TP 10

Exercice 1. chiffrement de César

Les lettres de l'alphabet sont représentées par des entiers de 0 à 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

Le codage de César consiste à décaler les lettres d'un texte d'une une plusieurs positions, ce traitement étant appliqué à toutes les lettres de ce texte.
Exemple :
ecole devient, en prenant c=3 hfroh.
Une chaine de caractère sera présentée sans espace, en lettres minuscules et sans ponctuation.
Exemple : 'lyceeschweitzer'
1) Ecrire une fonction **codecesar(texte,d)** codant un texte avec cette méthode à l'aide d'un décalage (clé) d.
Utiliser **ord(x)**qui donne le code ASCII de la lettre **x**, avec
$\text{ord}('a') = 97$, $\text{ord}('b') = 98$, $\cdots$, $\text{ord}('z') = 122$
et la fonction réciproque **chr(i)** qui renvoie le caractère associé à l'entier i. chr(97) ='a', $\cdots$, chr(122) ='z'.

2) Ecrire une fonction **decodecesar(tc,d)** qui permet de retrouver le texte d'origine à partir du texte chiffré tc à l'aide de la clé d.

Exercice 2

a) Lorsqu'on dispose d'un texte codé par cette méthode mais dont la clé est inconnue, une manière de déterminer cette clé est d'étudier la fréquence d'apparition de chaque lettre dans le texte chiffré. La lettre la plus fréquente dans un texte suffisamment long, en Français étant la lettre e.
Ecrire la fonction **def frequences(t) :** qui prend en argument un texte t et qui renvoie une liste de longueur 26 représentant le nombre d'apparitions de chaque lettre.

b) Ecrire une fonction **def decoauto(tc)** qui décode le texte chiffré tc après avoir déterminé la clé d par la méthode des fréquences.

Exercice 3 : Codage de Vigenère

Le codage de Vigenère est une amélioration du codage précédent. La clé est un texte, exemple 'concours', pour coder un texte on décale la première lettre de 2 (représentation de c), la deuxième de 14 et ainsi de suite, lorsqu'on atteint le 's' de concours on recommence au départ, c'est à dire décalage de 2.

Exemple : Codage de 'lyceeschweitzer' avec la cle concours : 'nmpgsmtzysvvnyi'.

a) Ecrire une fonction **def codevigenere(t,c) :** qui prend un argument un texte t et une chaine de caractère c, qui est la clé et qui code ce texte à l'aide de cette clé.

b) Ecrire une fonction **def decodevigenere(tc,c) :** qui prend un argument un textechiffré tc à partir d'une clé chaine de caractère c, et qui décode ce texte.

Exercice 4 : Chiffrement RSA

Le principe du chiffrement RSA est le suivant/ On choisit deux grands nombres premiers (environs 100 chiffres) p et q, $n = p * q$ et deux entiers e, qui est la clé publique, connue de tous et d qui est la clé privée connue de la personne qui déchiffrera le message, tels que $ed = 1 \mod (p-1)(q-1)$.
Le message M est chiffré sous la forme $C = M^e \mod n$ et C est déchiffré par $D = C^d \mod n$.

Exemple : chiffrer BONJOUR
1) Alice crée ses clés :

La clé secrète : p = 53 , q = 97 (Note : en réalité, p et q devraient comporter plus de 100 chiffres !) La clé publique : e = 7 (premier avec 52*96), n = 53*97 = 5141

2) Alice diffuse sa clé publique (par exemple, dans un annuaire).

3) Bob ayant trouvé le couple (n,e), il sait qu'il doit l'utiliser pour chiffrer son message. Il va tout d'abord remplacer chaque lettre du mot BONJOUR par le nombre correspondant à sa position dans l'alphabet : B = 2, O = 15, N = 14, J = 10, U = 21, R = 18

BONJOUR = 2 15 14 10 15 21 18

4) Ensuite, Bob découpe son message chiffré en blocs de même longueur représentant chacun un nombre plus petit que n. Cette opération est essentielle, car si on ne faisait pas des blocs assez longs (par exemple, si on laissait des blocs de 2 chiffres), on retomberait sur un simple chiffre de substitution que l'on pourrait attaquer par l'analyse des fréquences (Voir chiffre de César).

BONJOUR = 002 151 410 152 118

5) Bob chiffre chacun des blocs que l'on note B par la transformation C = Bemod n (où C est le bloc chiffré) :

C1 = 27mod 5141 = 128 C2 = 1517mod 5141 = 800 C3 = 4107mod 5141 = 3761 C4 = 1527mod 5141 = 660 C5 = 1187mod 5141 = 204

On obtient donc le message chiffré C : 128 800 3761 660 204.

a) Ecrire une fonction **def numer(t)** qui transforme une chaine de caractères en liste de trois chiffres comme ci-dessus lespaquets de trois chiffres étant considérés comme des chaines de caractères..

b) Ecrire une fonction **def codersa(t,n,e)** qui code chacun des éléments de la liste comme indiqué ci-dessus et qui crée une nouvelle liste d'entiers.

c) Ecrire une fonction **def decodersa(t,n,d)** qui décode la liste chiffrée obtenue ci dessus. et redonne la liste de a) constituée d'entiers cette fois.

d) Ecrire une fonction **def chaine(L)** qui reconstitue le message t d'origine en utilisant la liste de la question c).