Banque « Agro- Veto »
AT - 0517

Algorithmique et Informatique
Durée : 45 mn

Si au cours de l'épreuve, un candidat repère ce qui lui semble être une erreur d'énoncé, il le signale sur sa copie et poursuit sa composition en expliquant les raisons des initiatives qu'il a été amené à prendre.
L'usage d'une calculatrice est interdit pour cette épreuve.

- On rappelle que l'opération de concaténation de deux chaines de caractères `ch1` et `ch2` s'écrit `ch1 + ch2`.

  Ainsi `"MESSAGE" + "SECRET"` *est la chaine de caractères* `"MESSAGESECRET"`.

- On rappelle que la syntaxe `a % b` (lue `a` modulo `b`) renvoie le reste de la division euclidienne de l'entier `a` par l'entier (non nul) `b`.

  Ainsi l'entier `(12 + 18) % 26` *a pour valeur* `4`.

- Dans tout le sujet, on pourra utiliser une fonction `car_to_int` renvoyant un entier égal au rang (à partir de zéro) d'un caractère de l'alphabet passé en argument (écrit en majuscule et sans accent).

  La fonction `car_to_int` *est entièrement définie par l'ensemble de ses valeurs :* `car_to_int("A")= 0`, `car_to_int("B")= 1`, ..., `car_to_int("Y")= 24`, `car_to_int("Z")= 25`.

- On utilisera aussi sa réciproque notée `int_to_car`.

  La fonction `int_to_car` *est entièrement définie par l'ensemble de ses valeurs :* `int_to_car(0)= "A"`, `int_to_car(1)= "B"`, ..., `int_to_car(24)= "Y"`, `int_to_car(25)= "Z"`.

1 Questions préliminaires

a. Quelle est le type de `int_to_car(21)` ? Quelle est sa valeur ?

b. Quelle est le type de `car_to_int("F")` ? Quelle est sa valeur ?

2 Chiffrement de Vigenère

Le chiffrement de Vigenère est une méthode cryptographique qui consiste à coder une chaine de caractères (appelée *texte clair*) en une autre (appelée *texte chiffré*) à partir d'une clé, connue seulement de l'expéditeur et du destinataire du message.
Pour cela, on choisit une chaine de caractères (de longueur m inférieure à celle du texte à chiffrer) qui fera office de clé, qu'on "applique" successivement à des blocs de longueur m du message à chiffrer.
Dans toute la suite, on supposera que la longueur du texte à chiffrer est un multiple de la longueur de la clé.
On illustre par l'exemple ci-dessous les étapes du chiffrement de Vigenère.
On choisit de chiffrer la chaine de caractères `"MESSAGECODEPOURBOB"` *- appelée* ***texte clair*** *- avec la clé* `"SECRET"`.

- *On construit une chaine de caractères de la longueur du texte clair en concaténant autant de fois que nécessaire la clé* `"SECRET"`.

  Puisque dans cet exemple le texte chiffré est de longueur 18 et que la clé est de longueur 6, on répète trois fois la clé, de manière à construire la chaine de caractères `"SECRETSECRETSECRET"`.

- *on convertit les chaines de caractères - le texte à chiffrer - ainsi que la clé dupliquée en deux listes d'entiers via la correspondance bijective entre caractères et entiers décrite au début du sujet.*

  On obtient alors la liste `[12, 4, 18, 18, 0, 6, 4, 2, 14, 3, 4, 15, 14, 20, 17, 1, 14, 1]` *et la liste* `[18, 4, 2, 17, 4, 19, 18, 4, 2, 17, 4, 19, 18, 4, 2, 17, 4, 19]`.

- *Les deux listes ayant la même longueur, on somme terme-à-terme* ***modulo 26*** *les entiers de ces listes. On obtient alors une troisième liste d'entiers (compris entre 0 et 25).*

- *On convertit cette liste en une chaine de caractères via la correspondance entre entiers et caractères. La chaine ainsi construite est appelée* ***texte chiffré*** *; c'est cette chaine qui constitue le message qui sera envoyé.*

Les opérations présentées dans l'exemple sont illustrées dans l'exemple ci-après.

texte clair	*"M*	*E*	*S*	*S*	*A*	*G*	*E*	*C*	*O*	*D*	*E*	*P*	*O*	*U*	*R*	*B*	*O*	*B"*
	[12,	*4,*	*18,*	*18,*	*0,*	*6,*	*4,*	*2,*	*14,*	*3,*	*4,*	*15,*	*14,*	*20,*	*17,*	*1,*	*14,*	*1]*
clé dupliquée	*"S*	*E*	*C*	*R*	*E*	*T*	*S*	*E*	*C*	*R*	*E*	*T*	*S*	*E*	*C*	*R*	*E*	*T"*
	[18,	*4,*	*2,*	*17,*	*4,*	*19*	*18,*	*4,*	*2,*	*17,*	*4,*	*19*	*18,*	*4,*	*2,*	*17,*	*4,*	*19]*
	[4,	*8,*	*20,*	*9,*	*4,*	*25,*	*22,*	*6,*	*16,*	*20,*	*8,*	*8,*	*6,*	*24,*	*19,*	*18,*	*18,*	*20]*
texte chiffré	*"E*	*I*	*U*	*J*	*E*	*Z*	*W*	*G*	*Q*	*U*	*I*	*I*	*G*	*Y*	*T*	*S*	*S*	*U"*

a. On considère la fonction `mult` suivante.

```
def mult(chaine, n):
    chaine2 = ""
    for k in range(n):
        chaine2 += chaine
    return chaine
```

(i) Que renvoie `mult("SECRET", 3)` ?

(ii) Que fait la fonction `mult` ?

b. Modifier le code de la fonction ci-dessous de manière à ce qu'elle renvoie la liste des entiers correspondant - via la correspondance entre caractères et entiers présentée au début du sujet - aux caractères (écrits en majuscule sans accent) de la chaine de caractères passée en argument.

Exemple : `str_to_listofint("POURBOB")` *devra renvoyer la liste* `[15, 14, 20, 17, 1, 14, 1]`.

```
def str_to_listofint(chaine):
    liste = []
    for k in (0, len(chaine)):
        liste = liste + car_to_int(chaine[k])
    return liste
```

c. Parmi les fonctions suivantes, déterminer l'unique fonction `somme` qui renvoie une liste d'entiers construite comme la somme terme-à-terme modulo 26 de deux listes de même longueur.

Exemple : `somme([12, 4, 18, 18], [18, 4, 2, 17])` *devra renvoyer la liste* `[4, 8, 20, 9]`.

```
def somme1(liste1, liste2):
    return (liste1 + liste2) % 26
```

```
def somme2(liste1, liste2):
    liste = []
    for i in range(len(liste1)):
        for j in range(len(liste2)):
            s = liste1[i] + liste2[j]
            liste.append(s)
     return liste
```

```
def somme3(liste1, liste2):
    liste = []
    for k in range(len(liste1)):
        s = liste1[k] + liste2[k]
        liste.append(s%26)
    return liste
```

```
def somme4(liste1, liste2):
    liste = []
    for k in range(len(liste2)):
        s = (liste1[k] + liste2[k])%26
    liste.append(s)
    return liste
```

d. Parmi les fonctions suivantes, déterminer l'unique fonction `listofint_to_str`, réciproque de la fonction `str_to_listofint`, i.e. renvoyant une chaine de caractères correspondant aux éléments d'une liste d'entiers (compris entre 0 et 25) passée en argument.

Exemple : `listofint_to_str([4, 8, 20, 9, 4, 25])` *devra renvoyer la chaine de caractères* `"EIUJEZ"`.

```python
def listofint_to_str1(liste):
    chaine = ""
    for nb in liste:
        chaine += int_to_car(nb)
    return chaine
```

```python
def listofint_to_str2(liste):
    return int_to_car(liste)
```

```python
def listofint_to_str3(liste):
    s = 0
    for k in range(len(liste)):
        s = liste[k]
    return int_to_car(s%26)
```

```python
def listofint_to_str4(liste):
    chaine = ""
    for nb in liste:
        chaine = int_to_car(nb)
    return chaine
```

e. Parmi les fonctions précédentes, déterminer l'unique fonction `chiffreVigenere` qui, à partir de deux chaines de caractères `txt_clair` et `cle` passées en argument, renvoie le texte chiffré (une chaine de caractères) obtenu par le chiffrement de Vigenère.

Exemple : l'instruction `chiffreVigenere("MESSAGECODEPOURBOB", "SECRET")` *devra renvoyer la chaine de caractères* `"EIUJEZWGQUIIGYTSSU"`.

```python
def chiffreVigenere1(txt_clair,cle):
    n_txt = len(txt_clair)
    n_cle = len(cle)
    clair_int = str_to_listofint(txt_clair)
    cle_multi = mult(n_cle)
    cle_int = str_to_listofint(cle_multi)
    chiffre_int = somme(clair_int, cle_int)
    return listofint_to_str(chiffre_int)
```

```python
def chiffreVigenere2(txt_clair,cle):
    n_txt = len(txt_clair)
    n_cle = len(cle)
    clair_int = str_to_listofint(txt_clair)
    cle_multi = mult(cle, n_txt)
    cle_int = str_to_listofint(cle_multi)
    chiffre_int = somme(clair_int, cle_int)
    return listofint_to_str(chiffre_int)
```

```python
def chiffreVigenere3(txt_clair,cle):
    n_txt = len(txt_clair)
    n_cle = len(cle)
    clair_int = str_to_listofint(txt_clair)
    cle_multi = mult(cle, n_txt//n_cle)
    cle_int = str_to_listofint(cle_multi)
    chiffre_int = somme(clair_int, cle_int)
    return listofint_to_str(chiffre_int)
```

```python
def chiffreVigenere4(txt_clair,cle):
    n_txt = len(txt_clair)
    n_cle = len(cle)
    clair_int = str_to_listofint(txt_clair)
    cle_int = str_to_listofint(cle)
    chiffre_int = somme(clair_int, cle_int)
    return listofint_to_str(chiffre_int)
```

3 Déchiffrement

Pour déchiffrer un texte chiffré - ce qui se fait toujours en connaissant la clé, sinon on parle de cryptanalyse - on reprend les étapes précédentes dans l'ordre inverse.

1. Écrire une fonction `difference` qui renvoie une liste d'entiers construite comme la différence terme-à-terme modulo 26 de deux listes de même longueur. On "soustraira" la seconde liste à la première.

   Ainsi, `difference([4, 8, 20, 9], [18, 4, 2, 17])` *est la liste* `[12, 4, 18, 18]`.

2. Écrire une fonction `dechiffreVigenere` qui, à partir de deux chaines de caractères `txt_chiffre` et `cle`, renvoie la chaine de caractères correspondant au texte clair.

   Exemple : l'instruction `dechiffreVigenere("EIUJEZWGQUIIGYTSSU", "SECRET")` *devra renvoyer la chaine de caractères* `"MESSAGECODEPOURBOB"`.

4 Cryptanalyse par analyse fréquentielle

Rappels :

- La syntaxe `ch[k:]` désigne la chaine de caractères `ch` tronquée de ses `k` premiers caractères,

  Ainsi, si `ch` *désigne la chaine* `"SECRET"`, `ch[2:]` *est la chaine* `"CRET"`.

- Si `ch` désigne une chaine de caractères, `ch[i::d]` désigne la chaine de caractères construite en extrayant les caractères de `ch` d'indices `i, i+d, i+2d, i + 3d`, etc...

  Ainsi, si `ch` *désigne la chaine de caractères* `"EPREUVEINFORMATIQUE"`, `ch[1::2]` *est la chaine de caractères* `"PEVIFRAIU"`.

La cryptanalyse du chiffrement de Vigenère a lieu en deux étapes : la détermination de la longueur de la clé puis de la clé elle-même, à l'aide d'outils statistiques (inhérents à la langue dans laquelle est écrit le texte).
Dans toute la suite, on désigne par `ch` le texte chiffré à décrypter.

a. On appelle **indice de coïncidence** de deux chaines de caractères `ch1` et `ch2` la fréquence des indices des chaines où les caractères sont identiques, i.e. le rapport du nombre d'entiers k vérifiant `ch1[k] = ch2[k]` par le minimum des longueurs des deux chaines.

Exemple : l'indice de coïncidence des chaines "ABRACADABRA" et "SHAZAAAM" est $\frac{1}{8}$. *En effet, ces chaines ne partagent qu'un seul caractère commun situé au même indice (*`"A"` *à l'indice 5). Les trois derniers caractères (*`"BRA"`*) de la chaine* `"ABRACADABRA"` *sont ignorés.*

Parmi les quatre fonctions ci-dessous, indiquer (sans justification) l'unique fonction renvoyant l'indice de coïncidence de deux chaines de caractères.

```
def indice_coincidence1(ch1, ch2):
    m = len(ch1)
    compteur = 0
    for k in range(m+1):
        if ch1[k] in ch2:
            compteur += 1
    return compteur/m
```

```
def indice_coincidence2(ch1, ch2):
    m = min(len(ch1), len(ch2))
    compteur = 1
    for k in range(m):
        if ch1[k] == ch2[k]:
            compteur += 1
    return compteur
```

```
def indice_coincidence3(ch1, ch2):
    compteur = 0
    n1, n2 = len(ch1), len(ch2)
    j = 0
    while j < n1 or j < n2:
        if ch1[j] == ch2[j]:
            compteur = compteur + 1
        j = j + 1
    return compteur
```

```
def indice_coincidence4(ch1, ch2):
    compteur = 0
    n1, n2 = len(ch1), len(ch2)
    j = 0
    while j < n1 and j < n2:
        if ch1[j] == ch2[j]:
            compteur = compteur + 1
        j += 1
    return compteur/j
```

b. On peut prouver que l'indice de coïncidence de deux chaines de caractères aléatoires est égal à $\frac{1}{26} \approx 0,03846$. Pour des chaines de caractères écrites dans une langue dite *naturelle*, l'indice de coïncidence est plus élevé (la distribution des lettres n'est pas uniforme). En français par exemple, il est supérieur à 0,07. Ainsi, si `ch` désigne une chaine de caractères écrite en français et `k` un entier naturel, l'indice de coïncidence de `ch` et `ch[k:]` est (statistiquement) supérieur à 0,07.

Pour déterminer la longueur de la clé, on utilise le **test de Friedman** : si `ch` désigne une chaine codée par le chiffrement de Vigenère, on calcule successivement les indices de coïncidence entre `ch` et les chaines `ch[k:]` où `k` varie dans l'ensemble des indices **non nuls** de la chaine `ch`.

La propriété sur l'indice de coïncidence de `ch` et `ch[d:]` nous assure que cet indice dépasse 0,07 lorsque `d` est égal à la longueur de la clé (ou un multiple), et reste proche de $\frac{1}{26}$ dans le cas contraire.

Écrire une fonction `test_Friedman` qui prend en argument une chaine de caractères `ch` codée selon le chiffrement de Vigenère et qui renvoie le plus petit entier `d` ≥ 1 tel que l'indice de coïncidence de `ch` et `ch[d:]` dépasse 0.07, i.e. la longueur (probable) de la clé de chiffrement (on supposera qu'un tel indice existera toujours).

c. Modifier le code de la fonction ci-dessous pour qu'elle renvoie le caractère le plus fréquent - qu'on supposera unique - dans une chaine de caractères entrée en argument.

On pourra utiliser la méthode `count` *sur le type* `str` *de la manière suivante :* `ch.count(car)` *est le nombre de fois où le caractère* `car` *apparait dans la chaine* `ch`*. Ainsi, si* `ch` *désigne la chaine* `"SECRET"`*, l'entier* `ch.count("E")` *a pour valeur 2.*

```
def lettre_plus_freq(ch):
    nb_max = 0
    for k in range(26):
        car = car_to_int(k)
        nb = ch.count(car)
    return nb_max
```

d. Une fois la longueur de la clé connue, une simple analyse statistique suffit : en français, la lettre la plus courante est le "E". Ainsi, en notant `d` la longueur de la clé (calculée par la fonction `test_Friedman`), le caractère le plus fréquent de chacune des chaines extraites `ch[0::d], ch[1::d], ch[2::d], ..., ch[d-1::d]` correspond (statistiquement) à un "E" dans le texte clair (en supposant que le texte chiffré est suffisamment long). Chaque caractère de la clé se déduit par différence.

Modifier le code de la fonction `determine_cle` ci-dessous pour qu'elle renvoie la clé de chiffrement d'un texte passé en argument et chiffré par la méthode de Vigenère.

```
def determine_cle(txt_chiffre):
    d = test_Friedman(txt_chiffre)
    car_chiffre = lettre_plus_freq(txt_chiffre[0::d])
    car_cle = difference(car_chiffre, "E")
    return car_cle
```

e. En déduire une fonction `cryptanalyse_Vigenere` qui décrypte un texte chiffré selon la méthode de Vigenère.

⋆⋆⋆ FIN ⋆⋆⋆