Projet
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. Cinq documents texte : `MDES1.txt`, `MDES2.txt`, `MDES3.txt`, `MDES4.txt` et `MDES5.txt` qui sont des messages chiffrés suivant le protocole DES. En particulier, ces documents sont en binaire.
3. Cinq documents texte : `Clef1.txt`, `Clef2.txt`, `Clef3txt`, `Clef4.txt` et `Clef5.txt` qui sont des clefs (huits octets) du chiffrement DES. La `ClefX` a permit d'obtenir le message `MDESX`.
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 l'un des 5 messages qui vous aura été attribué.

Les livrables attendues sont :

1. Un programme en `Pyhton3` automatisant entièrement le processus de chiffrement et de déchiffrement DES. Un exemple de produit final pourra être :
   - Demander à l'utilisateur le mode d'utilisation (chiffrer ou déchiffrer)
   - Inviter l'utilisateur à saisir son texte (ou le chemin d'un fichier avec le texte) ainsi que la clef (ou le chemin d'un fichier contenant la clef).
   - Préciser le mode de retour (affichage ou écriture dans un ficher).
   - Réaliser le (dé)chiffrement
2. Un rapport détaillant, sur l'exemple du cours, le principe de déchiffrement. Cela devra être exposé aussi précisément que dans le cours. Pour produire ce rapport vous pourrez utiliser du LaTeX, langage éditeur d'équation, qui peut se faire directement en ligne par exemple ici : `latexbase.com`.