TP1

September 2022

1 Introduction

Objectif: mettre en pratique les connaissances théoriques vues en cours et en TD papier.
Prérequis:

- Connaître le chiffre de César et le chiffrement par bloc

Connaissances à acquérir:

- Être capable d'implémenter en Python le chiffre de César et un chiffrement par bloc

Instructions: Réaliser ces exercices seul.

2 Chiffrement par substitution

2.1 Chiffre de César

Implémentez une fonction qui prend en paramètre une chaîne de caractères et un nombre n, puis retourne le message chiffré correspondant à la chaine en paramètre déplacée sur la droite de n caractères. Par exemple:

- entrées: "ABC", 4
- sortie: "EFG"

2.2 Casser le chiffre de César

Proposez une fonction permettant de casser le chiffre de César en vous basant sur une analyse des fréquence des caractères de votre message chiffré et du tableau ci-dessous. Votre fonction prendra en paramètre le message chiffré et retournera une proposition de message déchiffré.

Fréquence des caractères[2] sur le corpus de Wikipédia en français

Rang	Caractère	Nombre d'occurrences	Pourcentage	
1	e	115 024 205	12.10%	
2	a	67 563 628	7.11%	
3	i	62 672 992	6.59%	
4	s	61 882 785	6.51%	
5	n	60 728 196	6.39%	
6	r	57 656 209	6.07%	
7	t	56 267 109	5.92%	
8	o	47 724 400	5.02%	
9	l	47 171 247	4.96%	
10	u	42 698 875	4.49%	

Figure 1: Fréquence des lettres dans le texte à déchiffrer

3 Chiffrement par bloc avec AES

L'objectif de cet exercice est de chiffrer votre fichier et de le sauvegarder sur votre disque dur, puis, à l'aide de votre clé, le déchiffrer pour vérifier son intégrité (si c'est un pdf, vous pouvez l'ouvrir par vous même pour vérifier qu'il soit lisible). Pour réaliser cet exercice, vous devrez utiliser le package *aes-cipher 2.0.0* de Python. Vous pouvez trouver ce package et sa documentation au lien suivant: *https://pypi.org/project/aes-cipher/*.

Développez deux fonction:

- une fonction prenant en paramètre le nom d'un fichier que vous souhaitez chiffrer sur votre disque dur (par exemple, ce sujet en pdf). La fonction doit également prendre en paramètre une clé permettant de chiffrer votre fichier.
- une fonction prenant en paramètre le nom d'un fichier que vous souhaitez déchiffrer sur votre disque dur. La fonction doit également prendre en paramètre une clé permettant de déchiffrer votre fichier.

4 Pour les plus rapides

Développez une application console avec un paradigme objet réutilisant les fonctions de l'exercice précédent et vous permettant de chiffrer et déchiffrer n'importe quel fichier de votre disque dur dont le nom est passé en paramètre du programme dans la console.