2 février 2015

Programmation structurée (420-PRS-DM)
Louis Marchand
Département d'informatique
Cégep de Drummondville

Travail pratique 2

Ce travail doit être fait individuellement. Il doit être remis avant le lundi 23 février 2015 à 23h59. La remise devra être faite par l'outil de soumission du logiciel Léa. Vous devez placer votre code source python et votre fichier LISEZMOI.txt dans une archive zip et vous ne soumettez que l'archive zip. Votre mandat consiste à programmer une librairie de cryptographie en Python. Veuillez noter que toutes les fonctionnalités de la librairie doivent être entièrement documentées et avoir une suite de test complète. Veuillez également noter que les fonctionnalités devront engendrer le moins de duplication de code possible.

Note : Pour créer ces fonctionnalités, sachez que vous pouvez transformer une chaîne de caractères (str) en liste (list) en utilisant «liste = list(chaine) ». De la même façon, on peut obtenir une chaîne de caractères à partir d'une liste en utilisant « chaine = str(liste) ».

Voici les fonctionnalités que la librairie doit fournir :

Le chiffre de César

Le chiffre de César est une technique de cryptographie par décalage utilisé par Jules César. La technique consiste à décaler chaque caractère d'une chaîne de caractères par un nombre prédéterminé (appelé distance). Par exemple, si on encode la chaîne de caractère "Hello world" avec un décalage de 5, on obtient "Mjqqt btwqi". Vous devez créer deux fonctions :

1. La fonction « creer_encodeur_cesar » prend en argument un entier positif représentant la distance que l'encodeur devra utiliser et retourne une fonction lambda. La fonction lambda retournée prend en argument représentant une chaîne de caractères (str) et retourne une copie de cette chaîne cryptée avec le chiffre de César utilisant la distance envoyée en argument à « creer_encodeur_cesar » plus haut.
2. La fonction « creer_decodeur_cesar » prend en argument un entier positif représentant la distance que le décodeur devra utiliser et retourne une fonction lambda. La fonction lambda retournée prend en argument une chaîne de caractères cryptée et retourne une copie de cette chaîne décryptée avec le chiffre de César utilisant la distance envoyée en argument à « creer_décodeur_cesar » plus haut.

Le ROT13

La technique de cryptographie ROT13 correspond au Chiffre de César en utilisant une distance de 13. La caractéristique principale de cette technique de cryptographie est que l'encodeur et le décodeur sont exactement identique. En d'autres mots, utiliser l'encodeur sur une chaîne de caractères cryptée permettra de la décrypter. Vous devez créer une seule fonction :

1. La fonction « creer_rot13 » ne prenant aucun argument et retournant une fonction lambda. Cette fonction lambda devra être un encodeur/décodeur prenant en argument une chaîne de caractères non cryptée (resp. crypté) et retournant une copie de la chaîne cryptée (resp. décrypté) avec la technique ROT13.

Chiffrement par substitution

La technique de chiffrement par substitution consiste à remplacer systématiquement chaque caractère par un autre caractère. Par exemple, prenons la clé de substitution suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	M	Q	P	A	L	X	N	W	O	S	K	C	B	E	I	D	J	V	R	U	H	F	G	T	Y

En utilisant cette clé de substitution, la chaîne de caractère « Bonjour les amis » deviendra : « Meboeuj kav zcwv ». Pour cette technique, vous devez créer les fonctions suivantes :

1. La fonction « creer_encodeur_substitution » prend en argument une chaîne de caractère de 26 caractères représentant la clé de substitution que l'encodeur devra utiliser et retourne une fonction lambda. La clé de substitution envoyée en argument devra contenir tous les caractères de « A » à « Z ». Le caractère à l'index 0 de la clé représentera la substitution du caractère « A »; le caractère à l'index 1 de la clé représentera la substitution du caractère « B » et ainsi de suite jusqu'à l'index 25 qui représente la substitution de « Z ». Par exemple, dans la clé de substitution présentée dans exemple précédemment, nous aurions la chaîne "zmqpalxnwoskcbeidjvruhfgty". La fonction lambda retournée prend un argument représentant une chaîne de caractères et retourne une copie de cette chaîne cryptée avec le chiffrement par substitution utilisant la clé de substitution envoyée en argument à « creer_encodeur_substitution » plus haut.
2. La fonction « creer_decodeur_substitution » prend en argument une fonction lambda représentant un encodeur de chiffrement par substitution (créer par la fonction « creer_encodeur_substitution » au point 1) et retourne une fonction lambda permettant de décrypter une chaîne de caractères cryptée avec l'encodeur reçu en argument. La fonction lambda retournée prend une chaîne de caractères cryptée en argument et retourne une copie de la chaîne décryptée.

Chiffrer un fichier

Créer la procédure « crypter_fichiers » permettant de crypter ou décrypter le contenu d'un ou plusieurs fichiers textes. Cette procédure prend un minimum de 2 arguments et peut prendre un nombre indéterminé d'arguments. Le premier argument est une fonction lambda qui correspond à l'encodeur ou au décodeur à utiliser. Les arguments suivants sont des chaînes de caractères correspondantes à des chemins vers les fichiers texte à crypter / décrypter. Le contenu de tous les fichiers spécifiés doit être crypté / décrypté en utilisant l'encodeur / décodeur passé en premier argument. À noter que le contenu

original des fichiers sera remplacé par le contenue crypté / décrypté.