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. Également disponible en ligne sur ataraXy.
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).

Un seul livrable est attendu sous deux formats : le document jupyter au format `.ipynb` et le même document au format `.html` (sous jupyter sélectionner *file* puis *download as*).

Les éléments qui devront apparaitre dans votre document sont au minimum :

— Les codes en python, commentés avec des noms de variable lisibles et raisonnables, permettant de chiffrer et de déchiffrer le protocole DES.
— Des éléments rédactionnels articulant vos fonctions, programmes et idées (en markdown, l'utilisation de LaTeX sera appréciée mais non obligatoire)
— Des explications détaillant la méthode utilisée pour déchiffrer du DES (en markdown, l'utilisation de LaTeX sera appréciée -voir indispensable- mais non obligatoire).
— La dernière case du document jupyter devra indiquer le processus de gestion du projet. Il pourra prendre des formes diverses et variées, laissés à l'appréciation des étudiants sur la gestion du projet (tableau récapitulant les missions, leur temps et les participants, la proportions de l'implication de chacun, etc).
— Cette dernière case devra se terminer par la phrase suivante, qu'il faudra compléter : *La note estimée pour ce projet par le groupe est* x*/20.*

En plus de ces éléments, le groupe pourra ajouter à sa convenance tous les éléments qui valoriseraient son travail. L'utilisation de librairies folkloriques est libre mais peut être dangereuse, surtout si elles cachent le principe et les calculs. Il n'est pas demandé de déchiffrer les messages transmis, mais cela peut être appréciable.

La grille critérié de l'évaluation est la suivante :

Évaluation du groupe.

- Respect des règles du rendu (5 points max)
- Cohésion du groupe (1 point max)
- Qualité de la soutenance (2 points max)
- Niveau d'expertise, défi technique, regard scientifique (2 points max)

Évaluation individuelle.

- Comportement au sein du groupe (1 point max)
- Implication dans le projet, difficultés (5 points max)
- Interaction avec le jury (1 point max)
- Démonstration et fonctionnement de la solution (3 points max)