**TIPE Cryptographie python**

Tout d’abord afin de comprendre comment fonctionner la cryptographie en python nous avons tout d’abord fait des tests avec des méthodes simple. Ce qui nous a donner un premier programme qui utilise le code ASCII de chaque caractère.

Nous avons ensuite fait des recherches sur les différentes méthodes de cryptage possible avec les bibliothèques python. Les recherches nous ont mené à différentes méthodes de cryptage :

* La méthode avec cryptage symétrique. Celle-ci permet le cryptage de fichier et un stockage sécurisé. Ce type est sécurisé car il est mathématiquement complexe. Ce type de cryptage est possible avec deux algorithmes diffèrent. Le AES et le Fernet. Le type AES est un algorithme qui supporte différentes tailles de clé et différents modes de chiffrement par exemple ECB (Electronic CodeBook) : chiffre chaque bloc de 128 bits indépendamment avec la même clé, rapide mais peu sécurisé. Mais aussi CBC (Cipher Block Chaining) : chaque bloc crypté dépend du bloc précèdent, beaucoup plus sécurisé que le ECB mais plus lent du au traitement séquentielle des blocs. Il y a aussi CFB, OFB … Fernet quant à lui utilise le mode CBC. Fernet permet de crypter des documents mais de vérifier avant cela si celui-ci est corrompue ou non. Le cryptage symétrique n’est décryptable qui si la clé de décryptage est détenue entièrement par la personne qui déchiffre.
* Il y a ensuite la méthode de cryptage asymétrique, celle-ci permet des communications sécurisées. Ce qui la rend sécurisé est la difficulté à factoriser de grand nombre premier. Cette méthode est permise grâce a l’algorithme RSA (Rivest Shamir-Adleman) contrairement au cryptage symétrique ici deux clés sont utilisées : la première publique utiliser pour chiffrer et la seconde privée afin de pouvoir déchiffrer.
* Enfin la méthode de Hachage. Celle-ci est une opération cryptographique qui transforme des données en une empreinte unique et irréversible. Il est utilisé pour vérifier l'intégrité des données, stocker des mots de passe et sécuriser des transactions. Cette méthode est sécurisée car elle est non réversible et qu’elle resiste aux collisions ce qui signifie que pour deux entrées différentes le hachage ne pourra jamais être le même.

Sur ce projet de TIPE nous avons pris le choix de faire du cryptage de fichier de ce fait nous avons choisis la méthode de cryptage symétrique avec Fernet. De ce fait nous nous sommes beaucoup moins préoccuper des autres méthodes possibles. En python il existe différentes bibliothèques de cryptage, nous avons pris le choix ici d’utiliser la bibliothèque cryptography qui contient les fonctions de Fernet.

Le fait de vouloir faire un programme de cryptage de fichier nous avons donc due utiliser une bibliothèque d’interface graphique afin de pouvoir sélectionner les fichiers et de les crypter. Notre choix a été tkinter du a son utilisation assez intuitive et poussé. Cette bibliothèque nous a permis d’obtenir une fenêtre ou l’on peut choisir le fichier à crypter directement dans l’explorateur de fichier et ensuite de le crypter en appuyant sur le bouton prévu à cet effet.

Nous avons aussi utilisé la bibliothèque os qui nous a permis de traiter tout ce qui tourner autour des fichiers et des dossiers d’enregistrement. Cela nous a permis de réaliser les actions voulu le plus simplement possible.