TP
DES

Les pièces suivantes vous ont été transmises :

1. `DES.pdf` est un cours détaillant très précisément comment le chiffrement suivant DES fonctionne avec le traitement d'un exemple complet.
2. Des documents texte : `Chiffrement_DES_de_1.txt`, `Chiffrement_DES_de_2.txt`, `Chiffrement_DES_de_3.txt`, `Chiffrement_DES_de_4.txt`, `Chiffrement_DES_de_5.txt` et `Chiffrement_DES_de_6.txt` qui sont des messages chiffrés suivant le protocole DES. En particulier, ces documents sont en binaire.
3. Des documents texte : `Clef_de_1.txt`, `Clef_de_2.txt`, `Clef_de_3.txt`, `Clef_de_4.txt`, `Clef_de_5.txt` et `Clef_de_5.txt` qui sont des clefs (huit octets) du chiffrement DES. La `Clef_de_X.txt` a permit d'obtenir le message `Chiffrement_DES_de_X.txt`.
4. Un répertoire `Bonus` contenant 3 fichiers :
   - `ConstantesDES.txt`, un fichier texte avec les nombreuses constantes du chiffrement DES.
   - `Extract_ConstantesDES.py`, un fichier python, avec une fonction, qui lorsqu'elle est appelé dans le même répertoire que le fichier `ConstantesDES.txt` renvoie un tableau associatif `X` avec les constantes chargées (`X['PI']` contient la permutation initiale, `X['CP_2']` la seconde permutation des clefs etc...). Explorez cette fonction pour déterminer les noms de clefs du tableau retour de cette fonction.
   - `ConvAlphaBin.py` un fichier python indiquant le codex qui a été utilisé pour transformer les caractères de texte en binaire. On observera en particulier que les caractères ont été codé sur 5 bits donnant ainsi un champ de valeur de 00000 (qui est la lettre `A`) à 11111 (qui est le caractère de saut de ligne).

Le but de ce projet est multiple :

1. Comprendre le principe de chiffrement DES.
2. Produire en `Pyhton3` un programme automatisant le chiffrement DES.
3. Donner les éléments mathématiques permettant de déchiffrer un message chiffré en DES.
4. Produire en `Pyhton3` un programme automatisant le déchiffrement DES.
5. Déchiffrer les messages.