LAB_1

1)

```
[epita@localhost:~/afs]$ openssl genrsa -out BobKeyPair
Generating RSA private key, 2048 bit long modulus
.......................+++++
..................................+++++
e is 65537 (0x10001)
```

```
[clement.chang@r05p01 Bob]$ openssl rsa -in BobKeyPair -pubout -out BobPublicKey
writing RSA key
[clement.chang@r05p01 Bob]$ ls
BobKeyPair  BobPublicKey
[clement.chang@r05p01 Bob]$ mv BobKeyPair BobPrivateKey
[clement.chang@r05p01 Bob]$ ls
BobPrivateKey  BobPublicKey
```

La première commande permet de créer une paire de clé, publique et privée. On extrait la clé publique de la paire de clé. On renomme ensuite BobKeyPair en BobPrivateKey.

2)

```
[clement.chang@r05p01 Alice]$ cp ../Bob/BobPublicKey .
[clement.chang@r05p01 Alice]$ ls
AliceDocument  AlicePrivateKey  AlicePublicKey  BobPublicKey
```

On revient dans le dossier Alice et l'on copie la BobPublicKey dans le fichier d'Alice.

```
[clement.chang@r05p01 Alice]$ openssl rsautl -encrypt -in AliceDocument -pubin -inkey BobPublicKey -out AliceDocumentEncrypted
[clement.chang@r05p01 Alice]$ cat AlicDocumentEncrypted
cat: AlicDocumentEncrypted: No such file or directory
[clement.chang@r05p01 Alice]$ cat AliceDocumentEncrypted
*EöBb'Xi̯î·ø¯buÇÛVhA/}ÿÿZBuäÆ:§qfÇö+µ~9XÝGR»={-_þwsK▯î▯9▯Á«(oCß,íH[wÏÄ c9j»¦?$ñÀ(ñ6!Gòìrhà2SDöÎô=3l
                                                               þÛâ ÆWë¡Z§¤ÃÑ6½{ØÁÁ£©h¸xEâ
                                                                               ÐM±´
                                                                                 ´éÛZ¥Û6t[=?cپ7µv=&47B:ô²ÆâàZ4
ø4h/åMG͵nGÛgdÎ0W
èß{ÔB>K!ý»▯ym[clement.chang@r05p01 Alice]$
```

On encrypte le document d'Alice grâce à la BobPublicKey. On check ensuite que le document a bien été encodé. Ainsi que son contenu.

3)

```
[clement.chang@r05p01 Alice]$ cp /home/clement.chang/afs/LAB1/Alice/AliceDocumentEncrypted /home/clement.chang/afs/LAB1/Bob/
[clement.chang@r05p01 Alice]$ cd ../bob
bash: cd: ../bob: No such file or directory
[clement.chang@r05p01 Alice]$ cd ../Bob/
[clement.chang@r05p01 Bob]$ ls
AliceDocumentEncrypted  BobPrivateKey  BobPublicKey
[clement.chang@r05p01 Bob]$
```

On vérifie qu'on est encore dans le fichier d'Alice et on copie le document AliceDocumentEncrypted chez Bob. On se déplace ensuite dans le fichier de Bob. On vérifie ensuite que le fichier AliceDocumentEncrypted a bien été envoyé.

```
[clement.chang@r05p01 Bob]$ openssl rsautl -decrypt -in  AliceDocumentEncrypted -inkey BobPrivateKey -out AliceDocument
[clement.chang@r05p01 Bob]$ ls
AliceDocument  AliceDocumentEncrypted  BobPrivateKey  BobPublicKey
[clement.chang@r05p01 Bob]$ cat AliceDocument
Hello Bob, I'm Alice
[clement.chang@r05p01 Bob]$
```

On décrypte ensuite AliceDocumentEncrypted avec la bobPrivateKey. On vérifie que le fichier est décrypté et on check son contenu.

4)

```
[clement.chang@r05p01 Bob]$ cd ../Alice
[clement.chang@r05p01 Alice]$ openssl rand -out LargeFile -base64 $((2**30 * 3/4))
```

On retourne dans le dossier d'Alice. Et on crée LargeFile et on l'encrypte grâce à la BobPublicKey, et devient LargeFileEncrypted.

5)

```
[clement.chang@r05p01 Alice]$ echo > AuthData "It's me MARIOOOO"
[clement.chang@r05p01 Alice]$ ls
AliceDocument  AliceDocumentEncrypted  AlicePrivateKey  AlicePublicKey  AuthData  BobPublicKey  LargeFile  LargeFileEncrypted
[clement.chang@r05p01 Alice]$ cat AuthData
It's me MARIOOOO
[clement.chang@r05p01 Alice]$
```

On vérifie qu'on est bien dans le fichier d'Alice (le cas) et on crée un fichier AuthData avec le message « It's me MARIOOOO » à l'intérieur. On check que le fichier a bien été créé et que son contenu est bon.

```
[clement.chang@r05p01 Bob]$ cp /home/clement.chang/afs/LAB1/Alice/AlicePublicKey /home/clement.chang/afs/LAB1/Bob/
[clement.chang@r05p01 Bob]$ ls
AliceDocument  AliceDocumentEncrypted  AlicePublicKey  BobPrivateKey  BobPublicKey
[clement.chang@r05p01 Bob]$
```

On copie la AlicePublicKey dans le dossier de Bob.

```
[clement.chang@r05p01 Alice]$ openssl dgst -sha256 -out  HashAuthData AuthData
[clement.chang@r05p01 Alice]$ ls
AliceDocument  AliceDocumentEncrypted  AlicePrivateKey  AlicePublicKey  AuthData  BobPublicKey  HashAuthD
[clement.chang@r05p01 Alice]$ cat HashAuthData
SHA256(AuthData)= f29213a8f329d5615bfb8405f15e119254d76ee7c8d6ce6f1ff929d268fbb7e5
```

On utilise une méthode de hashage sur AuthData et vérifie que HashAuthData a bien été créé. On check que HashAuthData a bien été encrypté.

```
[clement.chang@r05p01 Alice]$ openssl rsautl -sign -in HashAuthData -inkey AlicePrivateKey -out AliceSign
[clement.chang@r05p01 Alice]$ ls
AliceDocument  AliceDocumentEncrypted  AlicePrivateKey  AlicePublicKey  AliceSignature  AuthData  BobPublicKey  HashAuthData  LargeFile  LargeFileEncrypted
[clement.chang@r05p01 Alice]$ cat AliceSignature
 Â2P    »Ùkê<Ïâ]w _`Þc&Õ        lør{ ,(&Ç?Õ<K,êEâY$
                                          <½NUlÆ1¶ÿäý¡Î0}4
                                                    «ãXiÆfsÞ&êq|Q>ö¥v\²èiiU?Çp¹
p
É!°øvc=0}³Î2ÎÏø
Xs˜mu(FU@`Ç▯}A08ÑqD2öoAQã
                    è;öDÐ"KöèeöõF2sm¿xOüI63³?~hG*ùoŸ±Pöz7ýÖ7ç^[[?1;2c[clement.chang@r05p01 Alice]$ 1;2c^C
[clement.chang@r05p01 Alice]$ cd ../Bob/
[clement.chang@r05p01 Bob]$ cp ../Alice/AliceSignature /.
cp: cannot create regular file '/./AliceSignature': Permission denied
[clement.chang@r05p01 Bob]$ cp ../Alice/AliceSignature /home/clement.chang/afs/LAB1/Bob/
[clement.chang@r05p01 Bob]$ cp ../Alice/AuthData /home/clement.chang/afs/LAB1/Bob/
[clement.chang@r05p01 Bob]$ ls
AliceDocument  AliceDocumentEncrypted  AlicePublicKey  AliceSignature  AuthData  BobPrivateKey  BobPublicKey  HashAuthData
```

On signe le fichier HashAuthData avec la AlicePrivateKey qui s'appelera AliceSignature. On vérifie que AliceSignature a bien été créé. On regarde le contenu de AliceSignature. On se déplace dans le fichier de Bob On vérifie que AuthData et AliceSignature sont copiés dans le fichier de Bob.

```
[clement.chang@r05p01 Bob]$ openssl rsautl -verify -in AliceSignature -pubin -inkey AlicePublicKey -out HashAuthData
[clement.chang@r05p01 Bob]$ ls
AliceDocument  AliceDocumentEncrypted  AlicePublicKey  AliceSignature  AuthData  BobPrivateKey  BobPublicKey  HashAuthData
[clement.chang@r05p01 Bob]$ cat HashAuthData
SHA256(AuthData)= f29213a8f329d5615bfb8405f15e119254d76ee7c8d6ce6f1ff929d268fbb7e5
```

Bob utilise la même fonction de hashage sur le document AuthData d'Alice, et transforme ensuite en HashBob. Il vérifie ensuite l'authenticité du document avec la AliceSignature et la AlicePublicKey. Il compare ensuite les deux documents cryptés par la fonction de hashage avec la commande « diff Hashbob HashAuthData ». Le résultat est nul, il n'y a donc pas de changement.