Exercice 3

Le fichier *aes-128-ecb.enc* a été chiffré en AES mode ecb, la clef de chiffrement en base64 donnant : Y2VjaWVzdHVuZWNsZWY=

1 - Déchiffrez le fichier *aes-128-ecb.enc* et affichez son contenu.

```
nderousseaux@david ex3 % KEY=$(openssl base64 -d <<< Y2VjaWVzdHVuZWNsZWY=)

nderousseaux@david ex3 % openssl aes-128-ecb -d -in aes-128-ecb.enc -pass pass:$KEY
Bravo !! Vous avez réussi à déchiffer
```

2 - Créez un fichier *secret* dont la taille (en octets) ne soit pas un multiple de 8.

```
nderousseaux@david ex3 %  head -c 13 < /dev/urandom > secret
```

3 - Chiffrez-le sans *grain de sel* avec le système Blowfish en mode CBC. Le fichier chiffré se nommera *secret.enc*.

```
nderousseaux@david ex3 % openssl bf-cbc -in secret -out secret.enc -nosalt -pass
pass:password
```

4 - Déchiffrez ce fichier et enregistrez le résultat dans un fichier *secret.dec*. Vérifiez le contenu.

```
nderousseaux@david ex3 % openssl bf-cbc -in secret.enc -out secret.dec -nosalt -d -pass
pass:password
nderousseaux@david ex3 % xxd secret secret.bin

nderousseaux@david ex3 % xxd secret.dec secret.dec.bin
nderousseaux@david ex3 % diff secret.bin secret.dec.bin
nderousseaux@david ex3 % echo $?
0
```

5 - Comparez la taille des trois fichiers (clair,chiffré et déchiffré). Que constatez-vous?

On peut constater que le fichier chiffré `secret.enc` est un multiple de 8, on peut supposer que l'algorithme rajoute des octets manquants pour arriver à un multiple de 8.

L'algorithme de déchiffrage supprime les octets rajoutés lors du chiffrement.

6 - Déchiffrez maintenant votre fichier secret.enc en *secret2.dec* en utilisant l'option *-nopad*.

```
nderousseaux@david ex3 % openssl bf-cbc -in secret.enc -out secret2.dec -nosalt -d -
nopad -pass pass:password
```

7 - Comparez à nouveau les tailles des trois fichiers obtenus.

Avec l'option `-nopad`, on constate que la commande de déchiffrage n'a pas supprimé les octets ajoutés lors du chiffrement.

8 - Visualisez le fichier *secret2.dec* avec nano ou vi puis avec la commande *xxd*. Qu'en déduisez-vous?

Dans mon exemple, on peut constater que le processsus de chiffrement à ajouté 3 `0x03` à la fin de mon message pour arriver à un multiple de 8. On peut on conclure que l'algorithme travaille par bloc de 8 octets.