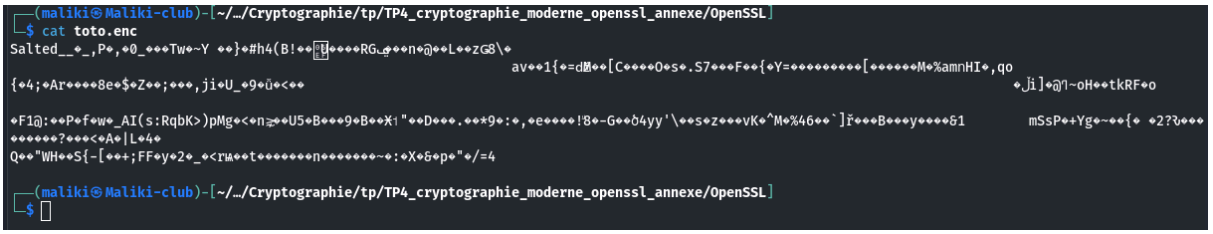
Travaux pratiques 1 : Crypto

Abdel-Malik FOFANA
Ivan KRIVOKUCA

Exercice 1:

-> chiffrement : openssl enc -bf-cbc -in toto.txt -out toto.enc -k master1
-> dechiffrement : openssl enc -bf-cbc -d -in toto.enc -out toto.dec -k master1

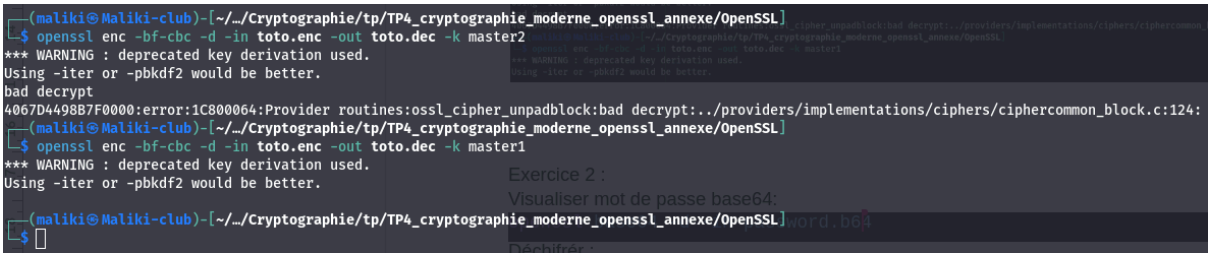
le fichier affiche ceci:



Le codage est : Blowfish en mode CBC ducoup hexadécimal (Cipher Block Chaining car on a mis “enc -bf-cbc” en option dans la commande)

->chiffrement en base 64 : openssl enc -bf-cbc -in toto.txt -out toto.b64 -k master1 -base64
Le codage est : base64

-> Voici ce qui se passe quand on dechiffre avec le mauvais et bon mot de passe



quand le mot de passe est mauvais, le terminal nous dit que le déchiffrage est mauvais.

Exercice 2 :
Visualiser mot de passe base64 et mettre le mot de passe en claire dans password.bin:

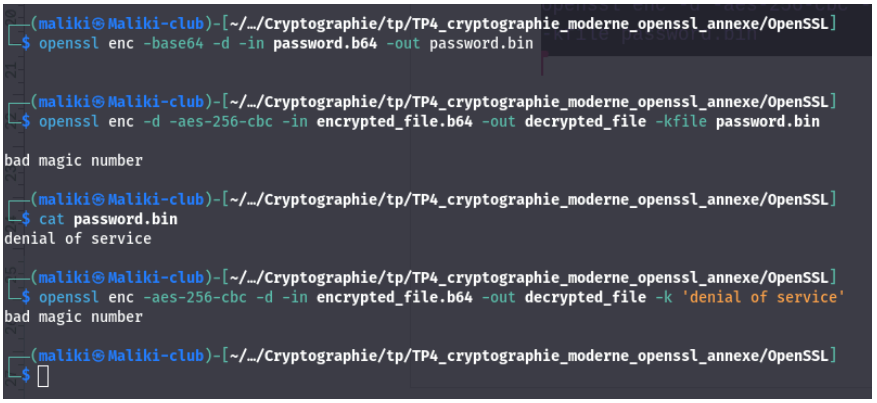
```
openssl enc -base64 -d -in password.b64 -out password.bin
```

Déchifrér à encrypted_file.b64 :

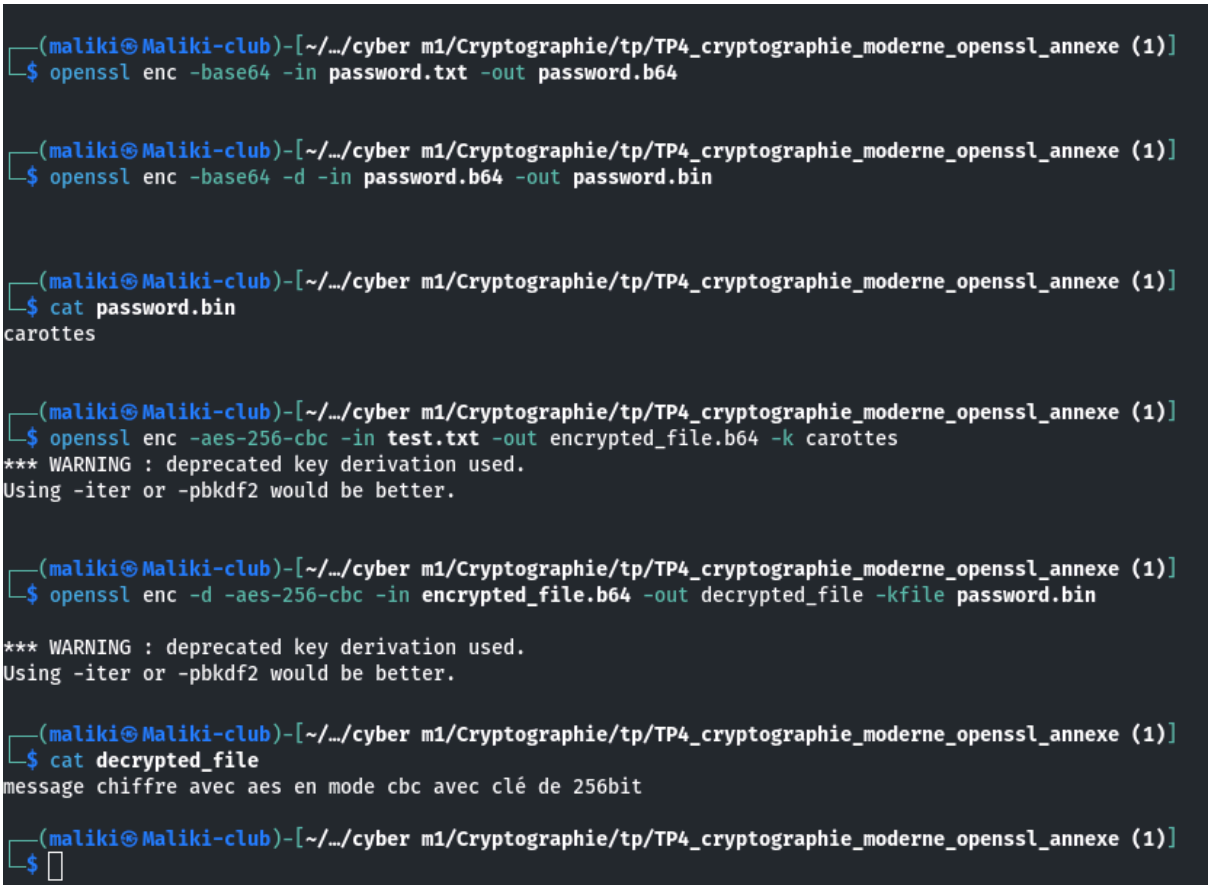
```
openssl enc -d -aes-256-cbc -in encrypted_file.b64 -out decrypted_file
-kfile password.bin
```

le mot de passe est : denial of service

cependant le mot de passe ne fonctionne pas voici la preuve :



j'ai donc refait l'exercice avec un fichier bien crypter par mes soins avec le mot de passe "carottes" et cela marche :



Exercice 3 :

```
1. openssl genrsa -out rsaprivatekey.pem 1024
```

1. `openssl rsa -in rsaprivatekey.pem -text -noout` (pour avoir et ensuite visualiser le contenu du fichier avec *openssl rsa*.)

2. `openssl rsa -in rsaprivatekey.pem -des3 -out rsaprivatekey.pem.des3 -passout pass:securite` → protège la clé avec le mdp securité

Clé normale:

```
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAMhKRTUAXOf04hR/
bxSn1EsKWuYhVldedFQzy5IN3BU8x1LB3dWL4Fih1oIQT19nJuwQlOuycXbXaV72
M0vHj+8itfb8vfoeJgEy+dekM0ZesDnDjoNabMuv7IsK30AvTFEhEHbuYvU7z6UH
jOQZVF7fT0RQBwb57vJOe400OFz5AgMBAAECgYEAs81AvajavnyurDoOLRvQz6C3
I1qQGRS5F5H70NzSUtpiEV/qVjcgqlB2sgIUTw/Z+BeWqNRjWY1dkZsxR3kaMrt+
MHGgI5UNZp9LSNqK1D2Qqgcnv7CWOFwnW6ZqBFreVusVrjJ53xKSaj3nibi3nPzd
FUp3rVtqiEHetbXeLjUCQQDlZMjV0DQs9WMh1vXDJu0fUy7QfSSs6oeqjExEI3Zz
XuWgMb3z1/8HD5pfsFAgSkafvsUEOAEuLvxERs2u4y5HAkEA34VV0b7HPO2/gymX
Zg5IE1ibMQXKrPGOBZy2M/uqhdDkzGJbWv5REEi+K+lWcKIpLnWMigGckobBh+7B
RH16vwJAFTRNxEXsrMM6GKSwLwvoG18rEqaev0UmqUMywZGtn1iETVyLvICY2GQ+
1t2LapCzGo0d1RgAM+6v7vfEh4gEfQJAJPlwdc7CNID7kh3aLoakQ5b/rP9RRIR8
ws7mkPjLf3FLt8d5Zzb0f+YYlzj1FJKuj0Hgqp+Tn+VstCi5jbPYDwJABgRgT1YY
CnvaaBQWyW4TT+hWsoCXdYihvlLT2lhO5718W7BQZrmyOgo63jSi6zZ0TBlEjGEh
PXg8Nq+pYpmygw==
-----END PRIVATE KEY-----
```

cat affiche :

Clé 3DES

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIC1DBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQI/g+h9p0wZg0CAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECC12oXFh4Sv/BIICgOVd6rgMpd/k
K2OkMjk4VoeHyOZbfxHr5xzEZ9lKmylwjeEvYXKJZ2BwIYgDLSAeVRNMXD7VDTSG
XK8zFo8sOpHoCJ2XQ3Chn70wdrGflCte1/2ngz3OX9t1taLDWOUQaM1ZjomEvyeG
0YryHClD3Zhp8ntZNgCnz//3+/Nk93A605ZQZPH+Bjn2OMHR7jFQzGdQwtCS+Cu5
WXCktJdk9/ewQmsQIRNk4usWXLzFlPkC3FCeVrQPgRXQG4JPhVQ/ZY8xWLMCMZJH
k3z0gmmZzLw3GTE8bQcBwkhVojgs5PnLJ10eAgdKJWxyjNC4t9iEuZUcCMFlfa7r
gIswAgnj7ATE/OntK799deexTtdThOzXgSDtKDZlYIoTm6H9+JWccJ3E09pTv9Ka
bPMNHKi3LOsY3GWg0o3tK6tUxS489pvlTaB2zSHBkcjr7dzV0l3ybSJdOWmsvxcw
0In2MTLFWQu+hCU2do5dxBR0u46TraDneJdIIEeqTBRxWa6Hk2mMMiBP7clGoyEf
FNMo5iFyPQJ/dHQFl2G2ziMIkdb1RQxudZ5KtdiGBnObt+CJGCbq82NuH6LUtSVp
s4VcnFSYCFjPihpSREiaxD6kk8K088jhZdv1pJR5PwmMXlHg+Th1UhON1WlrHq/5
mX0vGZY75LUNU/tNSrbrWX6r33rl90gA6KqPFrqupKvquG6ntN2LsK6weWExba0R
r9XdWy7/bcP1xXWLZecawBqY/Lw+4xGZxzgx+/atV+YON2WZNavwNv0XUtw4KKrw
GOxt94DIM8yC1fkvBHGQq9kjVKo+fHoaqUQsc8tf1hDrQeikXgc0fAk2nbDBv582
gmdIpjh6u4I=
-----END ENCRYPTED PRIVATE KEY-----
```

Pour regarder les caractéristiques de la clé, on nous demande le mot de passe de la clé

```
~/Bureau/M1/UPC/crypto/OpenSSL ❯ openssl rsa -in rsaprivatekey.pem.des3 -text -noout
Enter pass phrase for rsaprivatekey.pem.des3:
```

(si le mdp rentrée est bon alors il affiche les caractéristiques de la clé, sinon il affiche une erreur)

3. `openssl rsa -in rsaprivatekey.pem -pubout -out rsapublickey.pem`

   `openssl rsa -pubin -in rsapublickey.pem -text -noout`

4. `echo "Ceci est un message classé confidentiel \!" > message.txt`
5. `openssl pkeyutl -encrypt -in message.txt -out message.enc -pubin -inkey rsapublickey.pem`

Exercice 4:

1.