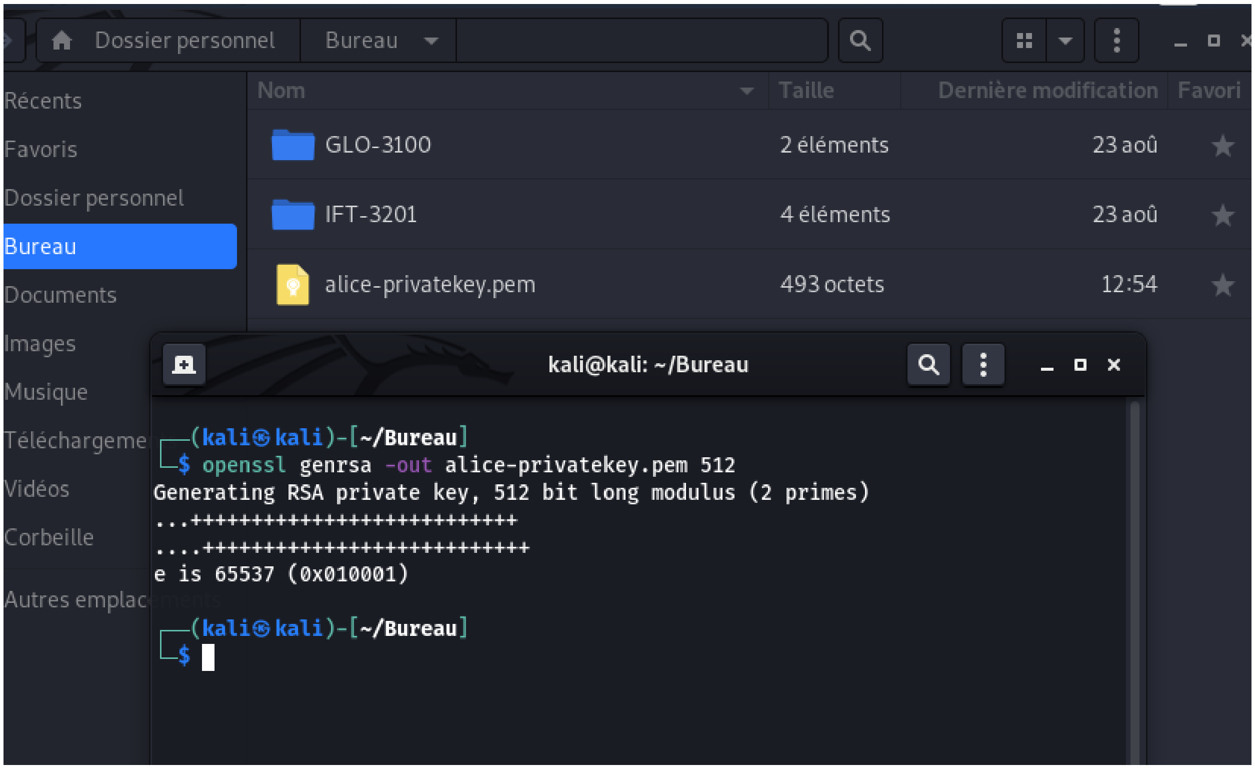
TP2

Exercice 3

Question 1

openssl genrsa -out alice-privatekey.pem 512



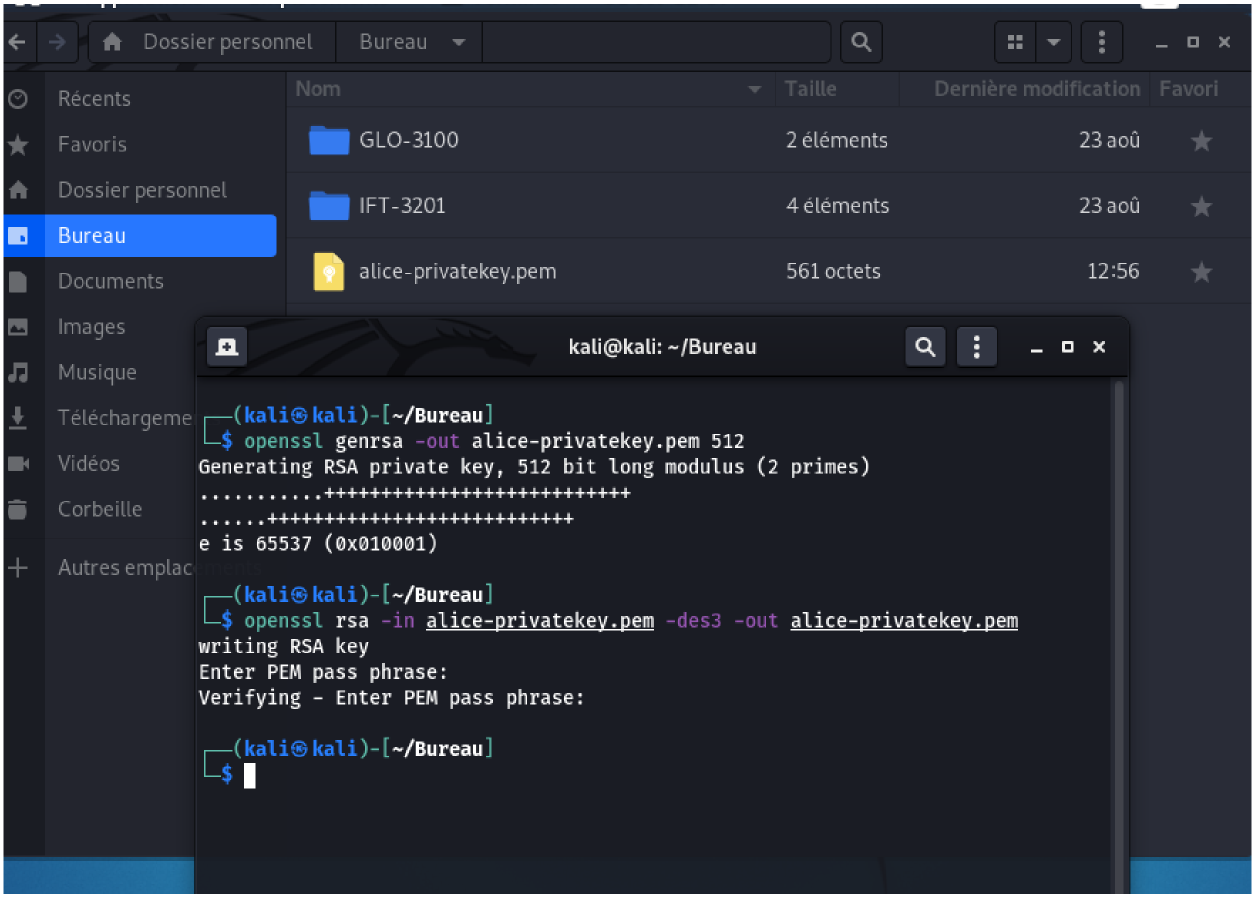
Nom	Taille	Dernière modification	Favori
GLO-3100	2 éléments	23 aoû	★
IFT-3201	4 éléments	23 aoû	★
alice-privatekey.pem	493 octets	12:54	★

```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl genrsa -out alice-privatekey.pem 512
Generating RSA private key, 512 bit long modulus (2 primes)
...+++++++++++++++++++++++++++
....+++++++++++++++++++++++++++
e is 65537 (0x010001)

┌──(kali㉿kali)-[~/Bureau]
└─$ 
```

openssl rsa -in alice-privatekey.pem -des3 -out alice-privatekey.pem

(mot de passe utilisé : “alice”)



Nom	Taille	Dernière modification	Favori
GLO-3100	2 éléments	23 aoû	★
IFT-3201	4 éléments	23 aoû	★
alice-privatekey.pem	561 octets	12:56	★

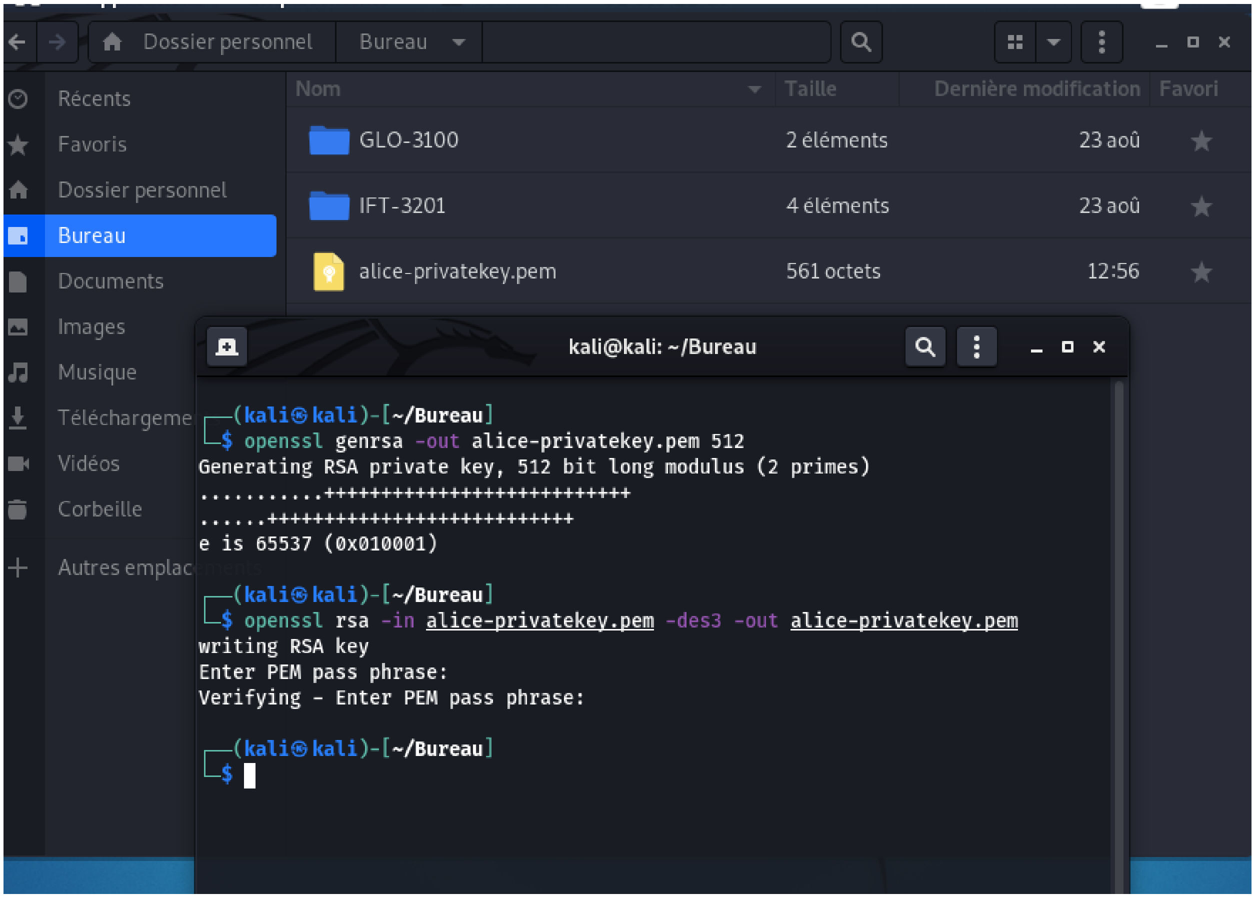
```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl genrsa -out alice-privatekey.pem 512
Generating RSA private key, 512 bit long modulus (2 primes)
..........+++++++++++++++++++++++++++
.....+++++++++++++++++++++++++++
e is 65537 (0x010001)

┌──(kali㉿kali)-[~/Bureau]
└─$ openssl rsa -in alice-privatekey.pem -des3 -out alice-privatekey.pem
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

┌──(kali㉿kali)-[~/Bureau]
└─$ █
```

Question 2

openssl rsa -in alice-privatekey.pem -pubout -out alice-publickey.pem



Nom	Taille	Dernière modification	Favori
GLO-3100	2 éléments	23 aoû	★
IFT-3201	4 éléments	23 aoû	★
alice-privatekey.pem	561 octets	12:56	★

```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl genrsa -out alice-privatekey.pem 512
Generating RSA private key, 512 bit long modulus (2 primes)
...........+++++++++++++++++++++++++++
......+++++++++++++++++++++++++++
e is 65537 (0x010001)

┌──(kali㉿kali)-[~/Bureau]
└─$ openssl rsa -in alice-privatekey.pem -des3 -out alice-privatekey.pem
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

┌──(kali㉿kali)-[~/Bureau]
└─$ █
```

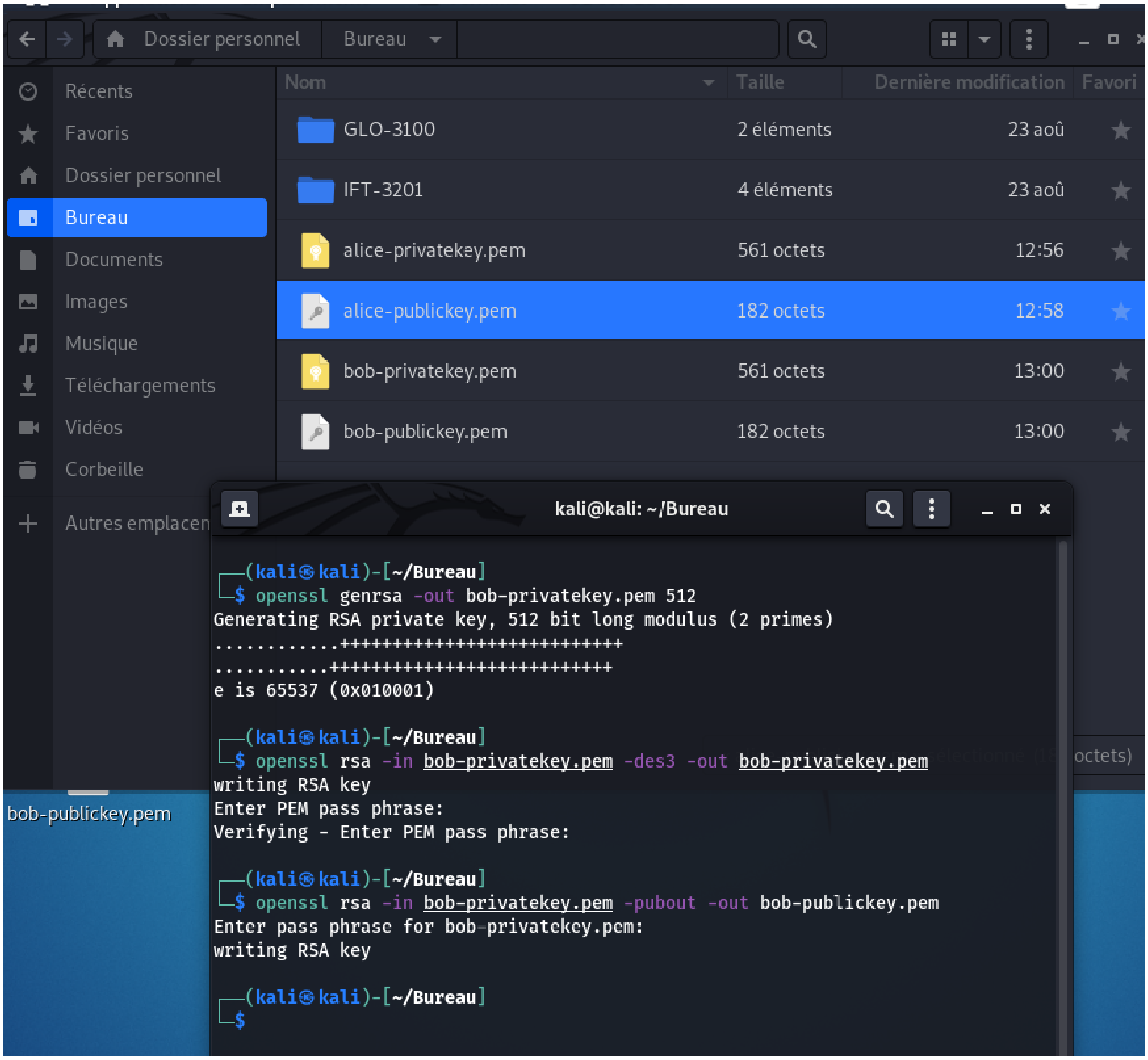
Question 3

openssl genrsa -out bob-privatekey.pem 512

openssl rsa -in bob-privatekey.pem -des3 -out bob-privatekey.pem

(mot de passe utilisé : “fabien” [“bob” n’était pas assez long])

openssl rsa -in bob-privatekey.pem -pubout -out bob-publickey.pem



Nom	Taille	Dernière modification	Favori
GLO-3100	2 éléments	23 aoû	★
IFT-3201	4 éléments	23 aoû	★
alice-privatekey.pem	561 octets	12:56	★
alice-publickey.pem	182 octets	12:58	★
bob-privatekey.pem	561 octets	13:00	★
bob-publickey.pem	182 octets	13:00	★

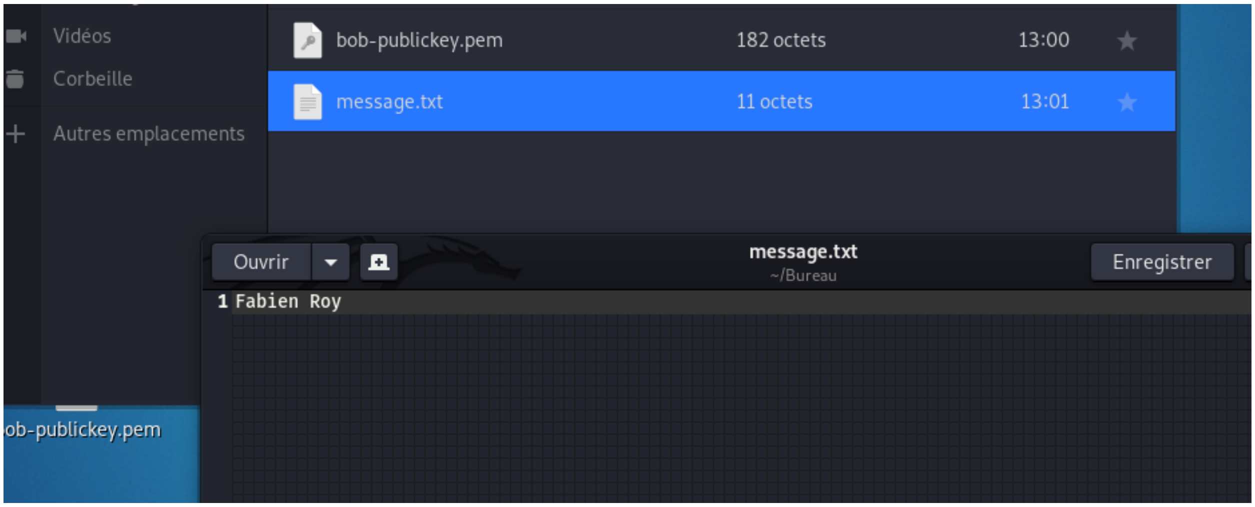
```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl genrsa -out bob-privatekey.pem 512
Generating RSA private key, 512 bit long modulus (2 primes)
...........+++++++++++++++++++++++++++
..........+++++++++++++++++++++++++++
e is 65537 (0x010001)

┌──(kali㉿kali)-[~/Bureau]
└─$ openssl rsa -in bob-privatekey.pem -des3 -out bob-privatekey.pem
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

┌──(kali㉿kali)-[~/Bureau]
└─$ openssl rsa -in bob-privatekey.pem -pubout -out bob-publickey.pem
Enter pass phrase for bob-privatekey.pem:
writing RSA key

┌──(kali㉿kali)-[~/Bureau]
└─$
```

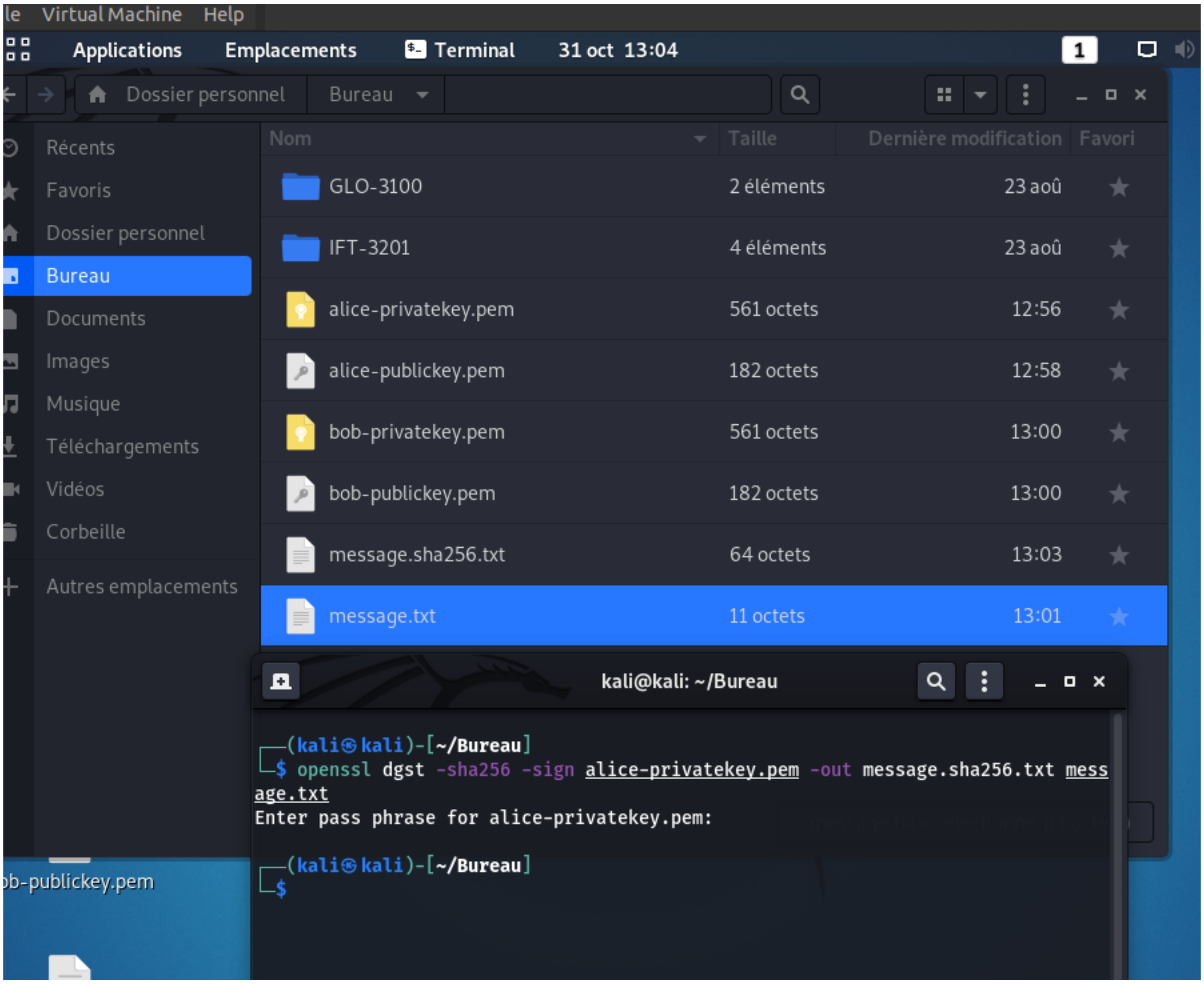
Question 4



```
1 Fabien Roy
```

Question 5

openssl gst -sha256 -sign alice-privatekey.pem -out message.sha256.txt message.txt



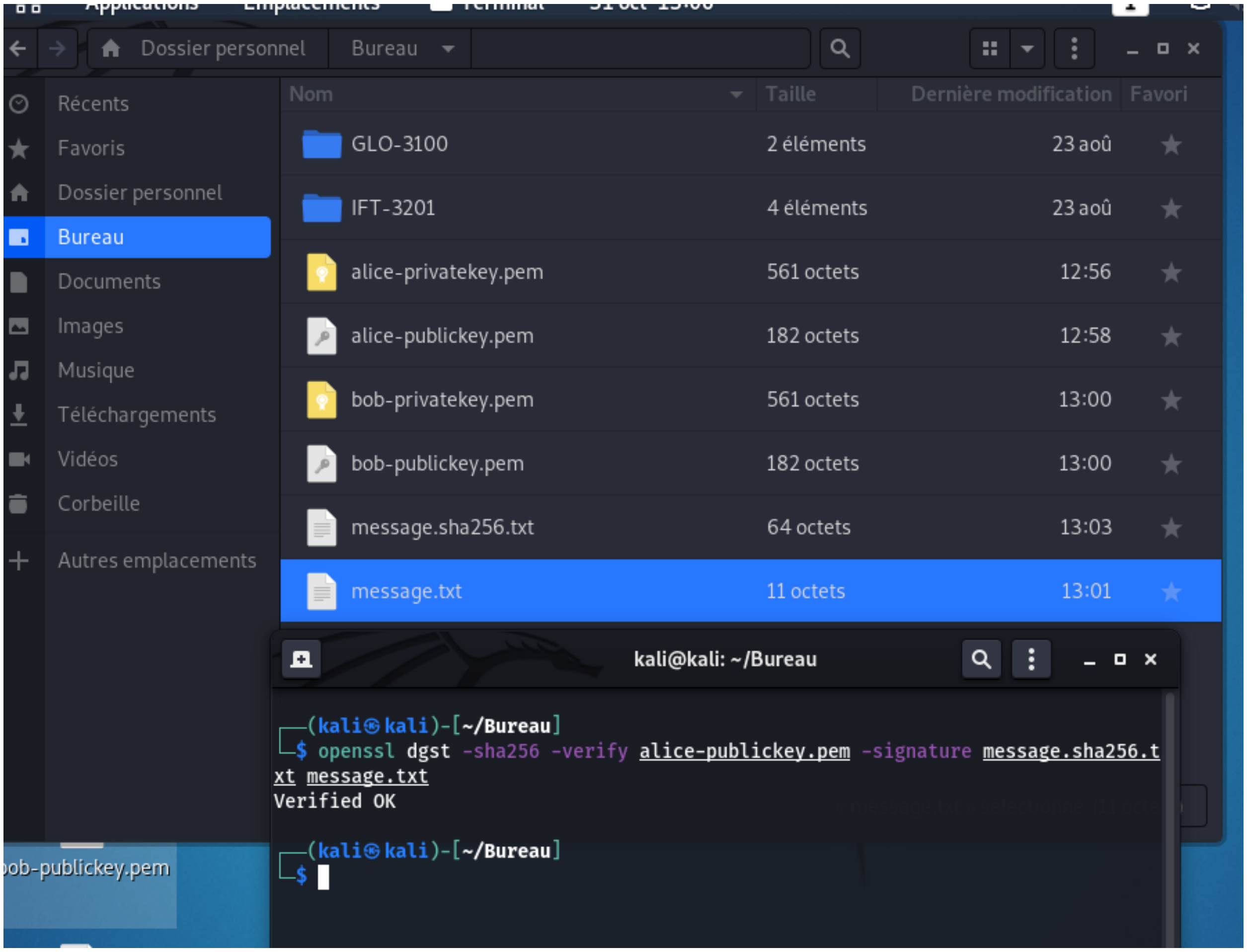
Nom	Taille	Dernière modification	Favori
GLO-3100	2 éléments	23 aoû	★
IFT-3201	4 éléments	23 aoû	★
alice-privatekey.pem	561 octets	12:56	★
alice-publickey.pem	182 octets	12:58	★
bob-privatekey.pem	561 octets	13:00	★
bob-publickey.pem	182 octets	13:00	★
message.sha256.txt	64 octets	13:03	★
message.txt	11 octets	13:01	★

```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl dgst -sha256 -sign alice-privatekey.pem -out message.sha256.txt mess
age.txt
Enter pass phrase for alice-privatekey.pem:

┌──(kali㉿kali)-[~/Bureau]
└─$
```

Question 6

openssl dgst -sha256 -verify alice-publickey.pem -signature message.sha256.txt message.txt



Nom	Taille	Dernière modification	Favori
GLO-3100	2 éléments	23 aoû	★
IFT-3201	4 éléments	23 aoû	★
alice-privatekey.pem	561 octets	12:56	★
alice-publickey.pem	182 octets	12:58	★
bob-privatekey.pem	561 octets	13:00	★
bob-publickey.pem	182 octets	13:00	★
message.sha256.txt	64 octets	13:03	★
message.txt	11 octets	13:01	★

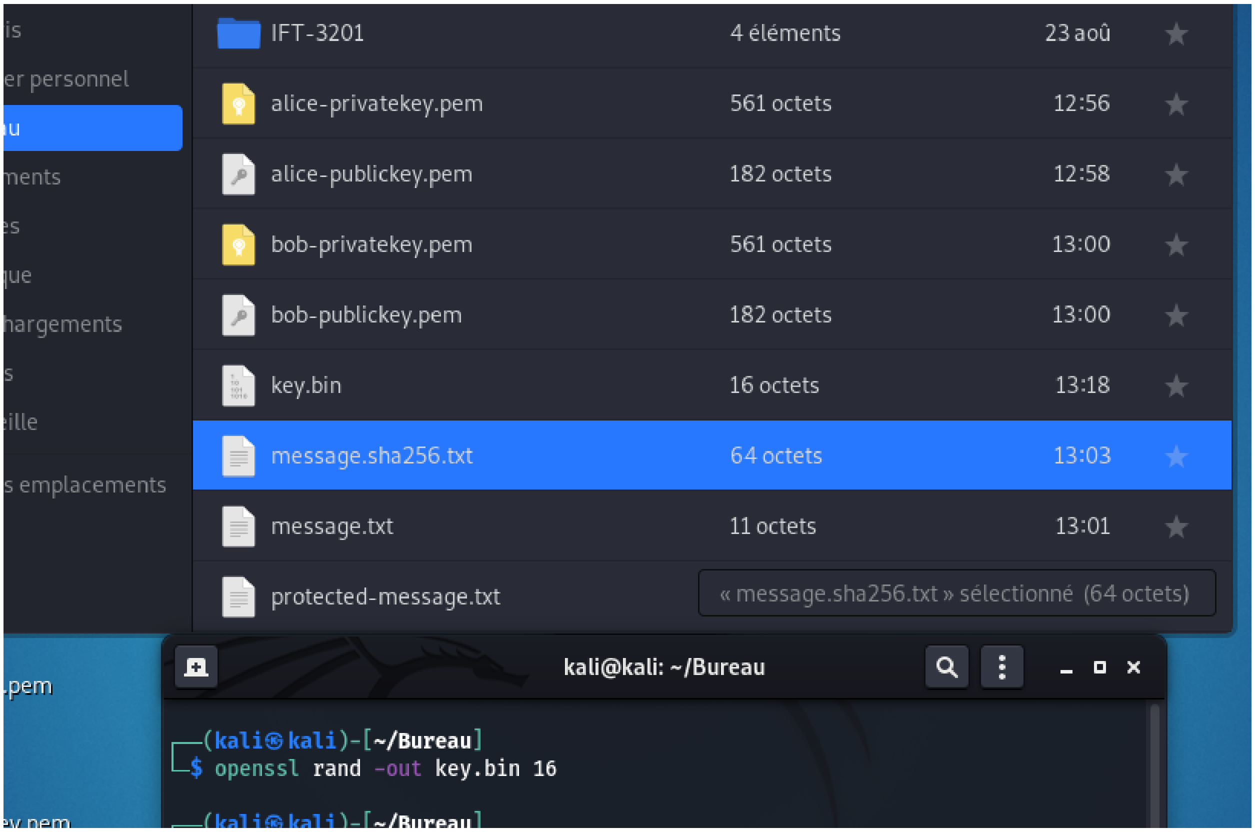
```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl dgst -sha256 -verify alice-publickey.pem -signature message.sha256.txt message.txt
Verified OK

┌──(kali㉿kali)-[~/Bureau]
└─$ 
```

Question 7

a

openssl rand -out key.bin 16



IFT-3201	4 éléments	23 aoû
alice-privatekey.pem	561 octets	12:56
alice-publickey.pem	182 octets	12:58
bob-privatekey.pem	561 octets	13:00
bob-publickey.pem	182 octets	13:00
key.bin	16 octets	13:18
message.sha256.txt	64 octets	13:03
message.txt	11 octets	13:01
protected-message.txt		

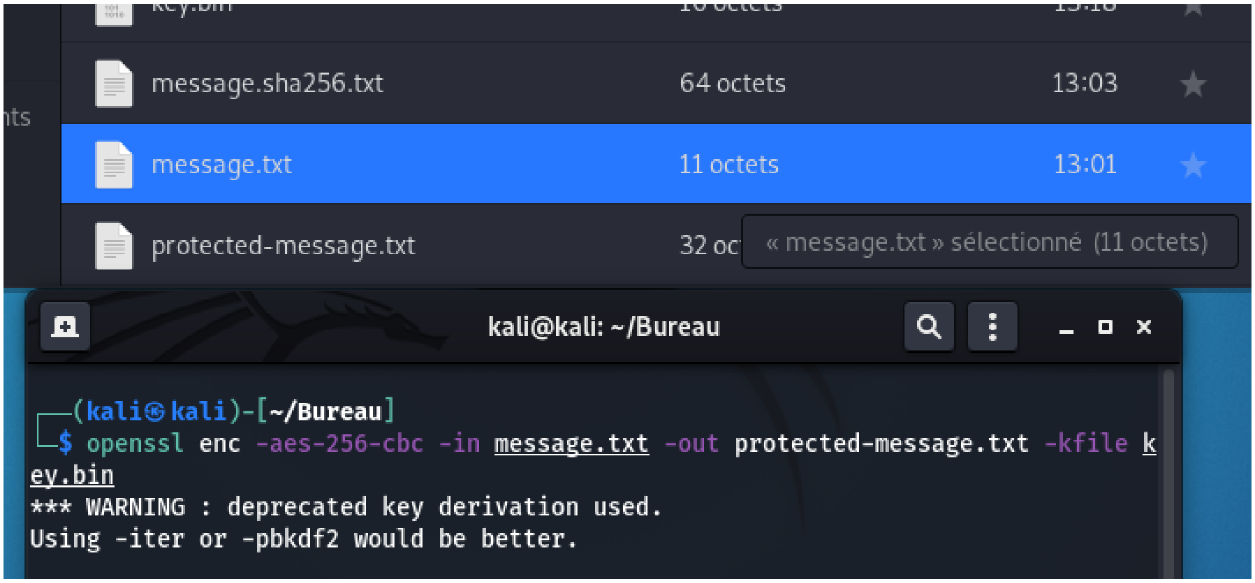
« message.sha256.txt » sélectionné (64 octets)

```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl rand -out key.bin 16

┌──(kali㉿kali)-[~/Bureau]
```

b

openssl enc -aes-256-cbc -in message.txt -out protected-message.txt -kfile key.bin



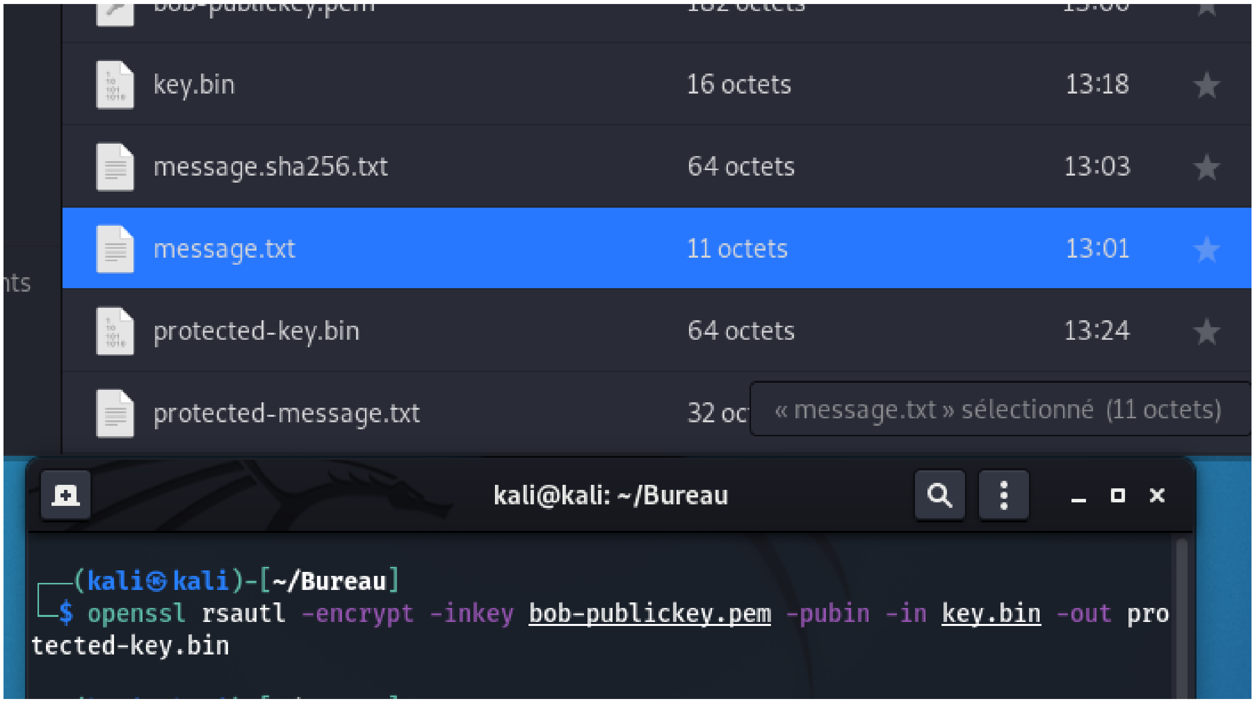
key.bin	16 octets	13:18
message.sha256.txt	64 octets	13:03
message.txt	11 octets	13:01
protected-message.txt	32 oc	

« message.txt » sélectionné (11 octets)

```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl enc -aes-256-cbc -in message.txt -out protected-message.txt -kfile k
ey.bin
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

C

openssl rsautl -encrypt -inkey bob-publickey.pem -pubin -in key.bin -out protected-key.bin



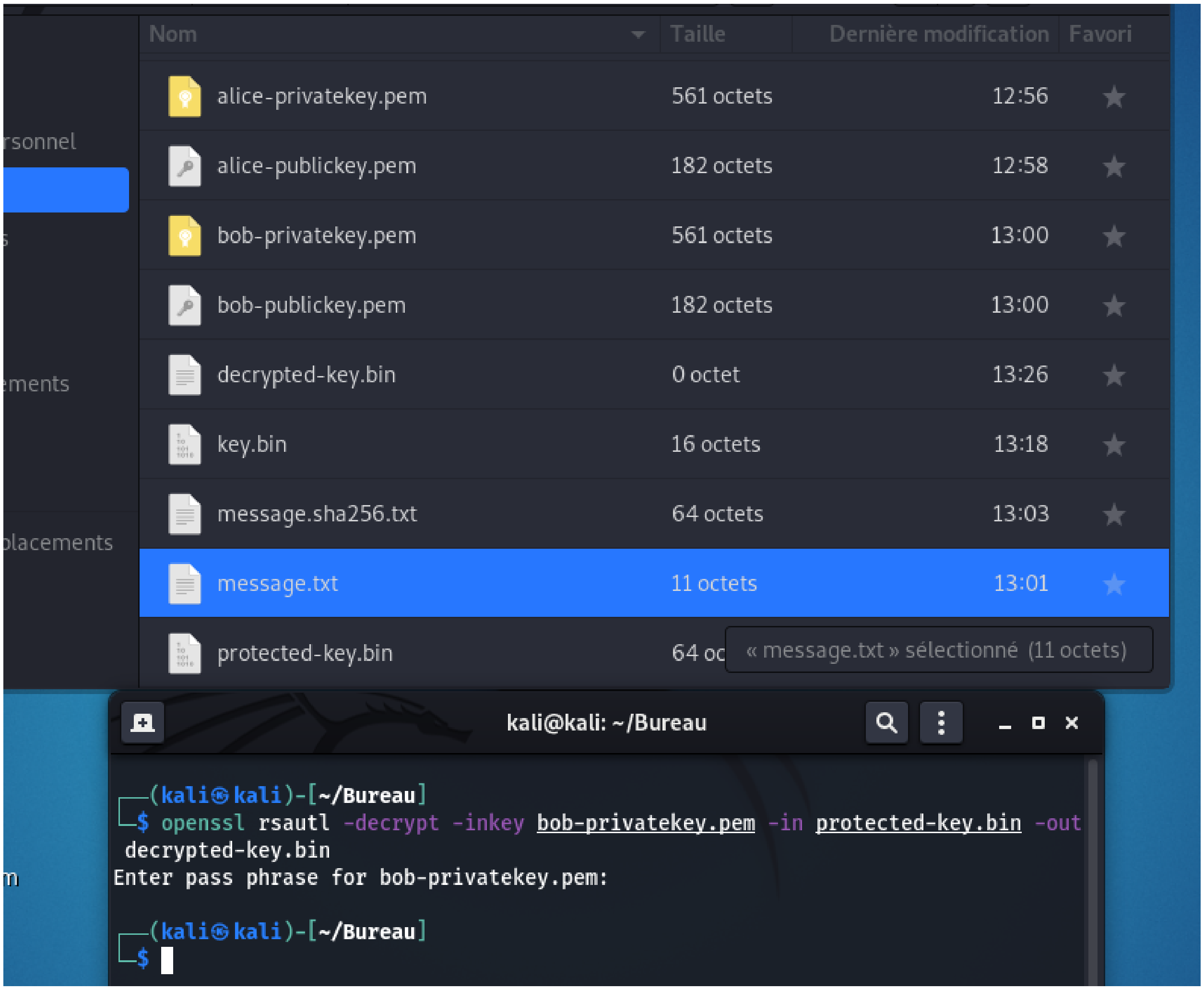
bob-publickey.pem	182 octets	13:00	★
key.bin	16 octets	13:18	★
message.sha256.txt	64 octets	13:03	★
message.txt	11 octets	13:01	★
protected-key.bin	64 octets	13:24	★
protected-message.txt	32 oc		

« message.txt » sélectionné (11 octets)

```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl rsautl -encrypt -inkey bob-publickey.pem -pubin -in key.bin -out pro
tected-key.bin
```

Question 8

openssl rsautl -decrypt -inkey bob-privatekey.pem -in protected-key.bin -out decrypted-key.bin



Nom	Taille	Dernière modification	Favori
alice-privatekey.pem	561 octets	12:56	★
alice-publickey.pem	182 octets	12:58	★
bob-privatekey.pem	561 octets	13:00	★
bob-publickey.pem	182 octets	13:00	★
decrypted-key.bin	0 octet	13:26	★
key.bin	16 octets	13:18	★
message.sha256.txt	64 octets	13:03	★
message.txt	11 octets	13:01	★
protected-key.bin	64 oc		

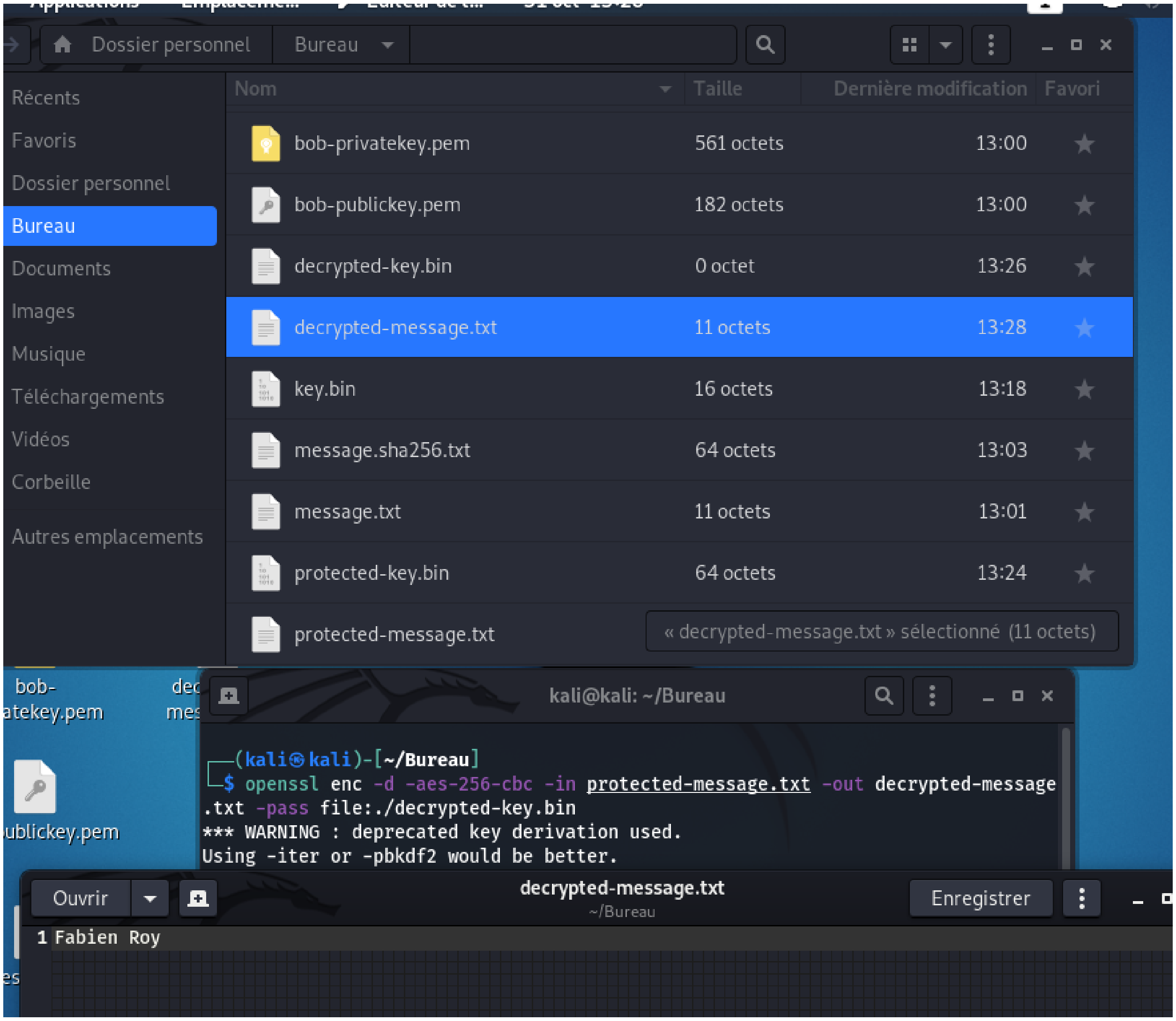
« message.txt » sélectionné (11 octets)

kali@kali: ~/Bureau

```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl rsautl -decrypt -inkey bob-privatekey.pem -in protected-key.bin -out
 decrypted-key.bin
Enter pass phrase for bob-privatekey.pem:

┌──(kali㉿kali)-[~/Bureau]
└─$ 
```

openssl enc -d -aes-256-cbc -in protected-message.txt -out decrypted-message.txt -pass file:./decrypted-key.bin



Nom	Taille	Dernière modification	Favori
bob-privatekey.pem	561 octets	13:00	★
bob-publickey.pem	182 octets	13:00	★
decrypted-key.bin	0 octet	13:26	★
decrypted-message.txt	11 octets	13:28	★
key.bin	16 octets	13:18	★
message.sha256.txt	64 octets	13:03	★
message.txt	11 octets	13:01	★
protected-key.bin	64 octets	13:24	★
protected-message.txt			

« decrypted-message.txt » sélectionné (11 octets)

```
┌──(kali㉿kali)-[~/Bureau]
└─$ openssl enc -d -aes-256-cbc -in protected-message.txt -out decrypted-message
.txt -pass file:./decrypted-key.bin
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

```
Fabien Roy
```