

TP : La cryptographie symétrique

OpenSSL est un logiciel de cryptographie qui possède de nombreux algorithmes de chiffrement. OpenSSL est disponible sur les systèmes **windows/linux/mac** et s'utilise en ligne de commandes.

Voici les commandes que nous allons utiliser :

Pour encoder :

```
1 openssl enc -e -encodage -in mon-fichier.txt
2 openssl enc -e -encodage -in mon-fichier.txt -out mon-fichier-crypte.txt
```

Pour décoder :

```
1 openssl enc -d -encodage -in mon-fichier.txt
2 openssl enc -d -encodage -in mon-fichier-crypte.txt -out mon-fichier-decrypte.txt
```

Parmi les nombreux encodages, on s'intéresse aux algorithmes de chiffrement **base64** et **aes-256-ecb** qui nécessite une clef (mot de passe).

- 1) Créer un fichier texte contenant un message court.
- 2) Chiffrer votre message avec l'algorithme base64 puis envoyer le à un camarade pour qu'il le déchiffre.
- 3)
 - a) Chiffrer votre message avec l'algorithme aes-256-ecb avec une clef de votre choix.
 - b) Envoyer votre message à un camarade en lui communiquant la clef.
- 4)
 - a) Créer un nouveau message court.
 - b) Chiffrer votre message avec l'algorithme aes-256-ecb en utilisant la clef de votre choix.
 - c) Chiffrer votre clef avec l'algorithme base64.
 - d) Envoyer le message et la clef à un camarade pour qu'il le déchiffre.
- 5) Sur le web, dans le code source des pages html, il arrive d'avoir des images encodées avec l'algorithme de chiffrement base64. Le source de l'image de la page html ne contient pas une url mais le code encodé avec l'algorithme base64.

Nous allons faire une petite démonstration.

- a) Créer une page html contenant une image au format jpg :

```
1 <!DOCTYPE html>
2 <html lang="fr">
3 <body>
4 <img src='chemin/vers/mon/image' />
5 </body>
6 </html>
```

- b) Chiffrer votre image avec **openssl** en utilisant l'algorithme base64.
- c) Copier et coller votre code chiffré dans votre image comme ci-dessous :

```
1 <!DOCTYPE html>
2 <html lang="fr">
3 <body>
4 <img src='data:image/jpeg;base64, votre-code-chiffré-en-base64' />
5 </body>
6 </html>
```