Exercices
Semaine 11

Cours Turing

1 Système DES simplifié

Dans cette exercice, nous vous proposons d'implémenter une version simplifée du système DES. En entrée, votre programme demandera une clé K (au format str, de longueur paire), ainsi qu'un texte T (au format str), dont la longueur soit un multiple de la longueur de la clé K.

a) Chiffrement : La première étape consiste à couper le texte T en une suite de messages M de même longueur que la clé K, puis pour chaque message M :

- convertir $M = (M_a, M_b)$ et $K = (K_a, K_b)$ en deux suites de nombres compris entre 0 et 25 ;

- calculer le message chiffré $C = (C_a, C_b)$ selon le schéma suivant :

pour la première moitié : $C_a[i] = M_a[i] \oplus f(K_a[i], M_b[i])$, $i = 0, \ldots, n-1$
(où on rappelle que $\oplus$ désigne l'addition modulo 26)

pour la seconde moitié : $C_b[i] = M_b[i] \oplus f(K_b[i], C_a[i])$, $i = 0, \ldots, n-1$

- finalement, convertir le message $C = (C_a, C_b)$ en string, et ajouter ce message chiffré au texte chiffré final.

- et répéter la même suite d'opérations pour toutes les parties du texte.

Remarque : Vous avez le choix de la fonction f ! Mais pour simplifier, nous vous proposons ici de choisir une fonction f non-linéaire qui agit sur deux nombres seulement, et pas sur les deux suites de nombres (vous pourriez par exemple choisir la fonction définie par $f(A, B) = A**B$).

b) Déchiffrement :

Refaire la même chose, mais en utilisant successivement :

pour la seconde moitié : $D_b[i] = C_b[i] \ominus f(K_b[i], C_a[i])$, $i = 0, \ldots, n-1$
(où on rappelle que $\ominus$ désigne la soustraction modulo 26)

pour la première moitié : $D_a[i] = C_a[i] \ominus f(K_a[i], D_b[i])$, $i = 0, \ldots, n-1$