov 29 13:16 bob-publickey.pem
-rw-rw-r-- 1 corentin corentin 16 Nov 29 13:16 message.txt
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q7 <master*>
$ openssl rand -out key.bin 16
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q7 <master*>
$ openssl enc -aes-128-cbc -kfile key.bin -in message.txt -base64 -out protected-message.txt
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q7 <master*>
$ openssl rsautl -encrypt -inkey bob-publickey.pem -pubin -in key.bin -out protected-key.bin
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q7 <master*>
$ ls -l
total 20
-rw-rw-r-- 1 corentin corentin 451 Nov 29 13:16 bob-publickey.pem
-rw-rw-r-- 1 corentin corentin 16 Nov 29 13:16 key.bin
-rw-rw-r-- 1 corentin corentin 16 Nov 29 13:16 message.txt
-rw-rw-r-- 1 corentin corentin 256 Nov 29 13:17 protected-key.bin
-rw-rw-r-- 1 corentin corentin 65 Nov 29 13:16 protected-message.txt
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q7 <master*>
$
```

## Question 8

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q8
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q8 112x16
$ ls -l
total 12
-rw----- 1 corentin corentin 1743 Nov 29 13:21 bob-privatekey.pem
-rw-rw-r-- 1 corentin corentin 256 Nov 29 13:21 protected-key.bin
-rw-rw-r-- 1 corentin corentin 65 Nov 29 13:21 protected-message.txt
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q8 <master*>
$ openssl rsautl -decrypt -inkey bob-privatekey.pem -in protected-key.bin -out key.bin
Enter pass phrase for bob-privatekey.pem:
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q8 <master*>
$ openssl enc -d -aes-128-cbc -in protected-message.txt -out message.txt -base64 -kfile key.bin
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q8 <master*>
$ cat message.txt
Corentin GIRAUD
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/autumn-session/cryptography/tp3/q8 <master*>
$
```