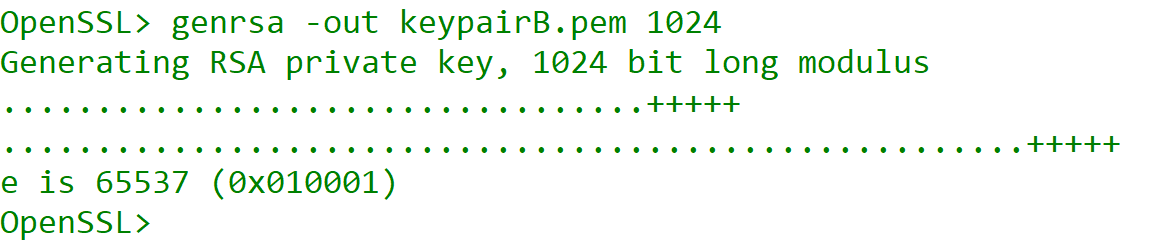
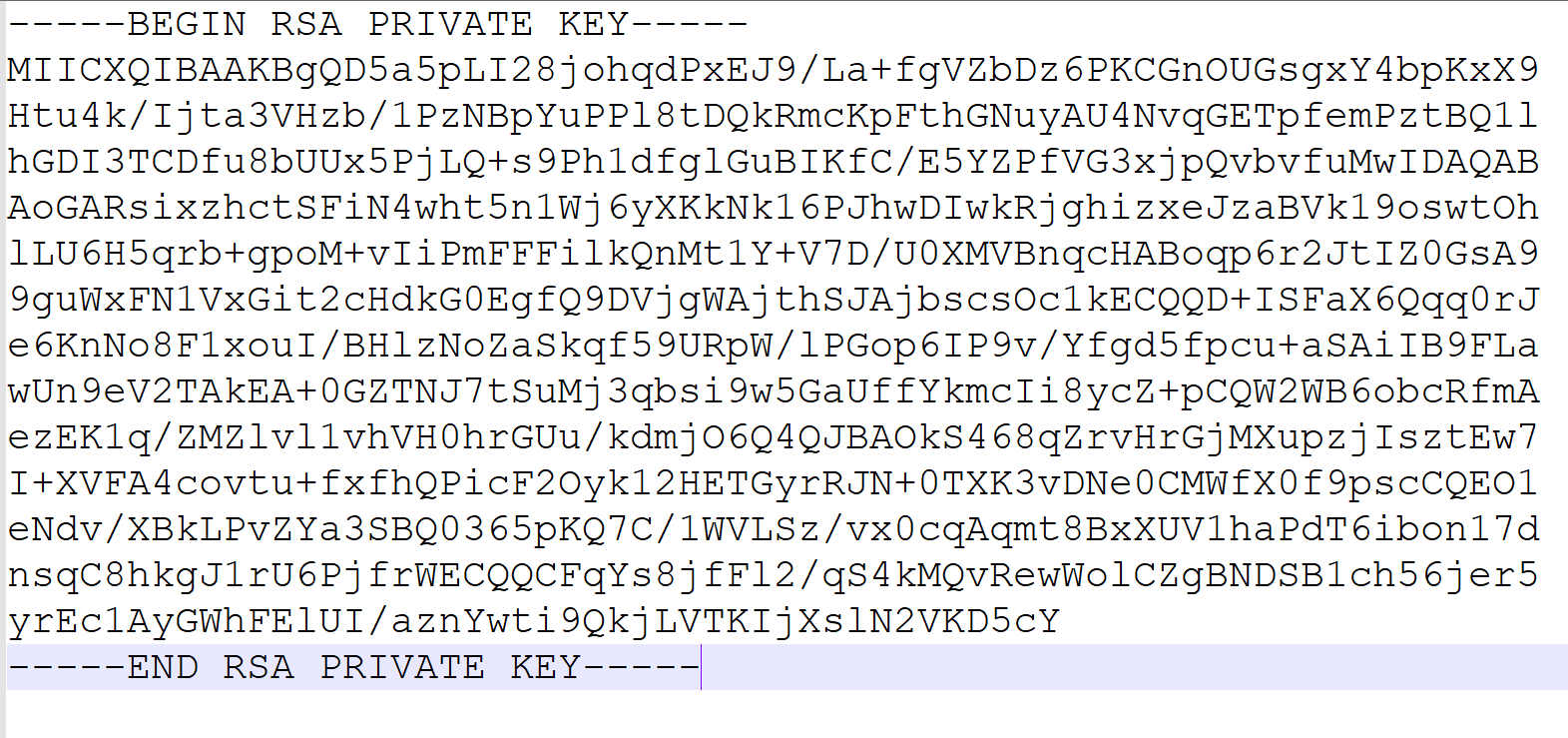
**Exercice 1**

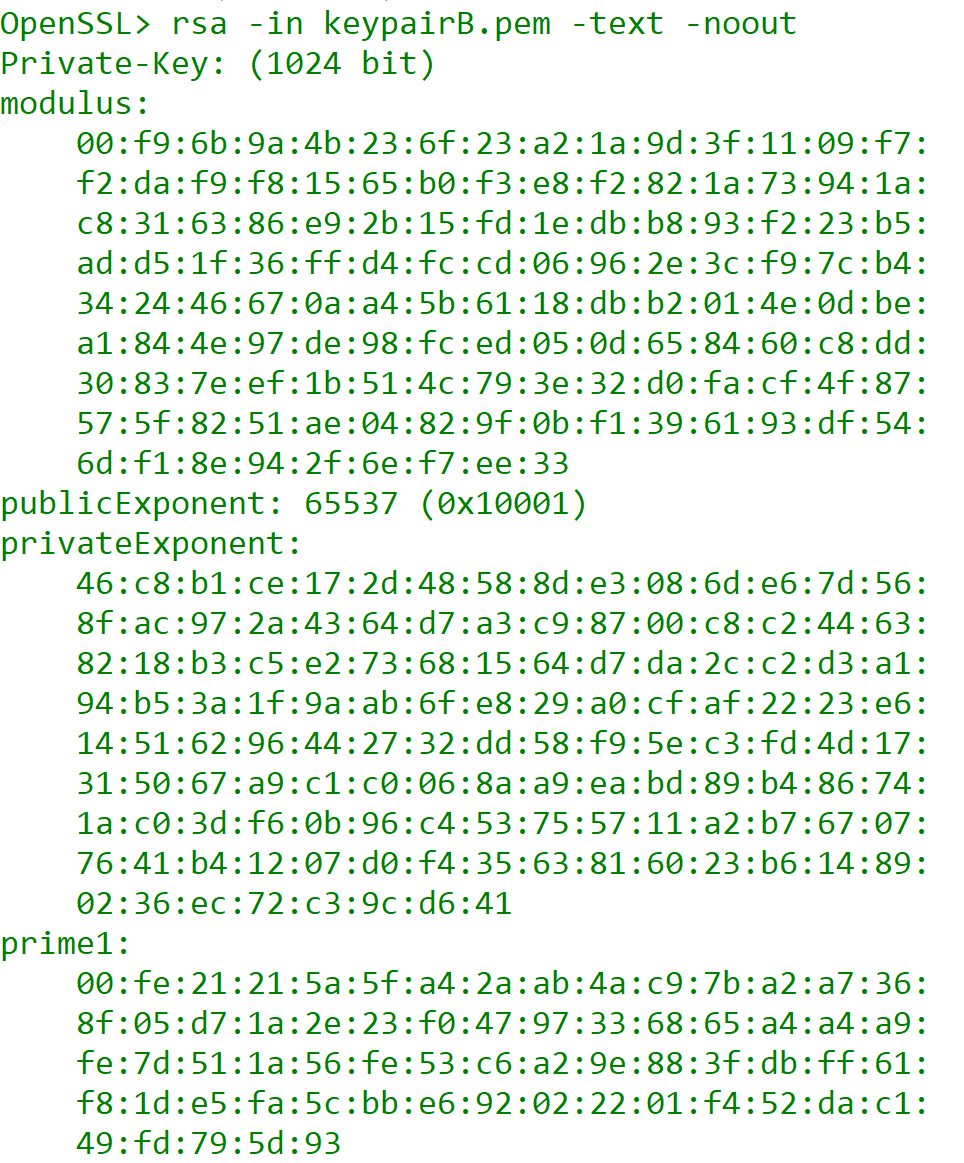
1.Openssl genrsa -out keypairB.pem 1024

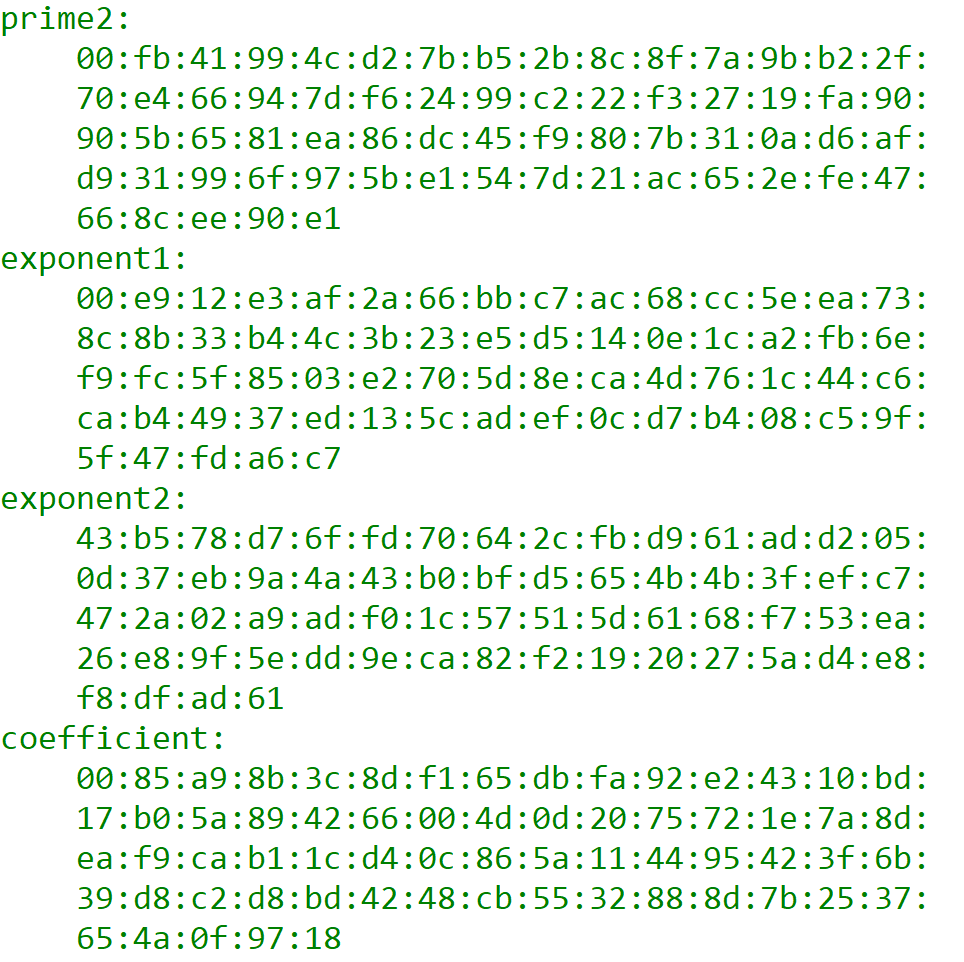


Capture du fichier générer



2. OpenSSL rsa -in keypairB.pem -text –noout



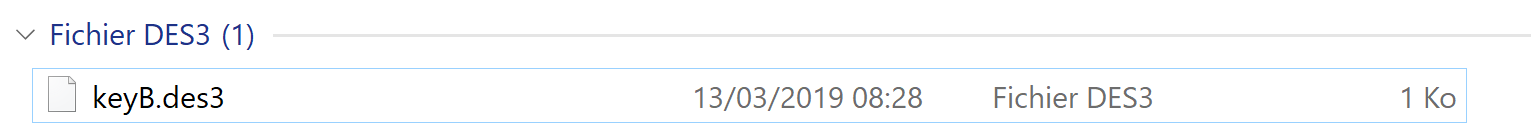


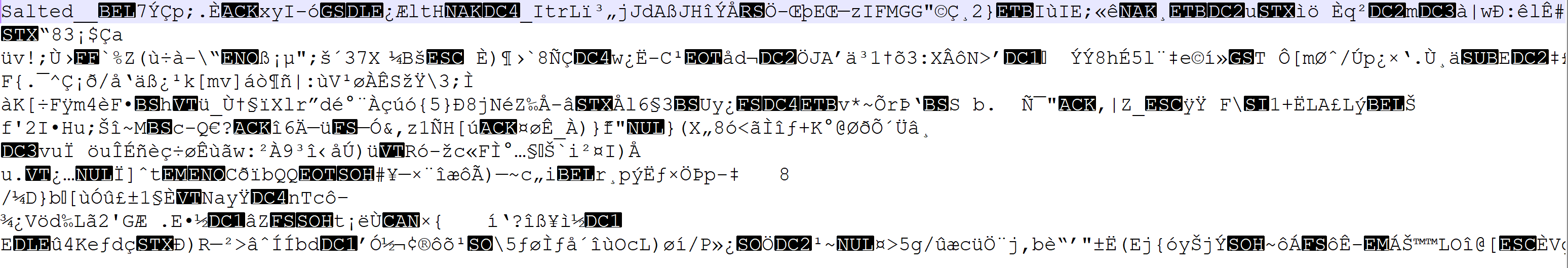
3.

4. et 5.

Openssl enc -des3 -salt -in keypairB.pem -out keyB.des3 -pass pass:upec

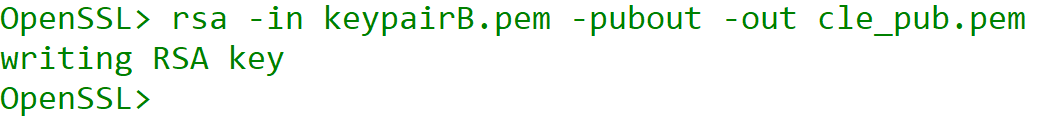
Capture du fichier générer avec DES3

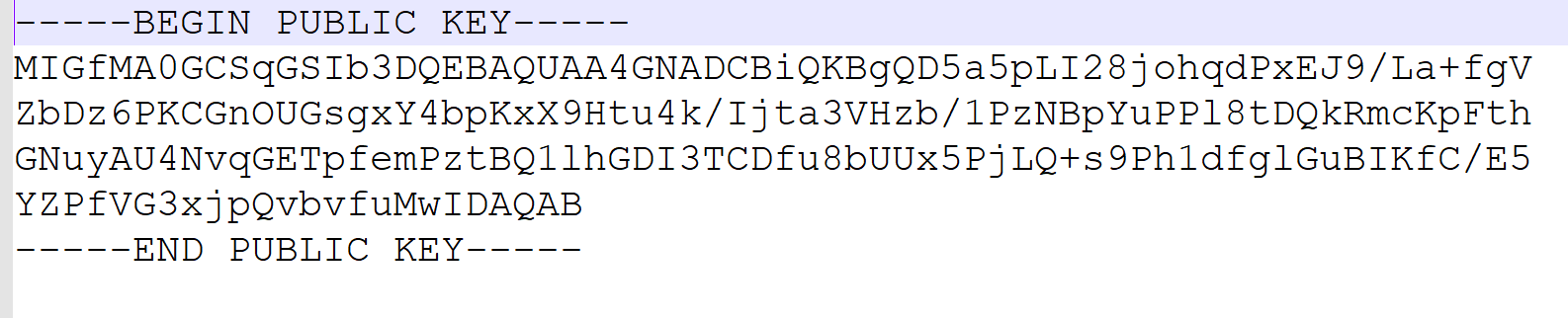


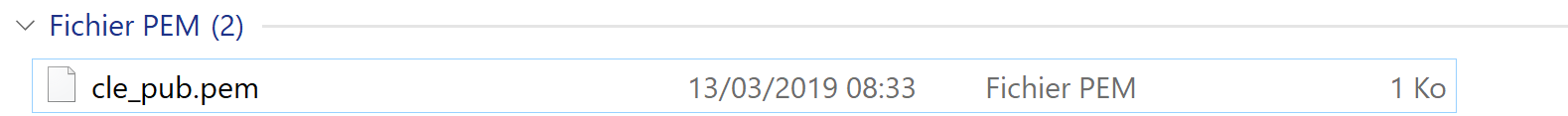


6.

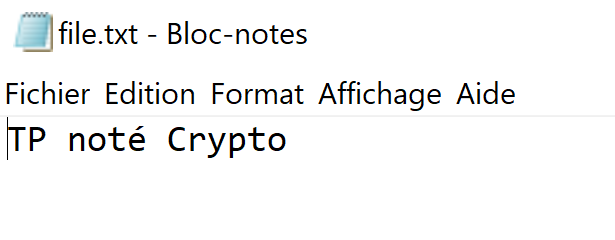
OpenSSL rsa -in keypairB.pem -pubout -out cle\_pub.pem



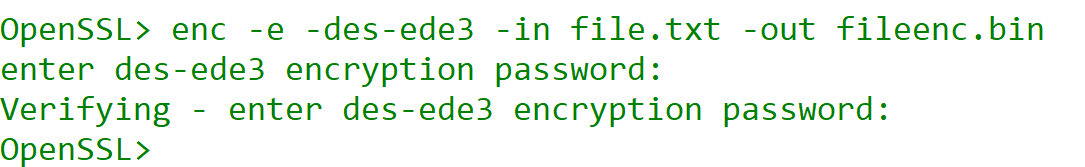




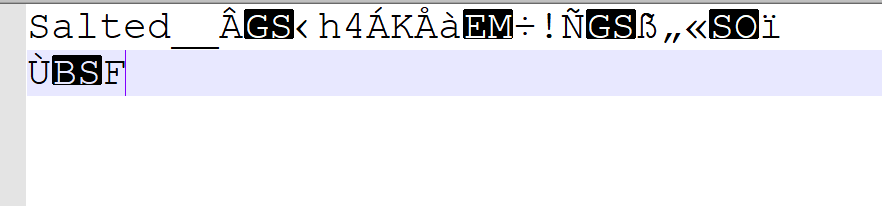
7. Chiffrement avec DES3 du fichier file.txt



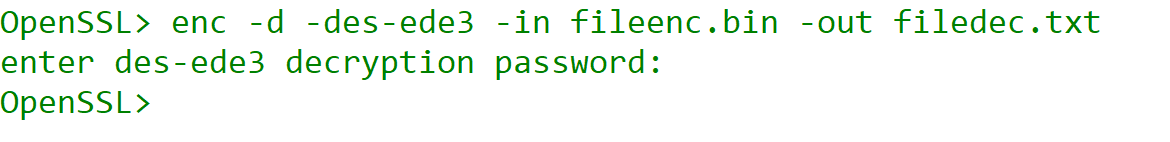
Openssl enc -e -des-ede3 -in file.txt -out fileenc.bin

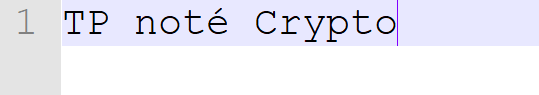


Fichier générer :

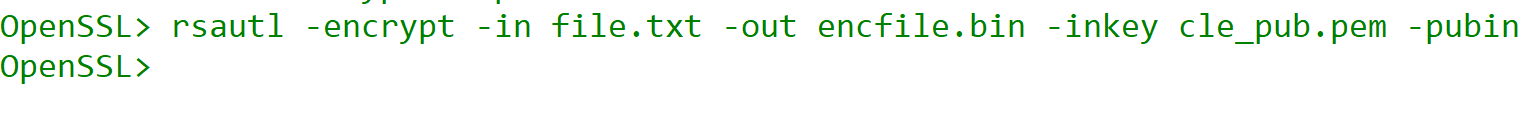


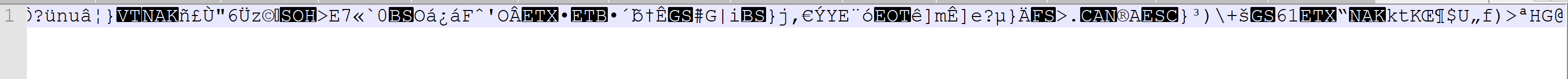
8. OpenSSL enc -d -des-ede3 -in fileenc.bin -out filedec.txt



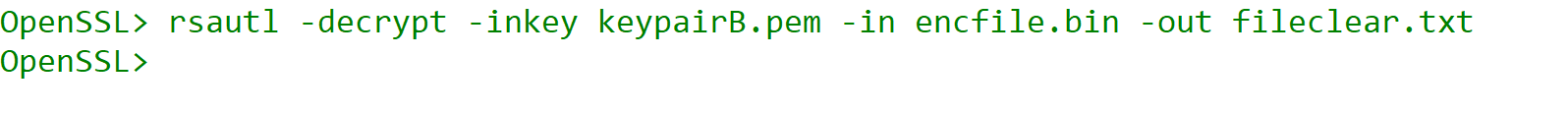


9. Openssl rsautl -encrypt -in file.txt -out encfile.bin -inkey cle\_pub.pem –pubin





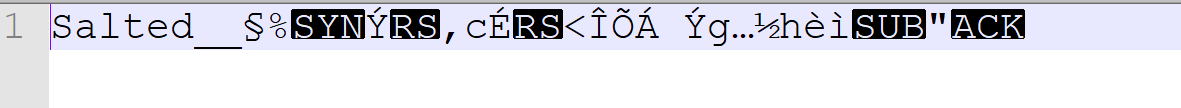
10. OpenSSL rsautl -decrypt -inkey keypairB.pem -in encfile.bin -out fileclear.txt



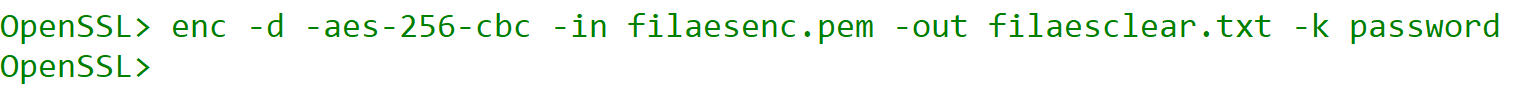


11. Openssl enc -d -aes-256-cbc -in fileaesenc.pem -out filaesclear.txt -k password





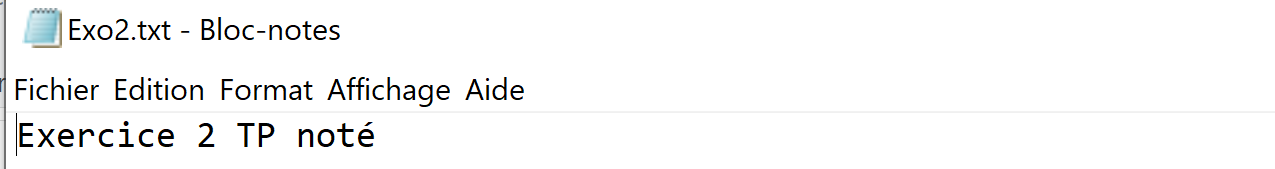
12. OpenSSL enc -d -aes-256-cbc -in filaesenc.pem -out filaesclear.txt -k password

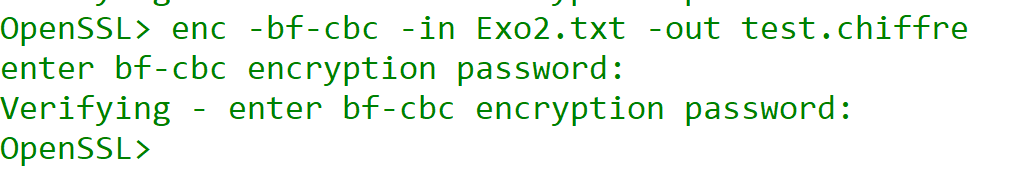




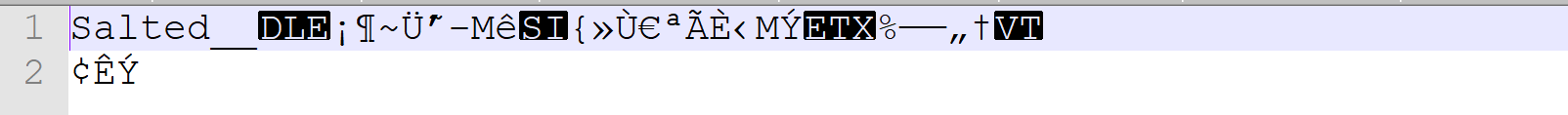
Exercice 2 :

1.OpenSSL enc -bf-cbc -in Exo2.txt -out test.chiffre

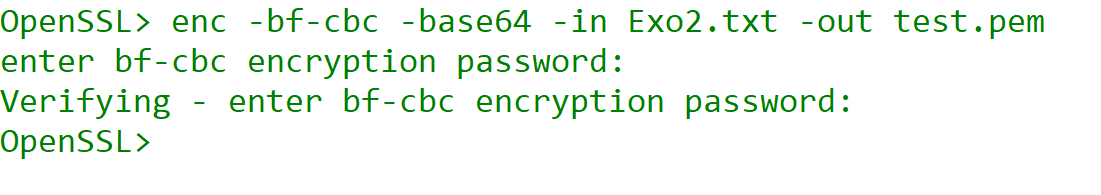




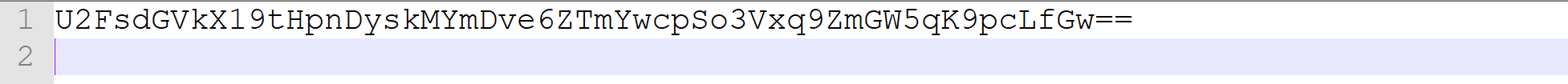
2. Le fichier générer : test.chiffre



3. OpenSSL enc -bf-cbc -base64 -in Exo2.txt -out test.pem

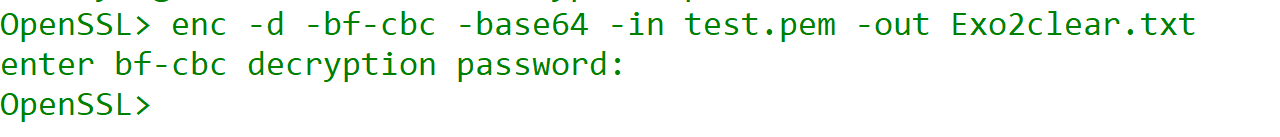


Fichier générer :



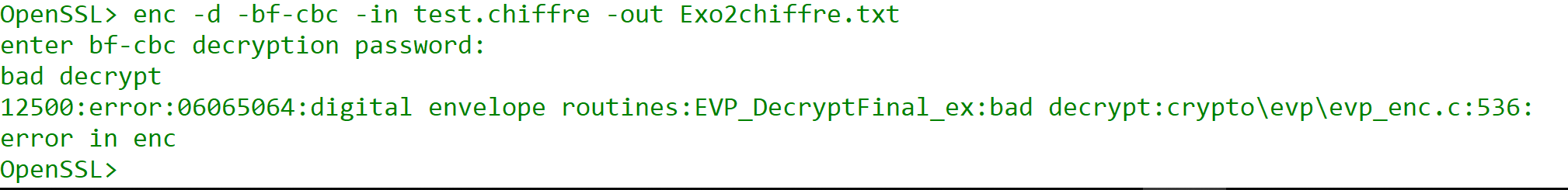
base64 est un encodage qui utilise 64 caractère ASCII disponibles sur la plupart des systèmes informatiques

4.





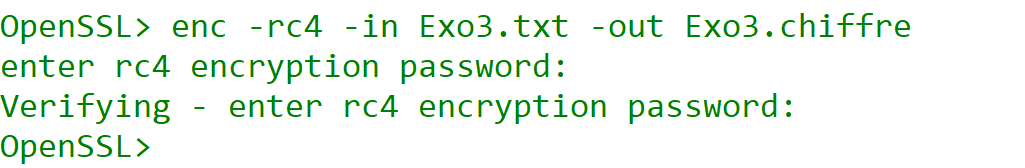
5.

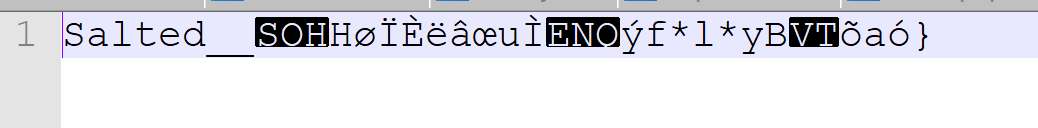


OpenSSl refuse de déchiffrer le fichier.

Exercice 3 :

1.

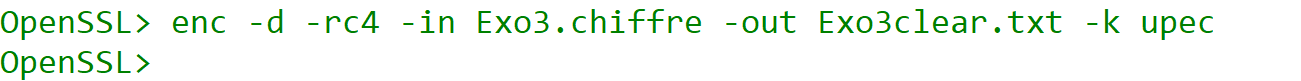


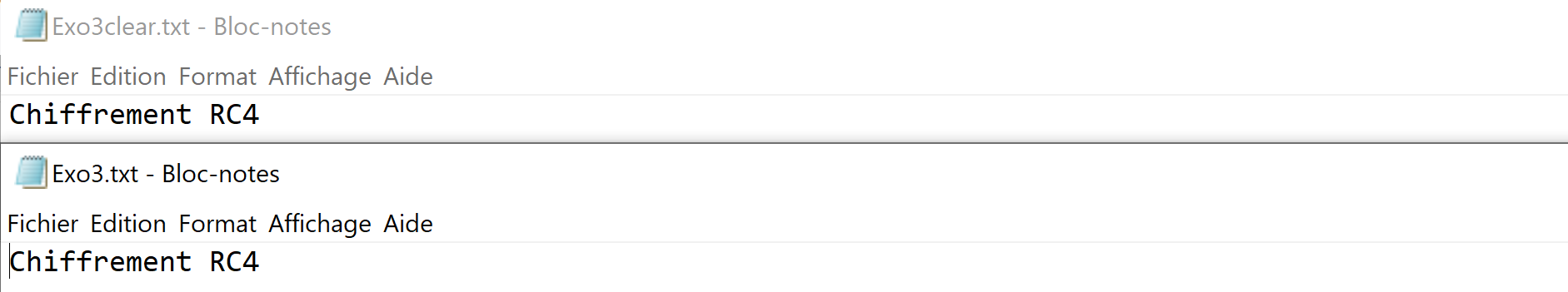


2. Ajout direct du mot de passe



3.

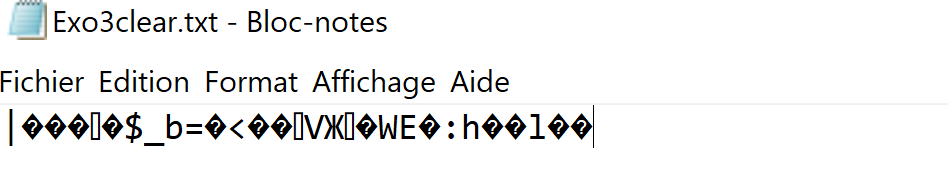




4.

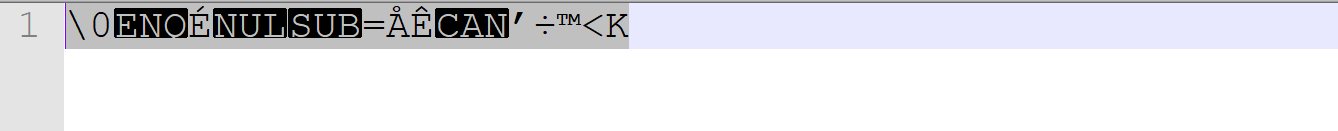


Fichier générer avec l’option –nosalt



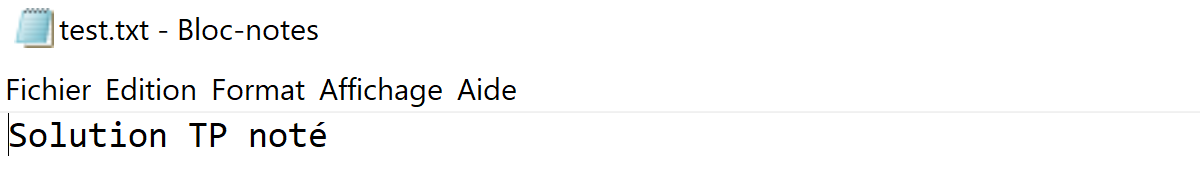
5.



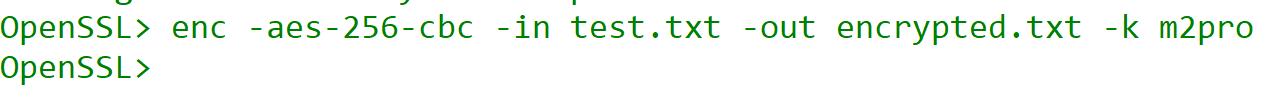


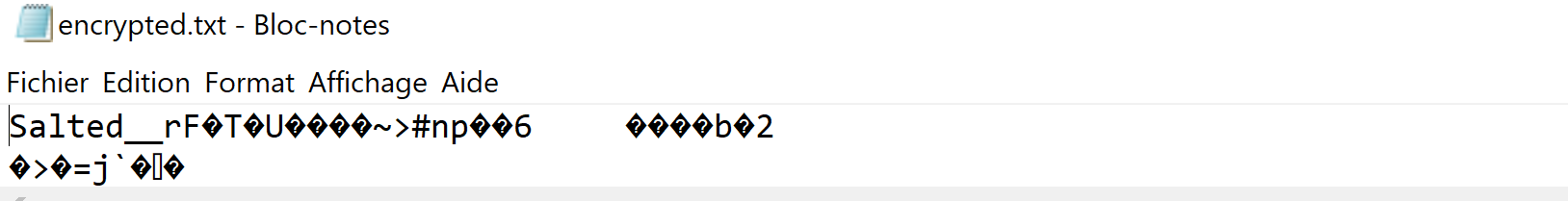
Exercice 4 :

1.



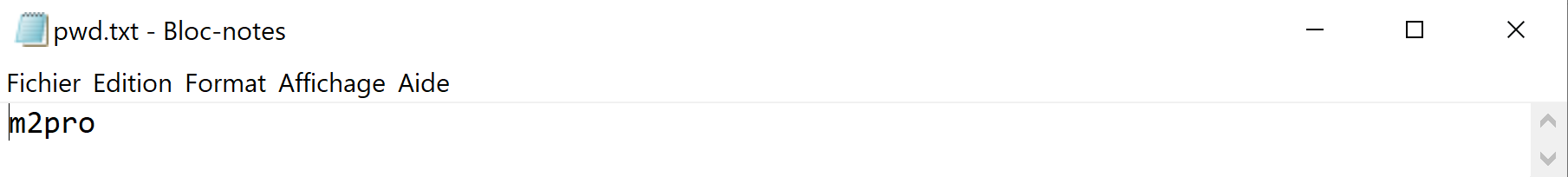
2.

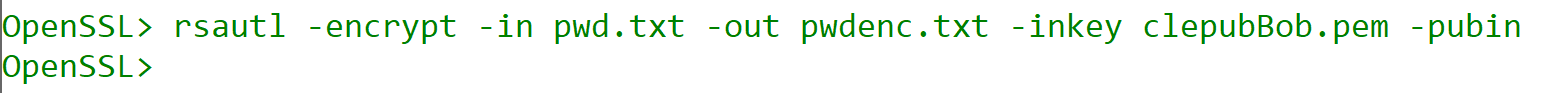




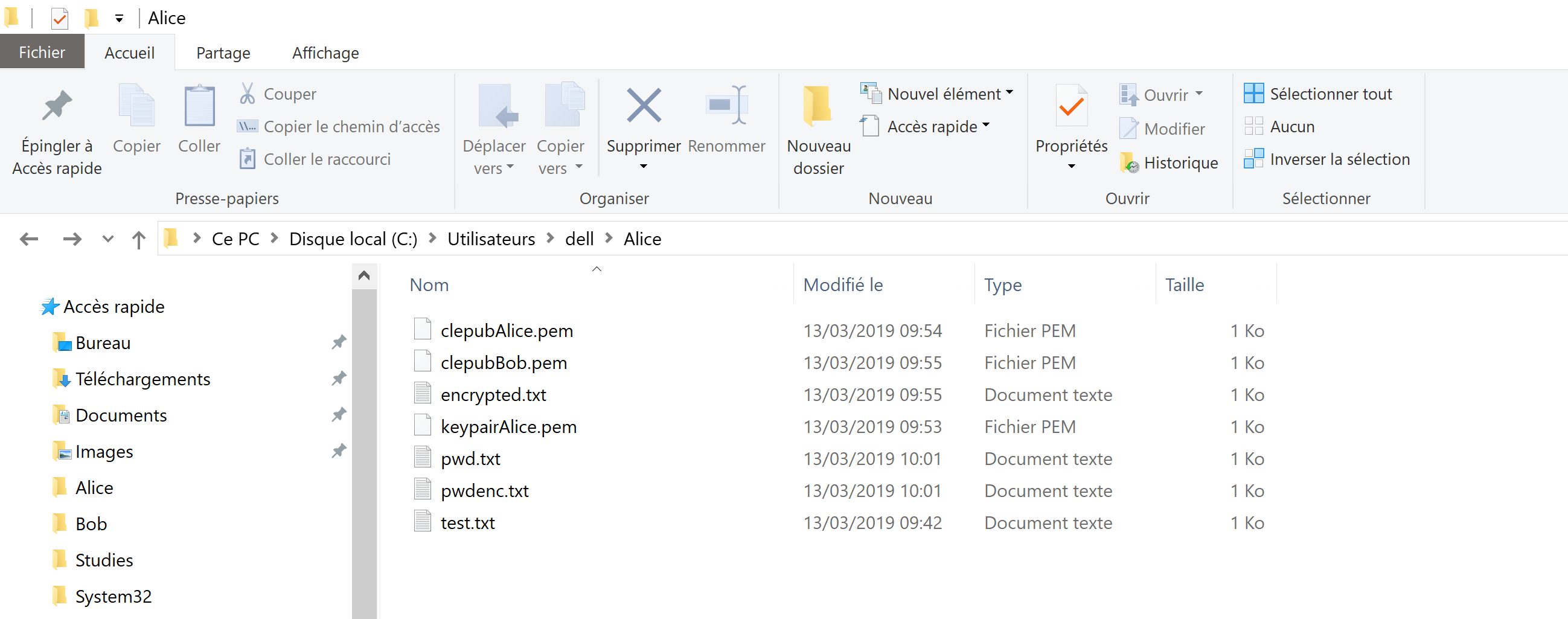
3.

On a mis la clé publique de bob dans le dossier d’alice pour qu’alice puisse chiffrer le mot de passe avec la clé publique de bob.





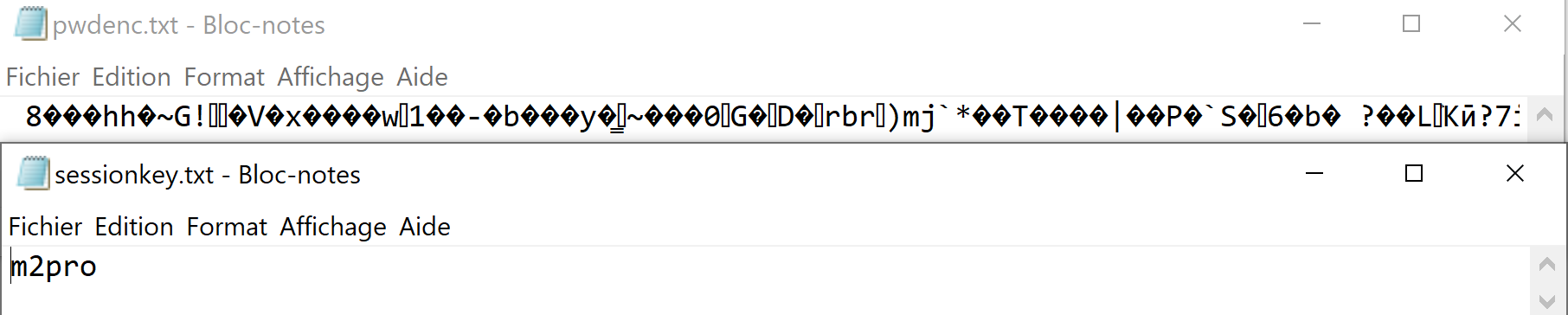
Dossier Alice :



Etape 2 :

Bob décrypte le mot de passe crypté par alice avec sa clé privée





Bob décrypte le fichier avec la clé de session qu’il a généré

