Année Universitaire :2024 – 2025
Département : Informatique
Module : Complexité et Cryptographie
Master : IDLD
Semestre: 2

Université Mohammed V
Faculté des Sciences
Rabat

Travaux Pratiques de Cryptographie Appliquée
TP2 : Cryptographie Moderne (DES)

Objectif : Implémenter l'algorithme de chiffrement DES (Data Encryption Standard) en Python, en manipulant directement des données binaires pour chaque étape du processus de chiffrement et de déchiffrement.

Consignes :

1. **Conversion texte-binaire :**
    - Développer une fonction permettant de convertir un texte clair (en ASCII) en une représentation binaire (chaîne de bits).
    - Développer une fonction inverse permettant de convertir une chaîne binaire en texte clair.
2. **Initialisation des blocs :**
    - Traiter le texte clair par blocs de 64 bits.
    - Ajouter un padding si le texte clair n'est pas un multiple de 64 bits.
3. **Permutations et tables :**
    - Implémenter les permutations et tables du DES suivantes :
        - Permutation initiale (IP)
        - Permutation inverse (IP^{-1})
        - Extension (E)
        - Permutation des P-box (P)
        - Tables PC1 et PC2 pour la génération des sous-clés.
4. **S-Boxes :**
    - Implémenter les 8 boîtes S conformes à la spécification DES.
    - Chaque boîte S prend un bloc de 6 bits en entrée et produit 4 bits en sortie.
5. **Génération des sous-clés :**
    - Générer 16 sous-clés à partir d'une clé principale de 64 bits.
    - Appliquer les décalages circulaires et les permutations PC1 et PC2 conformément à l'algorithme DES.
6. **Processus de chiffrement :**
    - Implémenter l'algorithme Feistel :
        - Diviser le bloc binaire en deux moitiés : gauche (L) et droite (R).
        - Appliquer 16 itérations du processus Feistel, incluant :
            - Expansion de R (fonction E).
            - XOR avec la sous-clé actuelle.
            - Passage par les S-boxes.

        - Application de la permutation P.
        - XOR du résultat avec L.
    - Echanger L et R après chaque itération, sauf à la dernière.
7. **Processus de déchiffrement :**
    - Implémenter l'algorithme de déchiffrement en utilisant les sous-clés dans l'ordre inverse.
8. **Interface utilisateur :**
    - Développer une interface permettant :
        - De saisir un texte clair et une clé en ASCII.
        - D'afficher les résultats du chiffrement sous forme binaire.
        - De déchiffrer un texte chiffré et d'afficher le texte clair obtenu.

Données : Fournissez les tables et constantes suivantes :

- Tables IP, IP_INV, E, P.
- Tables PC1, PC2.
- Contenu des 8 S-boxes.

Livrables :

1. Code source Python bien commenté et écrit de manière modulaire.
2. Documentation expliquant les étapes principales et l'utilisation du programme.