Cryptographie

TD n°2 : Chiffrement symétrique

Exercice 0

Deux mots de 7 lettres de la langue française ont été chiffrés avec la même clé. Les chiffrés sont **WIBXBCY** et **PIBKMAJ**. Quels sont ces deux mots ?

Note: Pour tous les exercices suivants, vous pouvez utiliser le package Python `cryptography` (il s'installe avec la commande `pip install cryptography`).

Exercice 1

Un texte de taille 16 octets a été chiffré en AES avec la clé (en hexadécimal) 0123456789ABCDEF0123456789ABCDEF et le chiffré obtenu est C682093BF20041C1053FF19C9FE6AF71. Quel était le message clair ?

Note : pour convertir une chaîne donnée sous format hexadécimal en séquence d'octets, vous pouvez utiliser la fonciton Python suivante : `bytes.fromhex`

Exercice 2 (optionnel)

A l'aide de la bibliothèque `cryptography`,

- écrivez une fonction effectuant le chiffrement et le déchiffrement d'un seul bloc d'AES, en prenant en entrée le texte à (dé-)chiffrer (de taille 16 octets) et la clé
- implémentez le mode de chiffrement CBC avec le padding de votre choix

Exercice 3 : un programme de chiffrement de fichier simple

Ecrivez un programme qui permette à son utilisateur de chiffrer un fichier. Votre programme doit prendre en entrée :

- le nom du fichier à chiffrer
- le nom du ficher chiffré à créer
- le mot de passe (de préférence, il ne doit jamais s'afficher en ligne de commande !)

Pour transformer un mot de passe en clé, vous pouvez regarder du côté des fonctions de dérivation de clé (`Key derivation functions`) du module `cryptography`.

Quel mode et quel algorithme de chiffrement utilisez-vous ? Pourquoi ?