Introduction to Cybersecurity : Lab 1

Exercise ”Asymmetric cryptography”

1.

- *Repeat the same steps for Bob*

```
sh-3.2# cd Bob
sh-3.2# ls
sh-3.2# openssl genrsa -out BobKeyPair
Generating RSA private key, 2048 bit long modulus
..................+++
....................+++
e is 65537 (0x10001)
sh-3.2# ls
BobKeyPair
sh-3.2# openssl rsa -in BobKeyPair -pubout -out BobPublicKey
writing RSA key
sh-3.2# ls
BobKeyPair    BobPublicKey
sh-3.2# mv BobKeyPair BobPrivateKey
sh-3.2# ls
BobPrivateKey    BobPublicKey
sh-3.2# pwd
/Users/hugobeheray/Documents/ING4S2/IS Security/LAB1/Bob
sh-3.2#
```

2.

- *Go back to the parent folder LAB1 and access Alice’s folder*

`sh-3.2# cd ..`

`sh-3.2# cd Alice/`

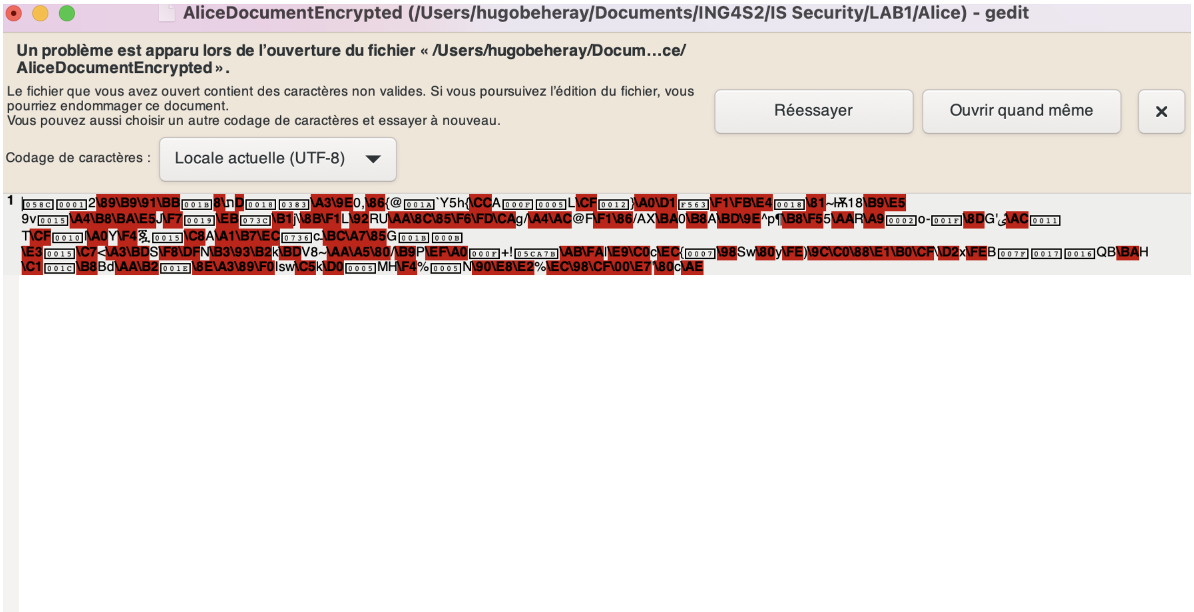
- *Check that BobPublicKey has been copied correctly to Alice’s folder*

```
sh-3.2# ls AliceDocument    AlicePrivateKey    AlicePublicKey    BobPublicKey
sh-3.2#
```

- *Check that AliceDocumentEncrypted has been created correctly*

```
openssl rsautl -encrypt -in AliceDocument -pubin -inkey BobPublicKey -out
AliceDocumentEncrypted
sh-3.2# ls
AliceDocument         AliceDocumentEncrypted    AlicePrivateKey
AlicePublicKey         BobPublicKey
sh-3.2# gedit AliceDocumentEncrypted
```

- *Check the content of the file AliceDocumentEncrypted*



AliceDocumentEncrypted (/Users/hugobeheray/Documents/ING4S2/IS Security/LAB1/Alice) - gedit

Un problème est apparu lors de l'ouverture du fichier « /Users/hugobeheray/Docum…ce/ AliceDocumentEncrypted ».

Le fichier que vous avez ouvert contient des caractères non valides. Si vous poursuivez l'édition du fichier, vous pourriez endommager ce document.
Vous pouvez aussi choisir un autre codage de caractères et essayer à nouveau.

Codage de caractères : Locale actuelle (UTF-8)

```
1 058C0001 2\89\B9\91\BB001B8\nD00180383\A3\9E0,\86{@001A`Y5h{\CCA000F0005L\CF0012}\A0\D1F563\F1\FB\E40018\81~lk18\B9\E5
9v0015\A4\B8\BA\E5J\F70019\EB073C\B1j\8B\F1L\92RU\AA\8C\85\F6\FD\CAg/\A4\AC@F\F1\86/AX\BA0\B8A\BD\9E^p¶\B8\F55\AAR\A90002o-001F\8DG'\AC0011
T\CF0010\A0Y\F4乭0015\C8A\A1\B7\EC0736c\BC\A7\85G001B000B
\E30015\C7<\A3\BDS\F8\DFN\B3\93\B2k\BDV8~\AA\A5\80/\B9P\EF\A0000F+!05CA7B\AB\FA\E9\C0c\EC{0007\98Sw\80y\FE)\9C\C0\88\E1\B0\CF\D2x\FEB007F00170016QB\BAH
\C1001C\B8Bd\AA\B2001E\8E\A3\89\F0lsw\C5k\D00005MH\F4%0005N\90\E8\E2%\EC\98\CF\00\E7\80c\AE
```

We notice that the message "Hello Bob I'm Alice" has been encrypted using incomprehensible characters.

3.

- *Make sure you are in Alice's folder. We ask you to copy AliceDocumentEncrypted to Bob's folder*

```
sh-3.2# pwd
/Users/hugobeheray/Documents/ING4S2/IS Security/LAB1/Alice
sh-3.2# cp /Users/hugobeheray/Documents/ING4S2/IS\
Security/LAB1/Alice/AliceDocumentEncrypted
/Users/hugobeheray/Documents/ING4S2/IS\ Security/LAB1/Bob/
sh-3.2#
```

- *Go back to the parent folder LAB1 and access Bob's folder*

```
sh-3.2# cd ..
sh-3.2# cd Bob
```

- *Check that AliceDocumentEncrypted has been copied correctly to Bob's folder*

```
sh-3.2# ls
AliceDocumentEncrypted    BobPrivateKey        BobPublicKey
```

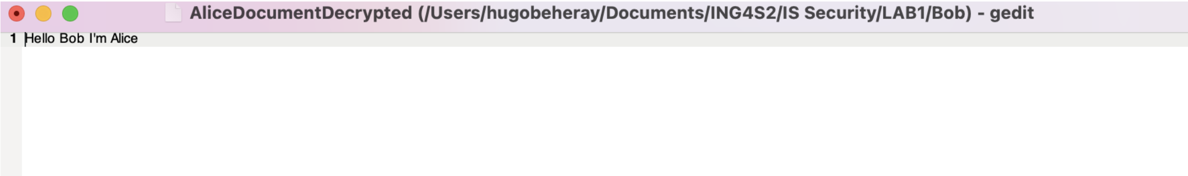
- *Decrypt AliceDocumentEncrypted thanks to BobPrivateKey*

```
sh-3.2# openssl rsautl -decrypt -in AliceDocumentEncrypted  -inkey BobPrivateKey
-out AliceDocumentDecrypted
```

- *Check that AliceDocumentDecrypted has been created correctly*

```
sh-3.2# ls
AliceDocumentDecrypted    AliceDocumentEncrypted    BobPrivateKey
BobPublicKey
```

- *Check the content of the file AliceDocumentDecrypted. What do you notice?*



AliceDocumentDecrypted (/Users/hugobeheray/Documents/ING4S2/IS Security/LAB1/Bob) - gedit

```
1 Hello Bob I'm Alice
```

We notice that the document has been decrypted correctly because we can see the previous message wrote in AliceDocument.

4.

- *Go back to the parent folder LAB1 and access Alice's folder*

```
sh-3.2# cd ..
sh-3.2# cd Alice
sh-3.2# pwd
/Users/hugobeheray/Documents/ING4S2/IS Security/LAB1/Alice
```

- *Try now to encrypt LargeFile by using BobPublicKey and by naming the encrypted file LargeFileEncrypted*

```
sh-3.2# openssl rsautl -encrypt -in LargeFile -pubin -inkey BobPublicKey -out
LargeFileEncrypted
RSA operation error
4492301996:error:04FFF06E:rsa routines:CRYPTO_internal:data too large for key
size:/System/Volumes/Data/SWE/macOS/BuildRoots/5b2e67f8af/Library/Caches/com.app
le.xbs/Sources/libressl/libressl-75.60.3/libressl-2.8/crypto/rsa/rsa_pk1.c:151:
sh-3.2#
```

5.

- *Create a file named AuthData and write a text of your choice*

```
sh-3.2# pwd
/Users/hugobeheray/Documents/ING4S2/IS Security/LAB1/Alice
sh-3.2# gedit AuthData
```

- *Check that AuthData has been created correctly*

```
sh-3.2# ls
AliceDocument		AlicePrivateKey		AuthData		LargeFile
AliceDocumentEncrypted	AlicePublicKey		BobPublicKey
LargeFileEncrypted
```

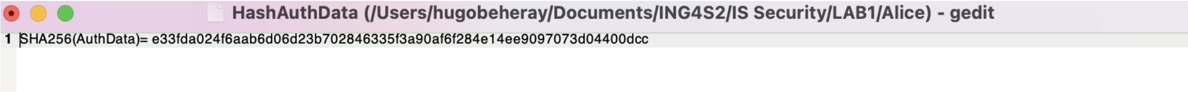
- *Copy AlicePublicKey to Bob's folder*

```
sh-3.2# cp /Users/hugobeheray/Documents/ING4S2/IS\
Security/LAB1/Alice/AlicePublicKey /Users/hugobeheray/Documents/ING4S2/IS\
Security/LAB1/Bob/
sh-3.2# cd ..
sh-3.2# cd Bob
sh-3.2# ls
AliceDocumentDecrypted	AliceDocumentEncrypted	AlicePublicKey
BobPrivateKey		BobPublicKey
```

- *Check that HashAuthData has been created correctly*

```
sh-3.2# openssl dgst -sha256 -out HashAuthData AuthData
sh-3.2# l
sh: l: command not found
sh-3.2# ls
AliceDocument		AlicePrivateKey		AuthData		HashAuthData
LargeFileEncrypted
AliceDocumentEncrypted	AlicePublicKey		BobPublicKey		LargeFile
```

- *Check the content of HashAuthData*


HashAuthData (/Users/hugobeheray/Documents/ING4S2/IS Security/LAB1/Alice) - gedit

```
SHA256(AuthData)= e33fda024f6aab6d06d23b702846335f3a90af6f284e14ee9097073d04400dcc
```

- *You will now proceed to sign HashAuthData thanks to AlicePrivateKey by naming the signature AliceSignature*

```
openssl rsautl -sign -in HashAuthData -inkey AlicePrivateKey -out AliceSignature
```

- *Check that AliceSignature has been created correctly*

```
sh-3.2# ls
AliceDocument        AlicePrivateKey        AliceSignature        BobPublicKey
     LargeFile
AliceDocumentEncrypted    AlicePublicKey        AuthData        HashAuthData
   LargeFileEncrypted
```

- *Copy AliceSignature and AuthData to Bob's folder*

```
sh-3.2# cp /Users/hugobeheray/Documents/ING4S2/IS\
Security/LAB1/Alice/AliceSignature /Users/hugobeheray/Documents/ING4S2/IS\
Security/LAB1/Bob/
sh-3.2# cp /Users/hugobeheray/Documents/ING4S2/IS\ Security/LAB1/Alice/AuthData
/Users/hugobeheray/Documents/ING4S2/IS\ Security/LAB1/Bob/
```

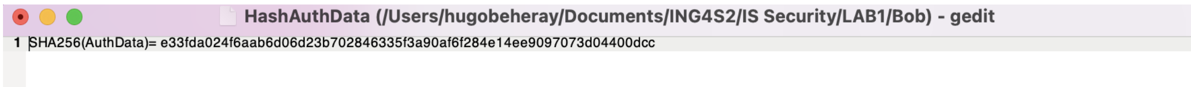
- Go back to the parent folder LAB1 and access Bob's folder

```
sh-3.2# cd ..
sh-3.2# cd Bob
sh-3.2# pwd
/Users/hugobeheray/Documents/ING4S2/IS Security/LAB1/Bob
```

- Check that AliceSignature and AuthData have been copied correctly to Bob's folder

```
sh-3.2# ls
AliceDocumentDecrypted    AliceDocumentEncrypted    AlicePublicKey
AliceSignature        AuthData        BobPrivateKey        BobPublicKey
```

- *Check that HashAuthData has been retrieved correctly*


HashAuthData (/Users/hugobeheray/Documents/ING4S2/IS Security/LAB1/Bob) - gedit

```
SHA256(AuthData)= e33fda024f6aab6d06d23b702846335f3a90af6f284e14ee9097073d04400dcc
```

- *Check that HashBob has been created correctly*

```
sh-3.2# openssl dgst -sha256 -out HashBob AuthData
sh-3.2# ls
AliceDocumentDecrypted    AlicePublicKey        AuthData        BobPublicKey
   HashBob
AliceDocumentEncrypted    AliceSignature        BobPrivateKey
HashAuthData
```