Informatique en CPGE (2017-2018)
TD 7 : codage

1 Chiffrement de César

C'est un chiffrement par décalage.

Le texte chiffré s'obtient en remplaçant chaque lettre du texte original par une lettre à distance fixe, toujours du même côté, dans l'ordre de l'alphabet.

Exercice 1

Utilisation de l'alphabet

Soit **n** un entier vérifiant $\mathbf{n} \leq 26$. On souhaite écrire un programme qui code un mot en décalant chaque lettre de l'alphabet de **n** lettres.

Par exemple pour $\mathbf{n} = 3$, le décalage sera le suivant :

avant décalage	a	b	c	d	...	...	x	y	z
après décalage	d	e	f	g	...	...	a	b	c

Le mot **oralensam** devient ainsi **rudohqvdp**.

1. Définir une chaîne de caractères contenant toutes les lettres dans l'ordre alphabétique (caractères en minuscule).
2. Ecrire une fonction **decalage**, d'argument un entier **n**, renvoyant une chaîne de caractères contenant toutes les lettres dans l'ordre alphabétique, décalées de **n**, comme indiqué ci-dessus.
3. Ecrire une fonction **indices**, d'arguments un caractère **x** et une chaîne de caractères **phrase**, renvoyant une liste contenant les indices de **x** dans **phrase** si **x** est une lettre de phrase et une liste vide sinon.
4. Ecrire une fonction **codage** d'arguments un entier **n** et une chaîne de caractères **phrase**, renvoyant **phrase** codé avec un décalage de **n** lettres.
5. Comment peut-on décoder un mot codé si on connaît le décalage ? Et si on ne le connaît pas ?

Note : en français les lettres les plus fréquentes dans un texte sont dans l'ordre "e", "s", "u" ; en anglais ce sont "e", "t", "a".

Exercice 2

Utilisation de la table ASCII comme alphabet

Pour représenter un caractère dans la machine, on attribue un nombre à chaque caractère par exemple à l'aide du code ASCII binaire (American Standard Code for Information Interchange). Ce code utilise un octet par caractère, avec le premier bit toujours égal à 0, et permet donc de représenter $2^7 = 128$ caractères. Ce sont les caractères que l'on trouve sur les touches d'un clavier "qwerty" d'ordinateur : par exemple, on attribue les nombres de "97" à "122" aux 26 lettres de l'alphabet a, b, c, ..., z ; les nombres de "48" à "57" aux neuf chiffres 0, 1, 2, ..., 9 ; l'espace est codé par le nombre "32", le point par le nombre "46", etc. (voir une table complète sur le site www.table-ascii.com)

Attention à ne pas confondre un chiffre avec le caractère qui le représente. Les caractères du pavé numérique 0, 1, 2, 3, ... sont codés en ASCII par les nombres 48, 49, 50, 51, ...

L'instruction `chr(97)` permet d'afficher 'a' et l'instruction `ord('a')` permet d'afficher 97.

Décoder la suite de nombres : 98 114 97 118 111

2 Chiffrement affine

Exercice 3

1. A chaque lettre de l'alphabet, on associe, grâce au tableau ci-dessous, un nombre entier compris entre 0 et 25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On définit un procédé de codage de la façon suivante :

Etape 1 : A la lettre que l'on veut coder, on associe le nombre m correspondant dans le tableau.

Etape 2 : On calcule le reste de la division euclidienne de $9m + 5$ par 26 et on le note p.

Etape 3 : Au nombre p, on associe la lettre correspondante dans le tableau.

(a) Coder la lettre U.

(b) Ecrire une fonction qui prend en argument un nombre m entier naturel, et renvoie le nombre p, calculé à l'aide du procédé de codage précédent.

2. (a) Trouver un nombre entier x tel que $9x \equiv 1 \quad [26]$.

(b) Démontrer alors l'équivalence :

$$9m + 5 \equiv p \quad [26] \iff m \equiv 3p - 15 \quad [26].$$

(c) Décoder alors la lettre B.

3. Ecrire un programme permettant de coder un message entré par l'utilisateur, puis de le décoder. On pourra utiliser le code ASCII ou pas.

3 Chiffrement de Vigenère

Pour le chiffrement de César, on utilise une clé unique pour coder toutes les lettres du message en procédant à un décalage (le même pour chaque lettre). Ici, nous procédons toujours par décalage mais nous allons utiliser une "phrase clé" dont chaque lettre va servir de clé : la première lettre du message sera codée à l'aide de la première lettre de la phrase clé, la deuxième lettre du message sera codée à l'aide de la deuxième lettre de la phrase clé, et ainsi de suite. On pourra parcourir plusieurs fois la phrase clé si elle est plus courte que le message.

Exercice 4

1. Définir le texte à coder et la phrase clé, par exemple :
   texte="Hello my friend, you are going to decode my message"
   phrase_cle="Attention, le texte est en anglais !"
2. Ecrire une fonction qui prend en argument deux chaînes de caractères, le texte à coder et la phrase clé, et renvoie le texte codé. Pour chaque lettre du texte, la clé sera donnée par la fonction **ord** appliquée à chaque lettre de la phrase clé.