

Autotest n°4 – correction

EXERCICE 1 : Faire les exercices d’entraînement du site d’activités (thème 7).

EXERCICE 2 : Afin de s’envoyer des messages en secret, deux amies ont inventé la méthode suivante. Elles ont choisi 30 symboles composés des lettres en majuscule et de quelques symboles de ponctuation, comme les espaces représentés par la case vide. Ces symboles sont placés dans un tableau de 5 lignes et de 6 colonnes. La lettre A se trouve dans une case choisie initialement et les autres symboles sont écrits, dans l’ordre, de gauche à droite et de haut en bas. Une fois arrivé en bas à droite du tableau, on repart en haut à gauche.

	0	1	2	3	4	5
0	A	B	C	D	E	F
1	G	H	I	J	K	L
2	M	N	O	P	Q	R
3	S	T	U	V	W	X
4	Y	Z		.	,	'

Table 1

	0	1	2	3	4	5
0	W	X	Y	Z		.
1	,	'	A	B	C	D
2	E	F	G	H	I	J
3	K	L	M	N	O	P
4	Q	R	S	T	U	V

Table 2

	0	1	2	3	4	5
0	B	C	D	E	F	G
1	H	I	J	K	L	M
2	N	O	P	Q	R	S
3	T	U	V	W	X	Y
4	Z		.	,	'	A

Table 3

	0	1	2	3	4	5
0	R	S	T	U	V	W
1	X	Y	Z		.	,
2	'	A	B	C	D	E
3	F	G	H	I	J	K
4	L	M	N	O	P	Q

Table 4

Pour chiffrer un message, on part d’une case choisie au hasard et ensuite, on indique la suite de déplacements pour aller sur le premier symbole du message, puis le deuxième et ainsi de suite. Les deux amies connaissent toutes les deux la case sur laquelle se trouve la lettre A, pour refaire le tableau, et elles s’envoient pour chaque message les coordonnées de la case de départ et la liste des déplacements à faire.

Les coordonnées sont des couples de la forme (ligne, colonne) et les vecteurs sont de la forme (déplacement vertical, déplacement horizontal). De plus, les déplacements sont toujours positifs. Lors d’un déplacement vertical, si on arrive en bas du tableau, on repart en haut, dans la même colonne et si lors d’un déplacement horizontal on arrive au bord droit, on repart à gauche, sur la même ligne. C’est comme si on dupliquait le tableau à droite et en bas autant de fois que nécessaire.

Dans la table ci-contre, on voit le chemin parcouru pour chiffrer le mot “NSI”. Le “A” se trouve en (3, 2). C’est le générateur de la table. La case choisie pour commencer est (3, 3). Il faut descendre de 2 pour aller sur “N”, puis descendre de 1 et aller à droite 5 fois pour arriver sur “S”. Enfin on descend de 3 puis on va à droite 2 fois à droite pour arriver sur “I”. Le code secret est donc composé de (3, 3) et de la liste de vecteurs [(2, 0), (1, 5), (3, 2)].

	0	1	2	3	4	5
0	K	L	M	N	O	P
1	Q	R	S	T	U	V
2	W	X	Y	Z		.
3	,	'	A	X	C	D
4	E	F	G	H	I	J

Une autre façon de représenter les déplacements, c’est de dupliquer la table en bas ou à droite autant de fois que nécessaire. Voici le résultat en partant de (3, 3) et en faisant les déplacements [(2, 0), (1, 5), (3, 2)].

	0	1	2	3	4	5
0	K	L	M	N	O	P
1	Q	R	S	T	U	V
2	W	X	Y	Z		.
3	,	'	A	X	C	D
4	E	F	G	H	I	J
	K	L	M	N	O	P
	Q	R	S	T	U	V
	W	X	Y	Z		.
	,	'	A	B	C	D
	E	F	G	H	I	J

- 1) Quelles sont les coordonnées de “B” dans la table 2 ci-dessus? **Solution :** (1, 3)
- 2) Quel est le symbole se trouvant en (2, 4) dans la table 3? **Solution :** “R”
- 3) Laquelle des 4 tables ci-dessus correspond au générateur (2, 1)? **Solution :** Table 4

4) Pour les questions suivantes, on considère la table-ci-contre.

- Quel est le générateur de cette table? **Solution : (3, 4)**
- Déchiffrer à l'aide de la table le message défini par (2, 1) et [(1,4), (3,4), (2,1), (4,3), (4,5)]. **Solution : BRAVO**
- Donner la liste de vecteurs correspondant au chiffrement de "CHAT" en partant de (1, 0).

	0	1	2	3	4	5
0	I	J	K	L	M	N
1	O	P	Q	R	S	T
2	U	V	W	X	Y	Z
3		.	,	'	A	B
4	C	D	E	F	G	H

Table 5

Solution : [(3, 0), (0, 5), (4, 5), (3, 1)]

La fonction `creation_table` prend en paramètres deux entiers `i` et `j`, et renvoie le tableau à deux dimensions correspondant à la table où la lettre A se trouve en (`i`, `j`).

```
ALPHABET = "ABCDEFGHIJKLMNOPQRSTUVWXYZ .,"
def creation_table(i, j):
    # On fait un tableau vide
    table = [ [""] for j2 in range(6)] for i2 in range(5) ]
    # On place chaque symbole
    for symbole in ALPHABET:
        table[i][j] = symbole
        j = j + 1 # On avance d'une colonne
        if j >= 6: # On va à la ligne si on arrive à droite
            j = 0
            i = (i + 1) % 5
    return table
```

```
>>> creation_table(3, 2)
[['K', 'L', 'M', 'N', 'O', 'P'], ['Q', 'R', 'S', 'T', 'U', 'V'], ['W', 'X', 'Y', 'Z', ' ', '.'],
['.', ' ', 'A', 'B', 'C', 'D'], ['E', 'F', 'G', 'H', 'I', 'J']]
```

5) Compléter le code de la fonction `creation_table`.

La fonction `trouver` prend en paramètre un tableau à 2 dimensions `table` et un texte à un seul caractère `symbole`, et renvoie les coordonnées de `symbole` dans `table`. S'il n'y est pas, elle renvoie (0, 0).

```
def trouver(table, symbole):
    for i in range(5):
        for j in range(6):
            if table[i][j] == symbole:
                return (i, j)
    return (0, 0)
```

```
>>> table = creation_table(3, 2)
>>> trouver(table, 'T')
(1, 3)
```

6) Compléter le code de la fonction `trouver`.

Le tableau ci-dessous représente le reste de la division euclidienne de `x` par 5, notée en Python `x % 5`. Ce nombre est toujours compris entre 0 et 4. On peut remarquer que la suite de valeurs allant de 0 à 4 se répète plusieurs fois, toujours dans le même ordre.

<code>x</code>	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
<code>x % 5</code>	4	0	1	2	3	4	0	1	2	3	4	0	1	2

On peut remarquer aussi que lorsque les valeurs sont négatives, on peut obtenir le résultat de $x\%5$ en rajoutant une ou plusieurs fois le nombre 5 jusqu'à arriver à une valeur entre 0 et 4. Par exemple $-3 + 5 = 2$, donc $-3\%5 = 2$. De même, $-6 + 2 \times 5 = 4$, donc $-6\%5 = 4$. Pour les valeurs supérieures à 5, il suffit de retirer autant de fois 5 que nécessaire. $7 - 5 = 2$, donc $7\%5 = 2$.

7) Compléter le tableau correspondant à modulo 6.

x	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
$x \% 6$	0	1	2	3	4	5	0	1	2	3	4	5	0	1

8) En utilisant des opérations modulo 5 ou 6, on peut transformer les déplacements avec des coordonnées négatives en coordonnées positives. Par exemple dans la table ci-contre, en partant de (3, 3) on peut aller en (1, 1) en faisant un déplacement de (-2, -2) ou de (3, 4). En effet, on a $-2\%5 = 3$ et $-2\%6 = 4$.

	0	1	2	3	4	5
0	K	L	M	N	O	P
1	←	Ⓜ	→	↑	↓	↻
2	W	X	Y	Z	.	
3	,	'	A	⊗	C	D
4	E	F	G	H	I	J

Pour chacun des déplacements ci-dessous, indiquer le vecteur à coordonnées positives correspondant :

- a) (-1, 3) équivaut à (4, 3)
- b) (2, -3) équivaut à (2, 3)
- c) (-3, -1) équivaut à (2, 5)

La fonction `ecart` prend en paramètres 4 entiers i_1, j_1, i_2 et j_2 , et renvoie les plus petites coordonnées positives d'un vecteur permettant d'aller de (i_1, j_1) à (i_2, j_2) .

```
def ecart(i1, j1, i2, j2):
    d_i = (i2-i1) % 5
    d_j = (j2-j1) % 6
    return (d_i, d_j)
```

```
>>> ecart(2, 1, 3, 4)
(1, 3)
>>> ecart(3, 4, 2, 1)
(4, 3)
```

9) Compléter le code de la fonction `ecart`.

La fonction `chiffrer` prend en paramètres un tableau à 2 dimensions `table`, deux entiers i_0 et j_0 et un texte `message`, et renvoie la liste des déplacements nécessaires pour chiffrer `message` en partant de (i_0, j_0) en utilisant la table `table`.

```
def chiffrer(table, i0, j0, message):
    vecteurs = []
    for symbole in message:
        # On cherche la position du symbole
        i, j = trouver(table, symbole)
        d_i, d_j = ecart(i0, j0, i, j) # On calcule le déplacement
        vecteurs.append((d_i, d_j)) # On stocke le déplacement
        i0, j0 = i, j # On met à jour la position
    return vecteurs
```

```
>>> table = creation_table(3, 2)
>>> chiffrer(table, 3, 3, "NSI")
[(2, 0), (1, 5), (3, 2)]
```

10) Compléter le code de la fonction `chiffrer`.

La fonction `dechiffrer` prend en paramètres un tableau de dimension 2 `table`, 2 entiers i et j et une liste de couples d'entiers `vecteurs`, et renvoie le message obtenu en partant de (i, j) dans `table` et en suivant les déplacements contenus dans `vecteurs`.

```
>>> table = creation_table(3, 2)
>>> dechiffrer(table, 3, 3, [(2, 0), (1, 5), (3, 2)])
'NST'
```

```
def dechiffrer(table, i, j, vecteurs):
    message = ""
    for d_i, d_j in vecteurs:
        # On se déplace selon les coordonnées du vecteur
        i = (i + d_i) % 5
        j = (j + d_j) % 6
        # On rajoute le symbole au texte
        message += table[i][j]
    return message
```

11) Compléter la fonction dechiffrer.

Un professeur intercepte un papier contenant deux messages venant de chacune des amies. Elles utilisent la même table, qui n'est pas sur le papier. Les deux messages sont :

- (1, 2) et [(2, 1), (2, 1), (0, 5), (4, 2), (1, 5), (1, 0), (0, 3), (1, 4)]
- (3, 1) et [(0, 2), (2, 1), (0, 5), (4, 2), (1, 5), (1, 0), (0, 3), (1, 4)]

12) Expliquer pourquoi la première lettre est la même dans les deux messages.

Solution : Après le premier déplacement, on arrive en (3, 3) dans les deux cas.

13) Expliquer pourquoi les deux messages sont identiques.

Solution : La première lettre est la même et tous les déplacements suivants sont identiques.

14) Quel serait le premier déplacement si on chiffrait le même message mais en partant de (0, 0)? **Solution :** Il faut de déplacer selon (3, 3).

Une des deux amies veut envoyer le message "ON A EU CHAUD." à sa camarade, mais cette dernière lit (1, 3) pour le point de départ au lieu de (1, 2). Elle obtient le message : "PO.B.FV.DIBV,W".

15) On remarque que tous les "A" du message initial deviennent des "B", le "C" devient un "D" et le "E" devient un "F". Cela ressemble au chiffrement de César où chaque lettre est décalée dans l'alphabet. Donner un exemple de lettre du message qui ne respecte pas à ce principe. **Solution :** On remarque que "D" devient "I".

16) Un autre élève a repéré les échanges de messages et comprend le principe, mais n'a pas bien vu la table utilisée. Il recrée une table avec le générateur (0, 0). Il intercepte le message précédent et le déchiffre en partant de (0, 0). Il obtient " ZIMIWCLOTMCPJ". Comment est-ce qu'il peut faire pour rechercher les espaces dans le message d'origine?

Solution : Il peut chercher un symbole qui revient souvent et toutes les 4 ou 5 lettres.

17) Il suppose que les "I" correspondent aux espaces. À l'aide de sa table ci-dessous, déterminer la case de départ qu'il doit choisir au lieu de (0, 0) pour déchiffrer le message?

Solution : Le "I" est 3 cases au dessus de l'espace. Il doit donc partir de (3, 0).

18) Au final, il obtient "ON A KU CHAUD.". Expliquer pourquoi ni lui, ni l'expéditrice du message, n'ont commit d'erreur. Vous pouvez vous appuyer sur la table qu'il a utilisé et celle des deux autres élèves.

Solution : Le déplacement de " " vers "E" dans leur table correspond à un déplacement de " " vers "K" dans sa table.

	0	1	2	3	4	5
0	I	J	K	L	M	N
1	O	P	Q	R	S	T
2	U	V	W	X	Y	Z
3		.	,	'	A	B
4	C	D	E	F	G	H

Table 5

	0	1	2	3	4	5
0	A	B	C	D	E	F
1	G	H	I	J	K	L
2	M	N	O	P	Q	R
3	S	T	U	V	W	X
4	Y	Z		.	,	'

Sa table

	0	1	2	3	4	5
0	K	L	M	N	O	P
1	Q	R	S	T	U	V
2	W	X	Y	Z		.
3	,	'	A	B	C	D
4	E	F	G	H	I	J

Leur table

BONUS: (2, 3) et [(3, 0), (4, 3), (3, 4), (2, 3), (4, 1), (1, 2), (2, 5), (3, 3), (2, 2), (1, 2), (3, 1), (3, 3), (3, 0), (1, 2), (1, 0), (0, 4), (4, 2), (2, 2), (1, 3), (2, 1), (3, 5), (1, 5), (3, 2)]

Solution: "NE FAITES PAS CA EN NSI"