Centres étrangers – 2026 – sujet1

Exercice 2 (6 points)

Cet exercice porte sur la sécurisation des communications et la programmation.

Le chiffrement de Polybe est un algorithme de chiffrement par substitution qui utilise un tableau dans lequel sont réparties les 26 lettres de l'alphabet et les 10 chiffres.

Exemple de tableau :

	1	**2**	**3**	**4**	**5**	**6**
1	Q	7	A	X	2	J
2	9	E	H	0	R	M
3	L	Z	4	W	D	O
4	6	V	N	B	8	K
5	P	Y	1	S	T	F
6	G	C	3	I	U	5

Chaque caractère est alors associé à un couple d'entiers construit à partir de sa position dans le tableau. Dans l'exemple ci-dessus, la lettre `N` située ligne 4, colonne 3 est associée au couple d'entier (4,3).

Avec la répartition donnée dans le tableau ci-dessus, le message `NSI` sera chiffré sous la forme (4,3) (5,4) (6,4).

1. Déchiffrer le message (6,2) (3,6) (3,5) (2,2) en utilisant la grille ci-dessus.

Une façon simple de construire un tableau consiste à choisir un mot qu'on appellera *clé*, à écrire cette clé dans le tableau puis à compléter avec les autres lettres dans l'ordre alphabétique, et enfin avec les chiffres de 0 à 9 par ordre croissant. Dans tout l'exercice, la clé utilisée sera toujours composée de lettres différentes, sans aucune répétition.

Exemple : Avec la clé `2048ALGORITHMES`, l'ordre d'insertion des caractères dans le tableau est `2048ALGORITHMESBCDFJKNPQUVWXYZ135679`, la grille obtenue est donc :

	1	**2**	**3**	**4**	**5**	**6**
1	2	0	4	8	A	L
2	G	O	R	I	T	H
3	M	E	S	B	C	D
4	F	J	K	N	P	Q
5	U	V	W	X	Y	Z
6	1	3	5	6	7	9

2. Chiffrer le message `BAC` avec la clé `SECURITY1024`.

3. Expliquer pourquoi le chiffrement de Polybe peut être qualifié de symétrique.

Le code de la fonction `generer_ordre` est fourni ci-dessous :

```
1    def generer_ordre(cle):
2        ordre_insertion = cle
3        alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789'
4        for lettre in alphabet:
5            if lettre not in ordre_insertion:
6                ordre_insertion = ordre_insertion + lettre
7        return ordre_insertion
```

4. Quel sera le résultat de l'appel `generer_ordre('AXU7')` ?

5. Coder la fonction `grille_vide(n)` qui renvoie un tableau de n lignes constituées chacune de n chaînes de caractères vides. Par exemple, l'appel `grille_vide(3)` renvoie `[['','',''],['','',''],['','','']]`.

Le code de la fonction `generer_grille` est fourni ci-dessous :

```
1    def generer_grille(cle):
2        ordre_insertion = generer_ordre(cle)
3        grille = grille_vide(6)
4        indice = 0
5        for i in range(...):
6            for j in range(...):
7                grille[i][j] = ...
8                indice = indice + 1
9        return grille
```

6. Recopier et compléter les lignes 5, 6 et 7 de la fonction `generer_grille` qui prend en paramètre la clé et renvoie un tableau représentant la grille.

7. Recopier et compléter la ligne 5 de la fonction `dechiffrer` qui prend en paramètres une clé et le message chiffré sous la forme d'un tableau de tuples puis renvoie le message déchiffré sous la forme d'une chaîne de caractères. Par exemple, comme `NSI` se chiffre en (4,4) (3,3) (2,4) avec la clé `2048ALGORITHMES`, l'appel `dechiffrer('2048ALGORITHMES',[(4,4),(3,3),(2,4)])` renvoie `'NSI'`.

```
1  def dechiffrer(cle, message):
2      resultat = ''
4      grille = generer_grille(cle)
5      for t in message:
6          resultat = resultat + grille[...][...]
7      return resultat
```

On souhaite maintenant écrire une fonction `chiffrer`. Pour éviter d'avoir à parcourir la grille pour chaque lettre du message à chiffrer, on va construire un dictionnaire dont les clés sont les lettres de l'alphabet et les 10 chiffres et dont les valeurs sont les positions associées dans la grille sous forme de tuples.

Par exemple, le début du dictionnaire associé à la grille qui correspond à la clé `2048ALGORITHMES` est : `{'2': (1, 1), '0': (1, 2), '4': (1, 3), '8': (1, 4), 'A': (1, 5) ... }`

8. Écrire la fonction `generer_dico` prenant en paramètre la clé et renvoyant le dictionnaire associé.

9. Écrire la fonction `chiffrer` qui prend en paramètre la clé et le message puis renvoie le message chiffré sous forme de liste de tuples.

Alice souhaite envoyer des informations secrètes à Bob chaque jour. Pour cela, ils décident d'utiliser le chiffrement de Polybe et pour plus de sécurité, ils changeront de clé quotidiennement. Alice propose à Bob d'utiliser des méthodes de chiffrements asymétriques pour s'échanger la clé.

10. Expliquer la différence entre un algorithme de chiffrement symétrique et un algorithme de chiffrement asymétrique.