

II.2317 - Cybersecurity

Practical Work 1

LAB 1.....	1
LAB 2.....	7
LAB 3.....	14

GUO Xiaofan

LAB 1

1 Introduction to OpenSSL

5. - 7.

Terminal -

```
Fichier Édition Affichage Terminal Onglets Aide
xigu62705@pc-l305-7:/mnt/monster/home/elevex/x/xigu62705/openssl/openssl-1.0.0$ openssl version
OpenSSL 1.1.1q 5 Jul 2022
xigu62705@pc-l305-7:/mnt/monster/home/elevex/x/xigu62705/openssl/openssl-1.0.0$ cd
xigu62705@pc-l305-7:~$ ls
Bureau GUOXiaofan Modèles openssl Téléchargements
Documents Images Musique Public Vidéos
xigu62705@pc-l305-7:~$ mkdir LAB1
xigu62705@pc-l305-7:~$ cd LAB1
xigu62705@pc-l305-7:~/LAB1$ pwd
/home/elevex/x/xigu62705/LAB1
xigu62705@pc-l305-7:~/LAB1$ mkdir Alice
xigu62705@pc-l305-7:~/LAB1$ mkdir Bob
xigu62705@pc-l305-7:~/LAB1$ cd Alice
xigu62705@pc-l305-7:~/LAB1/Alice$ pwd
/home/elevex/x/xigu62705/LAB1/Alice
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit AliceDocument

(gedit:30781): Gtk-WARNING ***: 14:59:00.458: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: La méthode « Inhibit » n'existe pas
xigu62705@pc-l305-7:~/LAB1/Alice$ openssl genrsa -out AliceKeyPair
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
xigu62705@pc-l305-7:~/LAB1/Alice$ ls
AliceDocument AliceKeyPair
xigu62705@pc-l305-7:~/LAB1/Alice$
```

Terminal -

```
Fichier Édition Affichage Terminal Onglets Aide
Valid options are:
-help          Display this summary
-inform format Input format, one of DER PEM
-outform format Output format, one of DER PEM PKCS8
-in val         Input file
-out outfile   Output file
-pubin         Expect a public key in input file
-pubout        Output a public key
-passout val   Output file pass phrase source
-passin val   Input file pass phrase source
-RSAPublicKey_in Input is an RSAPublicKey
-RSAPublicKey_out Output is an RSAPublicKey
-noout         Don't print key out
-text          Print the key in text
-modulus       Print the RSA key modulus
-check         Verify key consistency
-*             Any supported cipher
-pvk-strong    Enable 'Strong' PKV encoding level (default)
-pvk-weak      Enable 'Weak' PKV encoding level
-pvk-none     Don't enforce PKV encoding
-engine val   Use engine, possibly a hardware device
xigu62705@pc-l305-7:~/LAB1/Alice$ ls
AliceDocument AliceKeyPair AlicePublicKey
xigu62705@pc-l305-7:~/LAB1/Alice$ mv AliceKeyPair AlicePrivateKey
mv: impossible d'évaluer 'AliceKeyPair': Aucun fichier ou dossier de ce type
xigu62705@pc-l305-7:~/LAB1/Alice$ mv AliceKeyPair AlicePrivateKey
xigu62705@pc-l305-7:~/LAB1/Alice$ ls
AliceDocument AlicePrivateKey AlicePublicKey
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit AlicePublicKey
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit AlicePrivateKey
```

AlicePrivateKey

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAoAQGry0qUS20CQw0Sg6TH3hGg5ggR4dnbbssSIVmabM9U
3gcj2JcxBAAMBzrm8Gq+xHs63Wu3z46tCbvjjd4HvETAFJ8TyK9v58+g064c+xPmr
4u0QszRJTPP7zgErU/07QWQJART/B1SYy0NLY6CgMiAJUEWjqDLw6X7pY7zvYfbQ0n
5yofLk10KGbC1sDn0dBnZhrWM2/frlrye2VZP809y5fB5/80wtMVbfo+U0i9wcZ0
6Ex9BwyzhU801YoMtqZme+JzerIrLyjDg5PKXB7+3Nvi2Rp0zOhdn3Wa/Q+Ee9txUx
7hch0IuMy3M7ak3YyGtF0dc+no7qNianbZ144JwIDAQABoIBAF8IS5Rth5EwgPlpR
8Ngtnw/AoFgvNv/TRM0+6u62zuZhly1rzqoEXMLHSI/43P0wtHo4/H4hg617y8hXW
9Yfx1Q8x3fa/+MCGLg5ru4+2rV1k7EtqK7Aalf+IvzwX7+YpzQVYvr7KmetftlAu
10Y9ymmaWPpnwoBNs9yeo0EfwlAdHD3nDrMI0N3ofwMMWULvIp++vdBRmDRSu
11tvSTSFn2lh1YTZWW/L0ampAUxDH+JftRQY1xyqCebkbCa7YDM2N080EYRcrmInV
12tg01LwvR7JYRC6Nxw90NB9ruNzML640w06hplbAC5wdI4Zq3WvIlYaZm0tJBW
13biCe4KcgYAz6hUuYf0C3oMgEzTnGyh65vuuwK0MexULChxEI3RU03q5X1YNG6
14/1MdhwvZa3gKowcvNzB0JK3y6cKuAjxK4q7SsuAsfp-doiFB
15Bfy01hhDNPw8zs1jB1mxHf7yDDlyDv0ST7yBAXiamUpJq3ppdGRkMcgYEAxUrO
16gkgt1gTkjhFzE29CsYIPBn1ZTa01L650GVRLkvqM6D0IV2VoFeg0ta5QkunYJ9
17PuGludZ4LExEk9ESZcgCvEHdT8g0sRuiBzsDZeNzv2+uGozyk49Bed48rkPQ/Wt
18hhC00Bygv9v4ZNaTsDE872yc/uaptLDarFWMk0CgYA+LGhooj5HrPHeCkrfoJ6
19udmn+NvwKaqAeTp3xS0kPLhcUWVb0cIAPi0dpJ72Tlyw7yAUJ4e+q649Pj8+i5p
202A+heU6R85GmMlcY+DixBgbL6Mcte0nkD18/6MFghYtgTjt8yeBHULcchcAHL
21usth+D0u0Rc3BgPSTAAmzQKBgFCxQu6UN+b73rw1zhtNFkL2KJ9G9xjDNoJik3FJ
22DK0q1NMJhEgZt/L0PLBX6kAsIjRz0ziBq4xxJnr0y1XqbzzfK/96EflopFneK9E
235wp7EAxm8Rj7Pt8Ny0mVXTMLmpmPKzyayWu0dUkkXR5Y277mkh2LaV13nwPhz
24wgahAoGBAjnL/ue7ENiMbaAfjojU0L8+y0z9hpARixfeDmuwenzG4g1TZisLkvBD
2570e+0ckPii/CruHhIgDx1CM/p3hyHXUVUK075kwjzka0+p5dkuxB3AUg4b4/JBM
26CQyY70JI+Pg92W7jnxcvSYX0BVN0VYjxmXAnGh6wyTfsmyxW7i
27-----END RSA PRIVATE KEY-----
```

Texte brut ▾ Largeur des tabulations : 8 ▾ Lig 1, Col 1 ▾ INS

2 Exercise “Asymmetric cryptography”

Terminal -

```

Fichier Édition Affichage Terminal Onglets Aide
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit AlicePrivateKey
xigu62705@pc-l305-7:~/LAB1/Alice$ cd
bash: cd: Bob: Aucun fichier ou dossier de ce type
xigu62705@pc-l305-7:~$ cd LAB1
xigu62705@pc-l305-7:~/LAB1$ cd Bob
xigu62705@pc-l305-7:~/LAB1/Bob$ pwd
/home/eleves/x/xigu62705/LAB1/Bob
xigu62705@pc-l305-7:~/LAB1/Bob$ gedit BobDocument

(gedit:32715): Gtk-WARNING **: 15:11:19.562: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: La méthode « Inhibit » n'existe pas
xigu62705@pc-l305-7:~/LAB1/Bob$ openssl genrsa -out BobKeyPair
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
xigu62705@pc-l305-7:~/LAB1/Bob$ ls
BobDocument BobKeyPair
xigu62705@pc-l305-7:~/LAB1/Bob$ openssl rsa -in BobKeyPair -pubout -out BobPublicKey
writing RSA key
xigu62705@pc-l305-7:~/LAB1/Bob$ ls
BobDocument BobKeyPair BobPublicKey
xigu62705@pc-l305-7:~/LAB1/Bob$ mv BobKeyPair BobPrivateKey
xigu62705@pc-l305-7:~/LAB1/Bob$ ls
BobDocument BobPrivateKey BobPublicKey
xigu62705@pc-l305-7:~/LAB1/Bob$ gedit BobPublicKey

```

BobPublicKey

1.(c)

Terminal -

```

Fichier Édition Affichage Terminal Onglets Aide
xigu62705@pc-l305-7:~/LAB1/Alice$ cd
xigu62705@pc-l305-7:~$ cd Bob
bash: cd: Bob: Aucun fichier ou dossier de ce type
xigu62705@pc-l305-7:~$ cd LAB1
xigu62705@pc-l305-7:~/LAB1$ cd Bob
xigu62705@pc-l305-7:~/LAB1/Bob$ pwd
/home/eleves/x/xigu62705/LAB1/Bob
xigu62705@pc-l305-7:~/LAB1/Bob$ gedit BobDocument

(gedit:32715): Gtk-WARNING **: 15:11:19.562: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: La méthode « Inhibit » n'existe pas
xigu62705@pc-l305-7:~/LAB1/Bob$ openssl genrsa -out BobKeyPair
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
xigu62705@pc-l305-7:~/LAB1/Bob$ ls
BobDocument BobKeyPair
xigu62705@pc-l305-7:~/LAB1/Bob$ openssl rsa -in BobKeyPair -pubout -out BobPublicKey
writing RSA key
xigu62705@pc-l305-7:~/LAB1/Bob$ ls
BobDocument BobKeyPair BobPublicKey
xigu62705@pc-l305-7:~/LAB1/Bob$ mv BobKeyPair BobPrivateKey
xigu62705@pc-l305-7:~/LAB1/Bob$ ls
BobDocument BobPrivateKey BobPublicKey
xigu62705@pc-l305-7:~/LAB1/Bob$ gedit BobPublicKey

```

BobPublicKey

1.(c)

```

xigu62705@pc-l305-7:~/LAB1/Bob$ pwd
/home/eleves/x/xigu62705/LAB1/Bob
xigu62705@pc-l305-7:~/LAB1/Bob$ cp /home/eleves/x/xigu62705/LAB1/Bob/BobPublicKey
y /home/eleves/x/xigu62705/LAB1/Alice/
xigu62705@pc-l305-7:~/LAB1/Bob$ cd..
cd.. : commande introuvable
xigu62705@pc-l305-7:~/LAB1/Bob$ cd ..
xigu62705@pc-l305-7:~/LAB1$ cd Alice
xigu62705@pc-l305-7:~/LAB1/Alice$ ls
AliceDocument AlicePrivateKey AlicePublicKey BobPublicKey
xigu62705@pc-l305-7:~/LAB1/Alice$ 
```

2.(c)

2.(d)

Terminal -

Fichier Édition Affichage Terminal Onglets Aide

```
xigu62705@pc-l305-7:~/LAB1/Alice$ openssl rsautl -help
Usage: rsautl [options]
Valid options are:
-help Display this summary
-in infile Input file
-out outfile Output file
-inkey val Input key
-keyform PEM|DER|ENGINE Private key format - default PEM
-pubin Input is an RSA public
-certin Input is a cert carrying an RSA public key
-ssl Use SSL v2 padding
-raw Use no padding
-pkcs Use PKCS#1 v1.5 padding (default)
-oaep Use PKCS#1 OAEP
-sign Sign with private key
-verify Verify with public key
-asn1parse Run output through asn1parse; useful with -verify
-hexdump Hex dump output
-x931 Use ANSI X9.31 padding
-rev Reverse the order of the input buffer
-encrypt Encrypt with public key
-decrypt Decrypt with private key
-passin val Input file pass phrase source
-rand val Load the file(s) into the random number generator
-writerand outfile Write random data to the specified file
-engine val Use engine, possibly a hardware device
xigu62705@pc-l305-7:~/LAB1/Alice$ ls
AliceDocumentEncrypted AlicePrivateKey BobPublicKey
AliceDocument AlicePublicKey
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit AliceDocumentEncrypted
```

2.(g)

Fichier Édition Affichage Terminal Onglets Aide

```
xigu62705@pc-l213-9:/mnt/monster/home/eleves/x/xigu62705/Bureau$ cd
xigu62705@pc-l213-9:~$ cd LAB1
xigu62705@pc-l213-9:~/LAB1$ cd Alice
xigu62705@pc-l213-9:~/LAB1/Alice$ gedit AliceDocumentEncrypted
```

2.(h)

We cannot directly read the content in AliceDocumentEncrypted
(it will appear as garbled characters)

```
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit AliceDocumentEncrypted  
xigu62705@pc-l305-7:~/LAB1/Alice$ cp /home/eleves/x/xigu62705/LAB1/Alice/AliceDo  
cumentEncrypted /home/eleves/x/xigu62705/LAB1/Bob/  
cp: impossible d'évaluer '/home/eleves/x/xigu62705/LAB1/Alice/AliceDocumentEncry  
pted': Aucun fichier ou dossier de ce type  
xigu62705@pc-l305-7:~/LAB1/Alice$ cp /home/eleves/x/xigu62705/LAB1/Alice/AliceDo  
cumentEncrypted /home/eleves/x/xigu62705/LAB1/Bob/
```

3.(a)

3.(b) xigu62705@pc-l305-7:~/LAB1/Alice\$ cd ..

xigu62705@pc-l305-7:~/LAB1\$ cd Bob

3.(c) xigu62705@pc-l305-7:~/LAB1/Bob\$ ls
AliceDocumentEncrypted BobDocument BobPrivateKey BobPublicKey
xigu62705@pc-l305-7:~/LAB1/Bob\$

```
xigu62705@pc-l305-7:~/LAB1/Bob$ openssl rsautl -decrypt -in AliceDocumentEncrypt  
ed -inkey BobPrivateKey -out AliceDocumentDecrypted
```

3.(d)

3.(e) xigu62705@pc-l305-7:~/LAB1/Bob\$ ls
AliceDocumentDecrypted BobDocument BobPublicKey
AliceDocumentEncrypted BobPrivateKey

```
xigu62705@pc-l305-7:~/LAB1/Bob$ gedit AliceDocumentDecrypted
```

The screenshot shows a Gedit window with the title "AliceDocumentDecrypted". The content of the file is displayed as follows:
1 Hello Bob, I'm Alice
2 |

3.(f)

After completing the decoding operation, we can read the initial content written to AliceDocument in the AliceDocumentDecrypted file in Bob's folder.

```
xigu62705@pc-l305-7:~/LAB1/Bob$ cd ..  
xigu62705@pc-l305-7:~/LAB1$ cd Alice
```

4.(a)

The screenshot shows a terminal window with the following command history:
xigu62705@pc-l305-7:~/LAB1\$ dd if=/dev/urandom of=LargeFile bs=1M count=100
xigu62705@pc-l305-7:~/LAB1\$ cd ..
xigu62705@pc-l305-7:~/LAB1\$ cd Alice
xigu62705@pc-l305-7:~/LAB1/Alice\$ pwd
/home/eleves/x/xigu62705/LAB1/Alice

4.(c)

```
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit AuthData
```

5.(a)

```
(gedit:39883): Gtk-WARNING **: 15:59:36.159: Calling org.xfce.Session.Manager.In  
hibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: La méthode «  
Inhibit » n'existe pas
```

```
xigu62705@pc-l305-7:~/LAB1/Alice$ ls  
AliceDocument AlicePublicKey HashAuthData  
AliceDocumentEncrypted AuthData LargeFile  
AlicePrivateKey BobPublicKey LargeFileEncrypted
```

5.(b)

```
xigu62705@pc-l305-7:~/LAB1/Alice$ cp /home/eleves/x/xigu62705/LAB1/Alice/AlicePublicKey /home/eleves/x/xigu62705/LAB1/Bob/
```

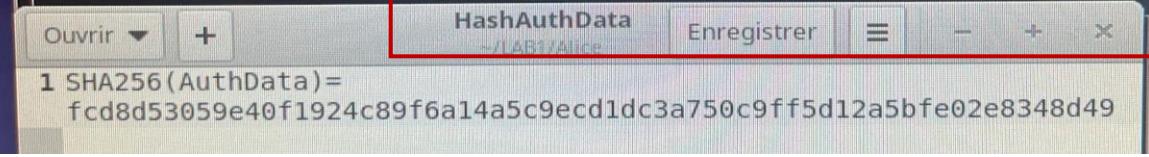
5.(c)

```
xigu62705@pc-l305-7:~/LAB1/Alice$ openssl dgst -sha256 -out HashAuthData AuthData
```

a

```
xigu62705@pc-l305-7:~/LAB1/Alice$ ls AliceDocument AlicePublicKey HashAuthData  
AliceDocumentEncrypted AuthData LargeFile  
AlicePrivateKey BobPublicKey LargeFileEncrypted
```

```
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit HashAuthData
```



The screenshot shows a Gedit window with the title bar 'HashAuthData'. The content of the file is a single line of text: 'SHA256(AuthData)= fcd8d53059e40f1924c89f6a14a5c9ecd1dc3a750c9ff5d12a5bfe02e8348d49'.

5.(e)

5.(f)

```
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit HashAuthData
```

```
xigu62705@pc-l305-7:~/LAB1/Alice$ openssl rsautl -sign -in HashAuthData -inkey AlicePrivateKey -out AliceSignature
```

5.(g)

```
xigu62705@pc-l305-7:~/LAB1/Alice$ openssl rsautl -help
```

```
Usage: rsautl [options]
```

```
Valid options are:
```

-help	Display this summary
-in infile	Input file
-out outfile	Output file
-inkey val	Input key
-keyform PEM DER ENGINE	Private key format - default PEM
-pubin	Input is an RSA public
-certin	Input is a cert carrying an RSA public key
-ssl	Use SSL v2 padding
-raw	Use no padding
-pkcs	Use PKCS#1 v1.5 padding (default)
-oaep	Use PKCS#1 OAEP
-sign	Sign with private key
-verify	Verify with public key
-asn1parse	Run output through asn1parse; useful with -verify
-hexdump	Hex dump output
-x931	Use ANSI X9.31 padding
-rev	Reverse the order of the input buffer
-encrypt	Encrypt with public key
-decrypt	Decrypt with private key
-passin val	Input file pass phrase source
-rand val	Load the file(s) into the random number generator
-writerand outfile	Write random data to the specified file
-engine val	Use engine, possibly a hardware device

```
xigu62705@pc-l305-7:~/LAB1/Alice$ ls
```

```
AliceDocument AlicePublicKey BobPublicKey LargeFileEncrypted
```

```
AliceDocumentEncrypted AliceSignature HashAuthData
```

```
AlicePrivateKey AuthData LargeFile
```

```
xigu62705@pc-l305-7:~/LAB1/Alice$
```

```
xigu62705@pc-l305-7:~/LAB1/Alice$ ls
AliceDocument          AlicePublicKey  BobPublicKey  LargeFileEncrypted
AliceDocumentEncrypted AliceSignature  HashAuthData
AlicePrivateKey        AuthData       LargeFile
xigu62705@pc-l305-7:~/LAB1/Alice$ cp /home/elevex/x/xigu62705/LAB1/Alice/AliceSi
gnature /home/elevex/x/xigu62705/LAB1/Bob/
xigu62705@pc-l305-7:~/LAB1/Alice$ cp /home/elevex/x/xigu62705/LAB1/Alice/AuthDat
a /home/elevex/x/xigu62705/LAB1/Bob/
xigu62705@pc-l305-7:~/LAB1/Alice$ cd ..
xigu62705@pc-l305-7:~/LAB1$ cd Bob
xigu62705@pc-l305-7:~/LAB1/Bob$ ls
AliceDocumentDecrypted AlicePublicKey  AuthData      BobPrivateKey
AliceDocumentEncrypted AliceSignature   BobDocument  BobPublicKey
xigu62705@pc-l305-7:~/LAB1/Bob$
```

```
xigu62705@pc-l305-7:~/LAB1/Bob$ cd ..
xigu62705@pc-l305-7:~/LAB1$ cd Alice
xigu62705@pc-l305-7:~/LAB1/Alice$ openssl rsautl -verify -in AliceSignature -pub
in -inkey AlicePublicKey -out HashAuthData
xigu62705@pc-l305-7:~/LAB1/Alice$ openssl rsautl -verify -in AliceSignature -pub
in -inkey AlicePublicKey -out HashAuthData
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit HashAuthData
```

```
xigu62705@pc-l305-7:~/LAB1/Alice$ openssl dgst -sha256 -out HashBob AuthData
xigu62705@pc-l305-7:~/LAB1/Alice$ ls
AliceDocument          AlicePublicKey  BobPublicKey  LargeFile
AliceDocumentEncrypted AliceSignature  HashAuthData  LargeFileEncrypted
AlicePrivateKey        AuthData       HashBob
xigu62705@pc-l305-7:~/LAB1/Alice$
```

```
xigu62705@pc-l305-7:~/LAB1/Bobs$ cd ..
xigu62705@pc-l305-7:~/LAB1$ cd Alice
xigu62705@pc-l305-7:~/LAB1/Alices$ openssl rsautl -verify -in AliceSignature -pub
in -inkey AlicePublicKey -out HashAuthData
xigu62705@pc-l305-7:~/LAB1/Alices$ openssl rsautl -verify -in AliceSignature -pub
in -inkey AlicePublicKey -out HashAuthData
xigu62705@pc-l305-7:~/LAB1/Alices$ gedit HashAuthData
xigu62705@pc-l305-7:~/LAB1/Alices$ openssl dgst -sha256 -out HashBob AuthData
xigu62705@pc-l305-7:~/LAB1/Alice$ ls
AliceDocument          AlicePublicKey  BobPublicKey  LargeFile
AliceDocumentEncrypted AliceSignature  HashAuthData  LargeFileEncrypted
AlicePrivateKey        AuthData       HashBob
xigu62705@pc-l305-7:~/LAB1/Alice$ diff HashBob HashAuthData
xigu62705@pc-l305-7:~/LAB1/Alice$ gedit HashBob
```

5.(n)

```
(gedit:43805): Gtk-WARNING **: 16:24:07.203: Calling org.xfce.Session.Manager.In
hibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: La méthode «
Inhibit » n'existe pas
xigu62705@pc-l305-7:~/LAB1/Alice$ diff HashBob HashAuthData
1cl
< SHA256(AuthData)= cd8d53059e40f1924c89f6a14a5c9ecd1dc3a750c9ff5d12a5bfe02e8348
d49
---
> SHA256(AuthData)= fcd8d53059e40f1924c89f6a14a5c9ecd1dc3a750c9ff5d12a5bfe02e834
8d49
```

5.(o)

LAB 2

1 Exercise “Symmetric cryptography”

```
xigu62705@pc-l305-7:~$ mkdir LAB2
xigu62705@pc-l305-7:~$ cd LAB2
xigu62705@pc-l305-7:~/LAB2$ mkdir Alice
xigu62705@pc-l305-7:~/LAB2$ mmdir Bob
La commande « mmdir » n'a pas été trouvée, voulez-vous dire :
  commande « rmdir » du deb coreutils (8.32-4.1ubuntu1)
  commande « mkdir » du deb coreutils (8.32-4.1ubuntu1)
  commande « mmdir » du deb simh (3.8.1-6.1)
  commande « mdir » du deb mtools (4.0.33-1+really4.0.32-1build1)
Essayez : apt install <nom du deb>
xigu62705@pc-l305-7:~/LAB2$ mkdir Bob
xigu62705@pc-l305-7:~/LAB2$ cd Alice
xigu62705@pc-l305-7:~/LAB2/Alice$ ls
AliceDocument AlicePrivateKey AlicePublicKey
xigu62705@pc-l305-7:~/LAB2/Alice$ cd ..
xigu62705@pc-l305-7:~/LAB2$ cd Bob
xigu62705@pc-l305-7:~/LAB2/Bob$ ls
BobDocument BobPrivateKey BobPublicKey
xigu62705@pc-l305-7:~/LAB2/Bob$
```

```
xigu62705@pc-l305-7:~/LAB2/Bob$ gedit AuthDataBob
(gedit:45596): Gtk-WARNING **: 16:35:29.942: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: La méthode « Inhibit » n'existe pas
xigu62705@pc-l305-7:~/LAB2/Bob$ gedit AuthDataBob
```



2.(b)

```
xigu62705@pc-l305-7:~/LAB2/Bob$ gedit AuthDataBob
xigu62705@pc-l305-7:~/LAB2/Bob$ openssl dgst -sha256 -sign BobPrivateKey -out BobSignature AuthDataBob
xigu62705@pc-l305-7:~/LAB2/Bob$ cp /home/elevex/x/xigu62705/LAB2/Bob/AuthDataBob
/home/elevex/x/xigu62705/LAB2/Alice
xigu62705@pc-l305-7:~/LAB2/Bob$ cp /home/elevex/x/xigu62705/LAB2/Bob/BobSignature
/home/elevex/x/xigu62705/LAB2/Alice
xigu62705@pc-l305-7:~/LAB2/Bob$ cp /home/elevex/x/xigu62705/LAB2/Bob/BobPublicKey
/home/elevex/x/xigu62705/LAB2/Alice
xigu62705@pc-l305-7:~/LAB2/Bob$ cd ..
xigu62705@pc-l305-7:~/LAB2$ cd Alice
xigu62705@pc-l305-7:~/LAB2/Alice$ ls
AliceDocument AlicePublicKey BobPublicKey
AlicePrivateKey AuthDataBob BobSignature
xigu62705@pc-l305-7:~/LAB2/Alice$
```

2.(c)

```

xigu62705@pc-l305-7:~/LAB2/Alice$ openssl dgst -sha256 -sign BobPublicKey -out BobSignature AuthDataBob
The data was indeed signed by BobPrivateKey, the
unable to load key file BobPublicKey cannot read.
140574057461568:error:0909006C:PEM routines:get_name:no start line:crypto/pem/pe
m lib.c:745:Expecting: ANY PRIVATE KEY
xigu62705@pc-l305-7:~/LAB2/Alice$ openssl dgst -help
Usage: dgst [options] [file...]
    file... files to digest (default is stdin)
    -help          Display this summary
    -list          List digests
    -c             Print the digest with separating colons
    -r             Print the digest in coreutils format
    -out outfile   Output to filename rather than stdout
    -passin val    Input file pass phrase source
    -sign val      Sign digest using private key
    -verify val    Verify a signature using public key
    -prverify val  Verify a signature using private key
    -signature infile File with signature to verify
    -keyform format Key file format (PEM or ENGINE)
    -hex            Print as hex dump
    -binary         Print in binary form
    -d              Print debug info
    -debug          Print debug info
    -fips-fingerprint Compute HMAC with the key used in OpenSSL-FIPS fingerprint
    -hmac val       Create hashed MAC with key
    -mac val        Create MAC (not necessarily HMAC)
    -sigopt val     Signature parameter in n:v form
    -macopt val    MAC algorithm parameters in n:v form or key
    -*             Any supported digest
    -rand val       Load the file(s) into the random number generator
    -writerand outfile Write random data to the specified file
    -engine val     Use engine e, possibly a hardware device
    -engine_impl    Also use engine given by -engine for digest operations
xigu62705@pc-l305-7:~/LAB2/Alice$ 
```

2.(f)

2.(g)

```

xigu62705@pc-l305-7:~/LAB2/Alice$ gedit AuthDataAlice
(gedit:47376): Gtk-WARNING **: 16:47:08.989: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: La méthode « Inhibit » n'existe pas
xigu62705@pc-l305-7:~/LAB2/Alice$ openssl dgst -sha256 -out HashAuthData AuthData
AuthData: No such file or directory
xigu62705@pc-l305-7:~/LAB2/Alice$ openssl rsautl -sign -in HashAuthData -inkey Alice
AlicePrivateKey -out AliceSignature
xigu62705@pc-l305-7:~/LAB2/Alice$ ls
AliceDocument  AlicePublicKey  AuthDataAlice  BobPublicKey  HashAuthData
AlicePrivateKey AliceSignature  AuthDataBob   BobSignature
xigu62705@pc-l305-7:~/LAB2/Alice$ cp /home/elevex/x/xigu62705/LAB2/Alice/AuthDat
aAlice /home/elevex/x/xigu62705/LAB2/Bob
xigu62705@pc-l305-7:~/LAB2/Alice$ cp /home/elevex/x/xigu62705/LAB2/Alice/AliceSi
gnature /home/elevex/x/xigu62705/LAB2/Bob
xigu62705@pc-l305-7:~/LAB2/Alice$ cp /home/elevex/x/xigu62705/LAB2/Alice/AlicePu
blicKey /home/elevex/x/xigu62705/LAB2/Bob
xigu62705@pc-l305-7:~/LAB2/Alice$ cd ..
xigu62705@pc-l305-7:~/LAB2$ cd Bob
xigu62705@pc-l305-7:~/LAB2/Bob$ ls
AlicePublicKey  AuthDataAlice  BobDocument  BobPublicKey
AliceSignature  AuthDataBob   BobPrivateKey  BobSignature
xigu62705@pc-l305-7:~/LAB2/Bob$ 
```

3.(b)

3.(c)

AlicePublicKey can be used to verify AliceSignature

```
xigu62705@pc-l305-7:~/LAB2/Bob$ openssl rsautl -verify -in AliceSignature -pubin  
-inkey AlicePublicKey -out HashAuthData  
xigu62705@pc-l305-7:~/LAB2/Bob$ openssl dgst -sha256 -out HashBob AuthData  
AuthData: No such file or directory  
xigu62705@pc-l305-7:~/LAB2/Bob$ openssl dgst -sha256 -out HashBob AuthData  
xigu62705@pc-l305-7:~/LAB2/Bob$ diff HashBob HashAuthData  
1d0  
< SHA256(AuthData)= fcd8d53059e40f1924c89f6a14a5c9ecd1dc3a750c9ff5d12a5bfe02e834  
8d49  
xigu62705@pc-l305-7:~/LAB2/Bob$
```

3.(f)

```
xigu62705@pc-l305-7:~/LAB2/Bob$ openssl rand -hex -out SymKey 64  
xigu62705@pc-l305-7:~/LAB2/Bob$ ls  
AlicePublicKey AuthDataAlice BobPrivateKey HashAuthData  
AliceSignature AuthDataBob BobPublicKey HashBob  
AuthData BobDocument BobSignature SymKey  
xigu62705@pc-l305-7:~/LAB2/Bob$  
xigu62705@pc-l305-7:~/LAB2/Bob$
```

4.(b)

```
xigu62705@pc-l305-7:~/LAB2/Bob$ openssl rsautl -encrypt -pubin -inkey AlicePubli  
cKey -in SymKey -out SymKeyEncrypted
```

4.(d)

```
xigu62705@pc-l305-7:~/LAB2/Bob$ ls  
AlicePublicKey AuthDataAlice BobPrivateKey HashAuthData SymKeyEncrypted  
AliceSignature AuthDataBob BobPublicKey HashBob  
AuthData BobDocument BobSignature SymKey
```

4.(e)

```
xigu62705@pc-l305-7:~/LAB2/Bob$ cp /home/elevex/x/xigu62705/LAB2/Bob/SymKeyEncry  
pted /home/elevex/x/xigu62705/LAB2/Alice
```

```
xigu62705@pc-l305-7:~/LAB2/Bob$ cd ..
```

```
xigu62705@pc-l305-7:~/LAB2$ cd Alice
```

```
xigu62705@pc-l305-7:~/LAB2/Alice$ ls
```

```
AliceDocument AlicePublicKey AuthDataAlice BobPublicKey HashAuthData  
AlicePrivateKey AliceSignature AuthDataBob BobSignature SymKeyEncrypted
```

```
xigu62705@pc-l305-7:~/LAB2/Alice$
```

```
xigu62705@pc-l305-7:~/LAB2/Alice$ openssl rsautl -decrypt -inkey AlicePrivateKey  
-in SymKeyEncrypted -out SymKey  
rsautl: Use -help for summary.
```

4.(i)

5.(j)

```
xigu62705@pc-l305-7:~/LAB2/Alice$ openssl enc -e -aes-128-cbc -salt -pbkdf2 -kfile SymKey -in DataAlice -out DataAliceEncrypted
xigu62705@pc-l305-7:~/LAB2/Alice$ openssl enc -help
Usage: enc [options]
Valid options are:
-help Display this summary
-list List ciphers
-ciphers Alias for -list
-in infile Input file
-out outfile Output file
-pass val Passphrase source
-e Encrypt
-d Decrypt
-p Print the iv/key
-P Print the iv/key and exit
-v Verbose output
-nopad Disable standard block padding
-salt Use salt in the KDF (default)
-nosalt Do not use salt in the KDF
-debug Print debug info
-a Base64 encode/decode, depending on encryption flag
-base64 Same as option -a
-A Used with -[base64|a] to specify base64 buffer as a single
line
-bufsize val Buffer size
-k val Passphrase
-kfile infile Read passphrase from file
-K val Raw key, in hex
-S val Salt, in hex
-iv val IV in hex
-md val Use specified digest to create a key from the passphrase
-iter +int Specify the iteration count and force use of PBKDF2
-pbkdf2 Use password-based key derivation function 2
-none Don't encrypt
-* Any supported cipher
-rand val Load the file(s) into the random number generator
-writerand outfile Write random data to the specified file
-engine val Use engine, possibly a hardware device
xigu62705@pc-l305-7:~/LAB2/Alice$
```

5.(e)

```
xigu62705@pc-l305-7:~/LAB2/Alice$ cp /home/elevex/x/xigu62705/LAB2/Alice/DataAliceEncrypted /home/elevex/x/xigu62705/LAB2/Bob
xigu62705@pc-l305-7:~/LAB2/Alice$ cd ..
xigu62705@pc-l305-7:~/LAB2$ cd Bob
xigu62705@pc-l305-7:~/LAB2/Bob$ ls
AlicePublicKey AuthDataBob BobSignature SymKey
AliceSignature BobDocument DataAliceEncrypted SymKeyEncrypted
AuthData BobPrivateKey HashAuthData
AuthDataAlice BobPublicKey HashBob
xigu62705@pc-l305-7:~/LAB2/Bob$ openssl enc -d -aes-128-cbc -salt -pbkdf2 -kfile SymKey -in DataAliceEncrypted -out DataAlice
xigu62705@pc-l305-7:~/LAB2/Bob$ cat DataAlice
DataAlice
xigu62705@pc-l305-7:~/LAB2/Bob$
```

5.(e)

5.(h)

5.(i)

2 Exercise “Certificates X509”

```
xigu62705@pc-l305-7:~/LAB2/Bob$ cd ..  
xigu62705@pc-l305-7:~/LAB2$ openssl s_client -connect www.lcl.fr:443 > CertificateLCL  
1.-2.  
-----  
depth=2 C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN =  
= USERTrust RSA Certification Authority  
verify return:1  
depth=1 C = GB, ST = Greater Manchester, L = Salford, O = Sectigo Limited, CN =  
Sectigo RSA Organization Validation Secure Server CA  
verify return:1  
depth=0 C = FR, ST = Auvergne-Rhône-Alpes, O = CREDIT LYONNAIS SA, CN = www.  
.lcl.fr  
verify return:1  
xigu62705@pc-l305-7:~/LAB2$ openssl x509 -noout -in CertificateLCL -issuer  
issuer=C = GB, ST = Greater Manchester, L = Salford, O = Sectigo Limited, CN = S  
ectigo RSA Organization Validation Secure Server CA  
xigu62705@pc-l305-7:~/LAB2$ openssl x509 -help  
Usage: x509 [options]  
4.  
Valid options are:  
-help Display this summary  
-inform format Input format - default PEM (one of DER or PEM)  
-in infile Input file - default stdin  
-outform format Output format - default PEM (one of DER or PEM)  
-out outfile Output file - default stdout  
-keyform PEM|DER|ENGINE Private key format - default PEM  
-passin val Private key password/pass-phrase source  
-serial Print serial number value  
-subject_hash Print subject hash value  
-* Any supported digest  
-subject_hash_old Print old-style (MD5) subject hash value  
-issuer_hash_old Print old-style (MD5) issuer hash value  
-engine val Use engine, possibly a hardware device  
-preserve_dates preserve existing dates when signing  
xigu62705@pc-l305-7:~/LAB2$ openssl x509 -in CertificateLCL -noout -dates  
notBefore=Dec 15 00:00:00 2022 GMT  
notAfter=Dec 15 23:59:59 2023 GMT  
5.  
xigu62705@pc-l305-7:~/LAB2$ openssl x509 -in CertificateLCL -noout -text | grep  
"Signature Algorithm"  
Signature Algorithm: sha256WithRSAEncryption  
Signature Algorithm: sha256WithRSAEncryption  
6.  
xigu62705@pc-l305-7:~/LAB2$ openssl x509 -in CertificateLCL -noout -serial  
serial=CDB5B1A7D3A2D065D811C0643FC339A8  
7.  
xigu62705@pc-l305-7:~/LAB2$ openssl x509 -in CertificateLCL -pubkey -noout  
-----BEGIN PUBLIC KEY-----  
MIIBIjANBgkqhkiG9w0BAQEAAQCAQ8AMIIIBCgKCAQEArJRun3tjz3eGv0kUGd4S  
XXoCVxWjyfu0Qjml0Du6++cu6L5rAFPxFlCINETaiBp0T8IvszJn1vqc9jGhAfDK  
kqCn1py9xU14dIlP4y0UNsseufJVH6qb2C99aHF+yguFMP1K2VkhUEv7fYsKBG6Z  
l4SQmyVh4Ikktxms1v1bewi/+9BM8THVm6yW/OjvA/xk4U9meFowL2GFUB3XsqLF  
wCp2GwNHNQWjuoNCsdx0LKYix4qqqHX1mq/hW4v00z1LmXdD8p2e7w7B/Mu6ZuSb  
M6TB8CGkhYPVIkn1wrMU796C8USzz9trtAu4fw6oso+XxiZBoqla7KIV75h32jc8  
NQIDAQAB  
-----END PUBLIC KEY-----  
8.  
xigu62705@pc-l305-7:~/LAB2$
```

```
xigu62705@pc-l305-7:~/LAB2$ openssl genrsa -out ServerKeyPair -passout pass:password 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
xigu62705@pc-l305-7:~/LAB2$ openssl rsa -pubout -in ServerKeyPair -out ServerPublicKey
writing RSA key
xigu62705@pc-l305-7:~/LAB2$ mv ServerKeyPair ServerPrivateKey
xigu62705@pc-l305-7:~/LAB2$
```

9.(b)

```
e is 65537 (0x010001)
xigu62705@pc-l305-7:~/LAB2$ openssl rsa -pubout -in ServerKeyPair -out ServerPublicKey
writing RSA key
xigu62705@pc-l305-7:~/LAB2$ mv ServerKeyPair ServerPrivateKey
xigu62705@pc-l305-7:~/LAB2$ openssl req -new -key ServerPrivateKey -out ServerRequest.csr
Can't open ServerPrivateKey for reading, No such file or directory
139862413813568:error:02001002:system library:fopen:No such file or directory:crypto/bio/bss_file.c:69:fopen('ServerPrivateKey','r')
139862413813568:error:2006D080:BIOS routines:BIO_new_file:no such file:crypto/bio/bss_file.c:76:
unable to load Private Key
xigu62705@pc-l305-7:~/LAB2$ openssl req -new -key ServerPrivateKey -out ServerRequest.csr
```

9.(c)

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

```
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Ile de France
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [Internet Widgits Pty Ltd]:EPITA
Organizational Unit Name (eg, section) []:First year
Common Name (e.g. server FQDN or YOUR name) []:myserver.fr
Email Address []:xiaofan.guo@eleve.isep.fr
```

9.(e)

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []
xigu62705@pc-l305-7:~/LAB2$
```

```
xigu62705@pc-l305-7:~/LAB2$ openssl genrsa -aes256 -out CAKeyPair -passout pass:password 4096
```

9.(f)

```
Generating RSA private key, 4096 bit long modulus (2 primes)
.....+++++
.....+++++
.....+++++
e is 65537 (0x010001)
xigu62705@pc-l305-7:~/LAB2$
```

```
xigu62705@pc-l305-7:~/LAB2$ openssl req -x509 -new -key CAKeyPair -out CACertificate.crt -days 500
Enter pass phrase for CAKeyPair:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Ile de France
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCA
Organizational Unit Name (eg, section) []:MyCA
Common Name (e.g. server FQDN or YOUR name) []:MyCA
Email Address []:CAemail
xigu62705@pc-l305-7:~/LAB2$
```

9.(g)

```
xigu62705@pc-l305-7:~/LAB2$ openssl x509 -req -in ServerRequest.csr -CA CACertificate.crt -CAkey CAKeyPair -CAcreateserial -out ServerCertificate.crt -days 500
-sha256
Signature ok
subject=C = FR, ST = Ile de France, L = Paris, O = EPITA, OU = First year, CN =
myserver.fr, emailAddress = xiaofan.guo@eleve.isep.fr
Getting CA Private Key
Enter pass phrase for CAKeyPair:
xigu62705@pc-l305-7:~/LAB2$ openssl verify -CAfile CACertificate.crt ServerCertificate.crt
ServerCertificate.crt: OK
xigu62705@pc-l305-7:~/LAB2$
```

9.(h)

9.(i)

**Verify the certificate of the server by entering the OpenSSL command is successful:
ServerCertificate.crt: OK**

LAB 3

1 Exercise “Preparation of cryptographic security elements foreach actor”

```
xigu62705@pc-l305-7:/mnt/monster/home/elevens/x/xigu62705/LAB3$ cd  
xigu62705@pc-l305-7:~$ cd LAB3  
xigu62705@pc-l305-7:~/LAB3$ cd CARoot  
xigu62705@pc-l305-7:~/LAB3/CARoot$ openssl genrsa -out CAPrivateKey.key 4096  
Generating RSA private key, 4096 bit long modulus (2 primes)  
.....+++++  
e is 65537 (0x010001)  
xigu62705@pc-l305-7:~/LAB3/CARoot$ openssl req -new -x509 -key CAPrivateKey.key -ou  
t CACert.crt
```

2.(c)

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

```
-----  
Country Name (2 letter code) [AU]:FR  
State or Province Name (full name) [Some-State]:Ile de France  
Locality Name (eg, city) []:Paris  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:EPITA  
Organizational Unit Name (eg, section) []:First year  
Common Name (e.g. server FQDN or YOUR name) []:myserver.fr  
Email Address []:xigu62705@eleve.isep.fr
```

```
xigu62705@pc-l305-7:~/LAB3/CARoot$ openssl rsa -pubout -in CAPrivateKey.key -out CA  
PubKey.pem
```

2.(c)

```
writing RSA key  
xigu62705@pc-l305-7:~/LAB3/CARoot$
```

```
xigu62705@pc-l305-7:~/LAB3$ cd Server  
xigu62705@pc-l305-7:~/LAB3/Server$ openssl genrsa -out ServerPrivateKey.key 4096  
Generating RSA private key, 4096 bit long modulus (2 primes)  
.....+++++
```

2.(d)

```
e is 65537 (0x010001)  
xigu62705@pc-l305-7:~/LAB3/Server$ openssl rsa -pubout -in ServerPrivateKey.key -ou  
t ServerPublicKey.pem  
writing RSA key
```

```
xigu62705@pc-l305-7:~/LAB3/Server$ openssl req -new -newkey rsa:4096 -nodes -keyout ServerPrivKey.key -out ServerRequest.csr  
Generating a RSA private key  
.....+++++  
.....+++++  
writing new private key to 'ServerPrivKey.key'
```

2.(f)

```
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.
```

```
Country Name (2 letter code) [AU]:FR  
State or Province Name (full name) [Some-State]:Ile de France  
Locality Name (eg, city) []:Paris  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCA  
Organizational Unit Name (eg, section) []:MyCA  
Common Name (e.g. server FQDN or YOUR name) []:MyCA  
Email Address []:CAemail
```

```
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:password  
An optional company name []:CA
```

```
xigu62705@pc-l305-7:~/LAB3/Server$ cp /home/elevex/x/xigu62705/LAB3/Server/ServerRequest.csr /home/elevex/x/xigu62705/LAB3/CARoot  
xigu62705@pc-l305-7:~/LAB3/Server$
```

2.(f)

```
xigu62705@pc-l305-7:~/LAB3/CARoot$ openssl x509 -req -in ServerRequest.csr -CA CAcert.crt -CAkey CARrivKey.key -CAcreateserial -out ServerCert.crt -days 365  
Signature ok
```

2.(g)

```
subject=C = FR, ST = Ile de France, L = Paris, O = MyCA, OU = MyCA, CN = MyCA, e  
mailAddress = CAemail
```

```
Getting CA Private Key
```

```
Can't open CARrivKey.key for reading, No such file or directory
```

```
140469714433856:error:02001002:system library:fopen:No such file or directory:c  
rypto/bio/bss_file.c:69:fopen('CARrivKey.key','r')
```

```
140469714433856:error:2006D080:BIO routines:BIO_new_file:no such file:crypto/bio  
/bss_file.c:76:
```

```
unable to load CA Private Key
```

```
xigu62705@pc-l305-7:~/LAB3/CARoot$ openssl x509 -req -in ServerRequest.csr -CA CA  
Cert.crt -CAkey CAPrivKey.key -CAcreateserial -out ServerCert.crt -days 365  
Signature ok
```

```
subject=C = FR, ST = Ile de France, L = Paris, O = MyCA, OU = MyCA, CN = MyCA, e  
mailAddress = CAemail
```

```
Getting CA Private Key
```

```
xigu62705@pc-l305-7:~/LAB3/CARoot$
```

```
xigu62705@pc-l305-7:~/LAB3/CARoot$ cp /home/elevex/x/xigu62705/LAB3/CARoot/Server  
Cert.crt /home/elevex/x/xigu62705/LAB3/Server
```

2.(g)

```
xigu62705@pc-l305-7:~/LAB3/CARoot$ cp /home/elevex/x/xigu62705/LAB3/CARoot/CA  
Cert.crt /home/elevex/x/xigu62705/LAB3/Server
```

2.(h)

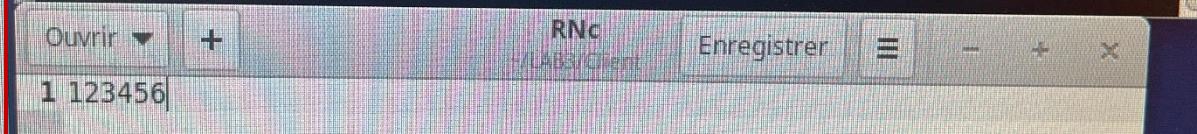
```
xigu62705@pc-l305-7:~/LAB3/CARoot$ cp /home/elevex/x/xigu62705/LAB3/CARoot/CA  
Cert.crt /home/elevex/x/xigu62705/LAB3/Client
```

```
xigu62705@pc-l305-7:~/LAB3/CARoot$
```

2 Exercise “TLS Protocol”

```
xigu62705@pc-l305-7:~/LAB3/CARoot$ cd ..  
xigu62705@pc-l305-7:~/LAB3$ cd Client  
xigu62705@pc-l305-7:~/LAB3/Client$ gedit RNC  
  
(gedit:12369): Gtk-WARNING **: 14:04:56.478: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: La méthode « Inhibit » n'existe pas  
xigu62705@pc-l305-7:~/LAB3/Client$ gedit RNC
```

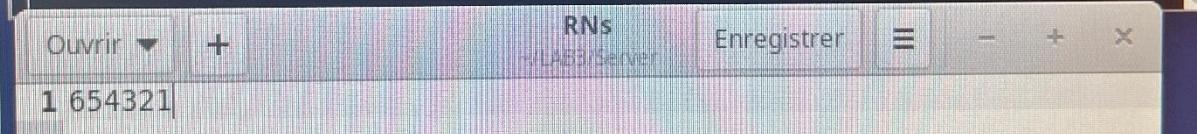
1.



```
xigu62705@pc-l305-7:~/LAB3/Client$ gedit RNC  
xigu62705@pc-l305-7:~/LAB3/Client$ cp /home/elevex/x/xigu62705/LAB3/Client/RNC /  
home/elevex/x/xigu62705/LAB3/Server  
xigu62705@pc-l305-7:~/LAB3/Client$ cd ..  
xigu62705@pc-l305-7:~/LAB3$ cd Server  
xigu62705@pc-l305-7:~/LAB3/Server$ ls  
xigu62705@pc-l305-7:~/LAB3/Server$ gedit RNs
```

```
(gedit:12737): Gtk-WARNING **: 14:06:49.573: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: La méthode « Inhibit » n'existe pas  
xigu62705@pc-l305-7:~/LAB3/Server$ gedit RNs
```

2.



```
xigu62705@pc-l305-7:~/LAB3/Server$ gedit RNs  
xigu62705@pc-l305-7:~/LAB3/Server$ cp /home/elevex/x/xigu62705/LAB3/Server/RNs /  
home/elevex/x/xigu62705/LAB3/Client  
xigu62705@pc-l305-7:~/LAB3/Server$ cd ..  
xigu62705@pc-l305-7:~/LAB3$ cd Client  
xigu62705@pc-l305-7:~/LAB3/Client$ ls  
CACert.crt RNC RNs  
xigu62705@pc-l305-7:~/LAB3/Client$
```

```
xigu62705@pc-l305-7:~/LAB3$ cd Server  
xigu62705@pc-l305-7:~/LAB3/Server$ cat RNC RNs > RNCRNs  
xigu62705@pc-l305-7:~/LAB3/Server$ openssl dgst -sha256 -out HashRNCRNs RNCRNs  
xigu62705@pc-l305-7:~/LAB3/Server$
```

3.(a)

```
xigu62705@pc-l305-7:~/LAB3/Server$ openssl dgst -sha256 -sign ServerPrivateKey.key  
-out SignS HashRNCRNs  
xigu62705@pc-l305-7:~/LAB3/Server$ cp /home/elevex/x/xigu62705/LAB3/Server/SignS  
/home/elevex/x/xigu62705/LAB3/Client
```

3.(b)

```
xigu62705@pc-l305-7:~/LAB3/Server$ cp /home/elevex/x/xigu62705/LAB3/Server/Server  
Cert.crt /home/elevex/x/xigu62705/LAB3/Client  
xigu62705@pc-l305-7:~/LAB3/Server$ cd ..
```

3.(c)

```
xigu62705@pc-l305-7:~/LAB3$ cd Client  
xigu62705@pc-l305-7:~/LAB3/Client$ ls  
CACert.crt RNs ServerCert.crt SignS  
xigu62705@pc-l305-7:~/LAB3/Client$
```

3.(d)

```
xigu62705@pc-l305-7:~/LAB3/Client$ openssl verify -CAfile CACert.crt ServerCert.crt  
ServerCert.crt: OK  
xigu62705@pc-l305-7:~/LAB3/Client$
```

3.(e)

```
CACert.crt RNC RNs ServerCert.crt SignS  
xigu62705@pc-l305-7:~/LAB3/Clients openssl verify -CAfile CACert.crt ServerCert.crt  
ServerCert.crt: OK  
xigu62705@pc-l305-7:~/LAB3/Clients openssl x509 -pubkey -noout -in ServerCert.crt > ServerPubKey.pem
```

3.(f)-1

```
xigu62705@pc-l305-7:~/LAB3/Clients echo "This is the content of AuthData" > AuthData  
xigu62705@pc-l305-7:~/LAB3/Clients cat AuthData  
This is the content of AuthData  
xigu62705@pc-l305-7:~/LAB3/Clients openssl dgst -sha256 -out HashAuthData AuthData  
AuthData: No such file or directory  
xigu62705@pc-l305-7:~/LAB3/Clients openssl dgst -sha256 -out HashAuthData AuthData  
xigu62705@pc-l305-7:~/LAB3/Client$ cat HashAuthData  
SHA256(AuthData)= 0de15aaae3a07a2a80b6d701d459b982a81f0fd46e3db66edd041a74a46b09  
3d  
xigu62705@pc-l305-7:~/LAB3/Client$ openssl rsautl -sign -in HashAuthData -inkey  
ServerPubKey.pem -out ServerSignature  
unable to load Private Key  
139968416565056:error:0909006C:PEM routines:get_name:no start line:crypto/pem/pe  
m_lib.c:745:Expecting: ANY PRIVATE KEY  
xigu62705@pc-l305-7:~/LAB3/Client$ openssl rsautl -sign -in HashAuthData -inkey  
ServerPubKey.key -out ServerSignature  
Can't open ServerPubKey.key for reading, No such file or directory  
140305119586112:error:02001002:system library:fopen:No such file or directory:cr  
ypto/bio/bss_file.c:69:fopen('ServerPubKey.key','r')  
140305119586112:error:2006D080: BIO routines:BIO_new_file:no such file:crypto/bio  
/bss_file.c:76:  
unable to load Private Key  
xigu62705@pc-l305-7:~/LAB3/Client$ openssl rsautl -sign -in HashAuthData -inkey  
ServerPrivKey.key -out ServerSignature  
xigu62705@pc-l305-7:~/LAB3/Client$ cat ServerSignature
```

3.(f)-2

```
00\000000"0=00N0000jUYu000@ /00700&000! S0xR j)00j0  
00/x(7200w00m@00I1#00$40t7@0P0zp0v000t0F0H+00j0!000000_?00n20]惋000]01i0X000  
P0Key!000t08L0t000mCn0Z1K00[()a00)!00  
;I00d_0{0PZ00W00v0' i0PU@cSJt>0#050"010/000aT%0,00\  
m  
N?xe@0000"0`'{e000u00000000L%l<0070 _{0U0E0)pV0000#E0"TO0j000R00b00L040n9(0v=0)3^  
NB000000CX0b0j00k'00l0e0000`R5,0000`!0T3002Vg0V0-0]<0Z00g00400r000y0a}h800P0000&  
xigu62705@pc-l305-7:~/LAB3/Client$ cp /home/eleves/x/xigu62705/LAB3/Client/Serve  
rSignature /home/eleves/x/xigu62705/LAB3/Server  
xigu62705@pc-l305-7:~/LAB3/Client$ cd LAB3  
bash: cd: LAB3: Aucun fichier ou dossier de ce type  
xigu62705@pc-l305-7:~/LAB3/Client$ cd ..  
xigu62705@pc-l305-7:~/LAB3$ cp /home/eleves/x/xigu62705/LAB3/Client/AuthData /ho  
me/eleves/x/xigu62705/LAB3/Server  
xigu62705@pc-l305-7:~/LAB3$ cd Server  
xigu62705@pc-l305-7:~/LAB3/Server$ openssl rsautl -verify -in ServerSignature -p  
ublic -inkey ServerPrivKey.key -out HashAuthData  
unable to load Public Key  
xigu62705@pc-l305-7:~/LAB3/Server$ openssl rsautl -verify -in ServerSignature -p  
ublic -inkey ServerPrivKey.pem -out HashAuthData  
RSA operation error  
139748771997504:error:0407008A:rsa routines:RSA_padding_check_PKCS1_type_1:invalid  
padding:crypto/rsa/rsa_pk1.c:67:  
139748771997504:error:04067072:rsa routines:rsa ossl_public_decrypt:padding che  
ck failed:crypto/rsa/rsa_oss1.c:588:  
xigu62705@pc-l305-7:~/LAB3/Server$ openssl dgst -sha256 -out HashServer AuthData  
xigu62705@pc-l305-7:~/LAB3/Server$ diff HashServer HashAuthData  
xigu62705@pc-l305-7:~/LAB3/Server$
```

Comparison
successful

```

xigu62705@pc-l305-7:~/LAB3/Server$ openssl dgst -sha256 -out HashServer AuthData
xigu62705@pc-l305-7:~/LAB3/Server$ diff HashServer HashAuthData
xigu62705@pc-l305-7:~/LAB3/Server$ cd ..
xigu62705@pc-l305-7:~/LAB3$ cd Client
xigu62705@pc-l305-7:~/LAB3/Client$ openssl rand -out PMsc.bin 48
xigu62705@pc-l305-7:~/LAB3/Client$ openssl rsa -encrypt -in PMsc.bin -pubin -  
4.(a)
inkey ServerPubKey.pem -out PMscEncrypted.bin
xigu62705@pc-l305-7:~/LAB3/Client$ cp /home/eleves/x/xigu62705/LAB3/Client/PMscE  
4.(b)
ncrypted.bin /home/eleves/x/xigu62705/LAB3/Server
xigu62705@pc-l305-7:~/LAB3/Client$ cd ..
xigu62705@pc-l305-7:~/LAB3$ cd Server
xigu62705@pc-l305-7:~/LAB3/Server$ openssl rsa -decrypt -in PMscEncrypted.bin  
4.(c)
-inkey ServerPrivKey.key -out PMsc.bin
xigu62705@pc-l305-7:~/LAB3/Server$ 
```

```

xigu62705@pc-l305-7:~/LAB3/Server$ echo "ClientData" > ClientData
xigu62705@pc-l305-7:~/LAB3/Server$ openssl enc -e -aes-256-cbc -salt -pbkdf2 -kf  
ile MS.bin -in ClientData -out ClientDataEncrypted.bin
xigu62705@pc-l305-7:~/LAB3/Server$ cd ..
xigu62705@pc-l305-7:~/LAB3$ cd Client
xigu62705@pc-l305-7:~/LAB3/Client$ openssl dgst -sha256 -out MS.bin -hex <<EOF  
5.(a)
> $(cat PMsc.bin)
> $(cat RNC)
> $(cat RNs)
> EOF
xigu62705@pc-l305-7:~/LAB3/Client$ echo "ClientData" > ClientData
xigu62705@pc-l305-7:~/LAB3/Client$ openssl enc -e -aes-256-cbc -salt -pbkdf2 -kf  
ile MS.bin -in ClientData -out ClientDataEncrypted.bin
xigu62705@pc-l305-7:~/LAB3/Client$ 
```

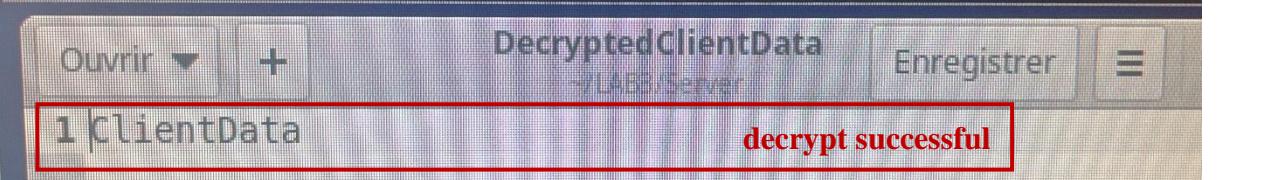
```

xigu62705@pc-l305-7:~/LAB3/Client$ cp /home/eleves/x/xigu62705/LAB3/Client/Clien  
tDataEncrypted.bin /home/eleves/x/xigu62705/LAB3/Server
xigu62705@pc-l305-7:~/LAB3/Client$ cd ..
xigu62705@pc-l305-7:~/LAB3$ cd Server
xigu62705@pc-l305-7:~/LAB3/Server$ openssl enc -d -aes-256-cbc -pbkdf2 -kfile MS  
.bin -in ClientDataEncrypted.bin -out DecryptedClientData
xigu62705@pc-l305-7:~/LAB3/Server$ ls
AuthData          MS.bin           ServerPrivateKey.key
CACert.crt       PMsc.bin        ServerPrivateKey.pem
ClientDataEncrypted.bin PMscEncrypted.bin ServerPublicKey.pem
DecryptedClientData RNC            ServerRequest.csr
HashAuthData     RNCRNs         ServerSignature
HashRNCRNs       RNs            SignS
HashServer        ServerCert.crt
xigu62705@pc-l305-7:~/LAB3/Server$ 
```

```

xigu62705@pc-l305-7:~/LAB3/Server$ gedit DecryptedClientData

```



The screenshot shows a gedit window with the title "DecryptedClientData". The text area contains the word "ClientData". Below the text area, a status bar displays the message "decrypt successful".

```
xigu62705@pc-l305-7:~/LAB3/Server$ echo "ServerData" > ServerData
xigu62705@pc-l305-7:~/LAB3/Server$ openssl enc -e -aes-256-cbc -salt -pbkdf2 -kfile MS.bin -in ServerData.txt -out ServerDataEncrypted.bin
xigu62705@pc-l305-7:~/LAB3/Server$ cp /home/elevex/x/xigu62705/LAB3/Server/ServerDataEncrypted.bin /home/elevex/x/xigu62705/LAB3/Client
xigu62705@pc-l305-7:~/LAB3/Server$ cd ..
xigu62705@pc-l305-7:~/LAB3$ cd Client
xigu62705@pc-l305-7:~/LAB3/Client$ openssl enc -d -aes-256-cbc -pbkdf2 -kfile MS.bin -in ServerDataEncrypted.bin -out DecryptedServerData
xigu62705@pc-l305-7:~/LAB3/Client$
```

6.(a)

```
xigu62705@pc-l305-7:~/LAB3/Client$ ls
AuthData          MS.bin           ServerDataEncrypted.bin
CACert.crt       PMsc.bin        ServerPrivateKey.key
ClientData        PMscEncrypted.bin ServerPubKey.pem
ClientDataEncrypted.bin RNC           ServerSignature
DecryptedServerData RNS           SignS
HashAuthData      ServerCert.crt
xigu62705@pc-l305-7:~/LAB3/Client$ gedit DecryptedServerData
```

6.(b)

