OPENSSL 5

1. Commençons par créer un fichier de taille 600M : dd if=/dev/zero of=LargeFile bs=1024 count=0 seek=$[300*2] ou bien tout simplement fallocate -l 600M Lar- geFile‘

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ dd if=/dev/zero of=LargeFile bs=1024 cou
t=0 seek=$[300*2]
0+0 enregistrements lus
0+0 enregistrements écrits
0 octet copié, 0,00539983 s, 0,0 kB/s
nathan@nathan-VirtualBox:~/Bureau/TP5$ ls
LargeFile
```

2. Générer une paire de clés : privée et publique : openssl req -x509 -nodes -days 100000 -newkey rsa:2048 -keyout privatekey.pem -out publickey.pem

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl req -x509 -nodes -days 100000 -ne
wkey rsa:2048 -keyout privatekey.pem -out publickey.pem
Generating a RSA private key
.....................................+++++
.....................................................................+++++
writing new private key to 'privatekey.pem'
-----
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]:TN
State or Province Name (full name) [Some-State]:Tunis
Locality Name (eg, city) []:Mutuelville
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UC
Organizational Unit Name (eg, section) []:UC
Common Name (e.g. server FQDN or YOUR name) []:UC
Email Address []:
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

3. Extraire votre clé publique `a partir du certificat généré : openssl x509 -in publi- ckey.pem -pubkey -noout > pub

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl x509 -in publickey.pem -pubkey -noout > pub
nathan@nathan-VirtualBox:~/Bureau/TP5$ ls
LargeFile  privatekey.pem  pub  publickey.pem
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

4. openssl rsautl -encrypt -pubin -inkey pub -in LargeFile -out LargeFile_encrypted, génère une erreur :RSA operation error : data too large for key size

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl rsautl -encrypt -pubin -inkey pub -in LargeFile -out La
rgeFile_encrypted
RSA operation error
140041962865984:error:0406D06E:rsa routines:RSA_padding_add_PKCS1_type_2:data too large for key size:.
./crypto/rsa/rsa_pk1.c:124:
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

et si on utilise
openssl rsautl -encrypt -pubin -inkey publickey.pem -in LargeFile -out Lar- geFile_encrypted un message d'erreur apparait : unable to load Public Key.

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl rsautl -encrypt -pubin -inkey publickey.pem -in LargeFi
le -out Lar- geFile_encrypted
rsautl: Use -help for summary.
```

(a) Première solution :

i. Chiffrer le fichier avec le certificat :

openssl smime -encrypt -aes256 -in LargeFile -binary -outform PEM - out LargeFile.enc publickey.pem

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl smime -encrypt -aes256 -in LargeFile -binary -outform P
EM -out LargeFile.enc publickey.pem
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

ii. Déchiffrer le fichier avec la clé privée :

openssl smime -decrypt -in LargeFile.enc -binary -inform PEM -inkey privatekey.pem -out LargeFile-1

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl smime -decrypt -in LargeFile.enc -binary -inform PEM -i
nkey privatekey.pem -out LargeFile-1
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

iii. comparer les deux fichiers avec *diff* .

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ diff LargeFile LargeFile-1
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

(b) Deuxième solution :

i. Générer d'une façon aléatoire une clé de session :

openssl rand -base64 32 > key

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl rand -base64 32 > key
```

ii. Chiffrer le fichier avec cette clé :

openssl enc -aes-256-cbc -salt -in LargeFile -out LargeFile_encrypted -pass file:./key

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl enc -aes-256-cbc -salt -in LargeFile -out LargeFile_enc
rypted -pass file:./key
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

ou bien pour remédier au problème de version de openssl etéviter le message Warning utilisez : openssl enc -aes-256-cbc -md sha512 -pbkdf2 -iter 100000 -salt -in LargeFile -out LargeFile_encrypted - pass file:./key

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl enc -aes-256-cbc -md sha512 -pbkdf2 -iter 100000 -salt
-in LargeFile -out LargeFile_encrypted -pass file:./key
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

iii. Récupérer la clé publique à partir de la clé privée générée :
openssl rsa -in privatekey.pem -pubout -out public.pem et la compa- rée avec (pub) celle extraite du certificat.

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl rsa -in privatekey.pem -pubout -out public.pem
writing RSA key
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ diff pub public.pem
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

iv. Chiffrer la clé pour que puissiez la transférer en toute sécurité :

openssl rsautl -encrypt -pubin -inkey pub -in key -out key.enc

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl rsautl -encrypt -pubin -inkey pub -in key -out key.enc
```

v. Envoyer à votre destinataire le LargeFile_encrypted et la key.enc.

J'ai tout fait sur la même machine du coup je n'ai pas fait d'envoi.

vi. Déchiffrer la key.enc pour obtenir la key :

openssl rsautl -decrypt -inkey privatekey.pem -in key.enc -out key

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl rsautl -decrypt -inkey privatekey.pem -in key.enc -out
key
```

vii. Déchiffrer LargeFile_encrypted avec key : openssl enc -aes-256-cbc -d -in LargeFile_encrypted -out LargeFile -pass file:./key

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ openssl enc -aes-256-cbc -d -in LargeFile_encrypted -out LargeF
ile1 -pass file:./key
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

J'ai appelé LargeFile1 car je travaille sur la même machine pour ne pas écraser mes fichiers

viii. comparer les deux fichiers avec *diff* .

```
nathan@nathan-VirtualBox:~/Bureau/TP5$ diff LargeFile LargeFile1
nathan@nathan-VirtualBox:~/Bureau/TP5$
```

Identiques