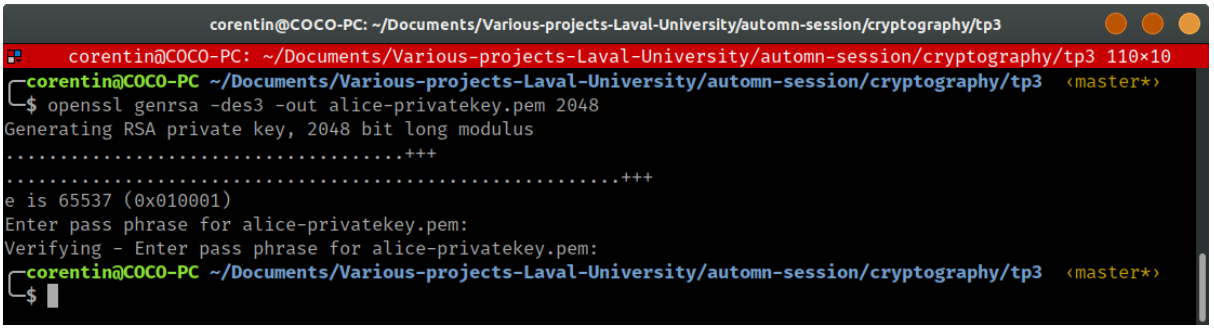
Corentin **GIRAUD**
NI: 111243057

UNIVERSITÉ LAVAL

Exercice 1

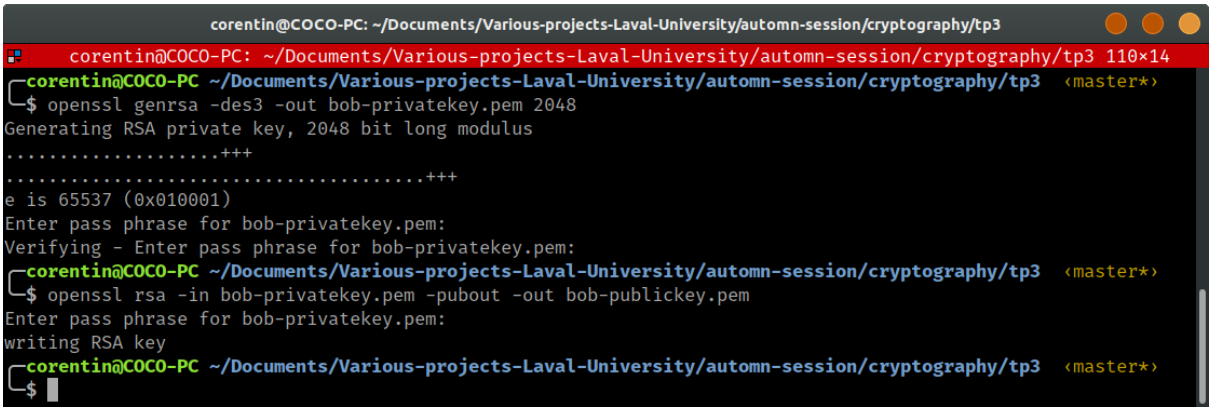
Question 1



Pass phrase: password

Question 2

Question 3



Pass phrase: password

Question 4

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/automn-session/cryptography/tp3
    corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/automn-session/cryptography/tp3 110×4
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/automn-session/cryptography/tp3  ‹master*›
$ echo "Corentin GIRAUD" > message.txt
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/automn-session/cryptography/tp3  ‹master*›
$
```

Question 5

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/automn-session/cryptography/tp3
    corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/automn-session/cryptography/tp3 110×5
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/automn-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/automn-session/cryptography/tp3  ‹master*›
$
```

Question 6

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/automn-session/cryptography/tp3
    corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/automn-session/cryptography/tp3 110×5
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/automn-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/automn-session/cryptography/tp3  ‹master*›
$
```

Question 7

```
corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/automn-session/cryptography/tp3/q7
    corentin@COCO-PC: ~/Documents/Various-projects-Laval-University/automn-session/cryptography/tp3/q7 115×21
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/automn-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/automn-session/cryptography/tp3/q7  ‹master*›
$ openssl rand -out key.bin 16
corentin@COCO-PC ~/Documents/Various-projects-Laval-University/automn-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/automn-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/automn-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/automn-session/cryptography/tp3/q7  ‹master*›
$
```

Corentin **GIRAUD**
NI: 111243057

UNIVERSITÉ LAVAL

Question 8