Exercice 3 (8 points)

Cet exercice porte sur la programmation en Python, les bases de données relationnelles, le langage SQL, les systèmes d'exploitation et la sécurisation des communications.

Pour simplifier la gestion de ses mots de passe, Alice décide de créer un gestionnaire de mots de passe regroupant les informations de connexion de chaque site qu'elle utilise.

Partie A

Dans cette partie, on s'intéresse à la création des mots de passe d'Alice. On s'aidera de la table ASCII de la Figure 1 donnant le code ASCII en décimal et en hexadécimal des différents caractères utilisés dans ce sujet (lettres minuscules, lettres majuscules et les caractères spéciaux encadrés).

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Figure 1. Table ASCII. Les caractères spéciaux utilisés dans ce sujet sont encadrés

Source : d'après https://fr.m.wikipedia.org/wiki/Fichier : ASCII-Table.svg

Alice souhaite créer une fonction Python `gen_mdp` lui permettant de créer aléatoirement un mot de passe. Cette fonction :

- prend en paramètres :
  - `longueur` (de type `int`) : le nombre de caractères du mot de passe ;
  - `cont_min` (de type `bool`) : un booléen indiquant si le mot de passe peut contenir des minuscules (`True`) ou non (`False`) ;
  - `cont_maj` (de type `bool`) : un booléen indiquant si le mot de passe peut contenir des majuscules (`True`) ou non (`False`) ;
  - `cont_spe` (de type `bool`) : un booléen indiquant si le mot de passe peut contenir des caractères spéciaux (`True`) ou non (`False`) ;
- et renvoie un mot de passe (de type `str`) respectant les conditions définies par les paramètres.

On donne ci-dessous le code de la fonction `gen_mdp` qui sera à compléter au fur et à mesure des questions.

```
 1 from random import randint
 2
 3 def gen_mdp(longueur, cont_min, cont_maj, cont_spe):
 4     # Pour qu'un mot de passe soit non vide, il doit
 5     # pouvoir contenir des minuscules ou des majuscules
 6     # ou des caractères spéciaux.
 7     assert (cont_min or cont_maj or cont_spe)
 8     minuscules = [chr(i) for i in ...]
 9     majuscules = [...]
10     caracteres_speciaux = ... + ...
11     jeu_caracteres = []
12     if cont_min:
13         ...
14     ...
15         ...
16     ...
17         ...
18     mot_de_passe = ''
19     n = len(jeu_caracteres)
20     for i in range(longueur):
21         mot_de_passe = ...
22     return mot_de_passe
```

On rappelle que l'opérateur + permet en Python d'additionner deux éléments de type `int`, mais aussi de concaténer deux éléments de type `list`, ou encore deux éléments de type `str`.

On rappelle également que `chr(i)` renvoie la chaîne représentant un caractère dont le code ASCII est le nombre entier `i`.

Par exemple, `chr(97)` renvoie la chaîne de caractères `'a'`, tandis que `chr(33)` renvoie la chaîne de caractères `'!'`.

1. Alice s'inscrit sur un nouveau site lui demandant de créer un mot de passe de 8 caractères minimum, composé uniquement de majuscules et de minuscules. Écrire un appel à la fonction `gen_mdp` qui permette de répondre aux exigences de ce site.

On admet que les caractères spéciaux sont uniquement ceux encadrés à la Figure 1.

2. Recopier et compléter les lignes 8 à 10 du code de la fonction `gen_mdp` permettant d'initialiser les trois variables `minuscules`, `majuscules` et `caracteres_speciaux`. On utilisera obligatoirement la syntaxe de tableaux donnés en compréhension pour cette initialisation.
   Après cette initialisation, on doit avoir :

   - `minuscules` initialisée à `['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']`
   - `majuscules` initialisée à `['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']`
   - `caracteres_speciaux` initialisée à `['!', '"', '#', '$', '%', '&', "'", '(', ')', '*', '+', ',', '-', '.', '/', ':', ';', '<', '=', '>', '?', '@']`

3. La variable `jeu_caracteres` de la fonction `gen_mdp` est une liste contenant tous les caractères autorisés pour fabriquer un nouveau mot de passe. Recopier et compléter la ligne 13 du code de la fonction `gen_mdp`, puis écrire les autres lignes de code afin de créer la variable `jeu_caracteres`. Le nombre de lignes de code à insérer est laissé à l'appréciation du candidat.

4. La documentation de la fonction `randint` indique que `randint(a, b)` renvoie un entier aléatoire compris entre les entiers `a` et `b` incluant les deux extrémités `a` et `b`. Recopier et compléter la ligne 21 du code de la fonction `gen_mdp`.

5. Un site demande de créer un mot de passe possédant obligatoirement les caractéristiques suivantes :

   - le mot de passe doit contenir au moins 12 caractères ;
   - le mot de passe doit contenir au moins un caractère spécial et au moins une lettre minuscule.

   Expliquer en quoi le code de la fonction `gen_mdp` peut renvoyer un mot de passe qui ne répond pas aux exigences du site.

Partie B

Dans cette partie, on pourra utiliser les clauses du langage SQL pour :

- construire des requêtes d'interrogation à l'aide de `SELECT`, `FROM`, `WHERE` (avec les opérateurs logiques `AND`, `OR`), `JOIN ... ON` ;
- construire des requêtes d'insertion et de mise à jour à l'aide de `UPDATE`, `INSERT`, `DELETE` ;
- affiner les recherches à l'aide de `DISTINCT`, `ORDER BY`.

Alice souhaite mettre en œuvre une base de données composée des deux tables `compte` et `site` dont des extraits sont donnés dans les tableaux suivants.

compte			
mot_de_passe	utilisateur	renouvellement	id_site
Asrtg!Myfj	aliceB24	2022-06-30	1
@rDfohpj!&	aliceB24	2021-03-12	2
GxRGDxc(u-PM	alice_B@votremailp.me	2018-10-14	4
Ghcj=+f*AZs	alice1276	2022-06-30	3
cYFgt!:Ehr;	alice_B2@votremailp.me	2022-06-30	4

site		
id	nom_site	url
1	Vosnotes	https://logi-educ.net/vosnotes/eleve.html
2	Banque Perso	https://www.banqueperso.fr/connexion.html
3	Elec verte	https://espace-client.ev.fr/login
4	Votremailp	https://account.votremailp.me/login

- L'attribut `mot_de_passe` est une clé primaire de la table `compte`.
- L'attribut `id` est une clé primaire de la table `site`.
- L'attribut `renouvellement`, correspondant au dernier renouvellement du mot de passe, est une chaîne de caractères de format AAAA-MM-JJ. Ainsi un mot de passe renouvelé le 21 février 2025 correspond à un attribut `renouvellement` de `'2025-02-21'`.

- Dans la table `compte`, l'attribut `id_site` est une clé étrangère référençant l'attribut `id` de la table `site`.

6. Expliquer en quoi il n'est pas possible, pour Alice, d'avoir le même mot de passe pour deux sites différents.

7. Écrire la requête SQL permettant d'afficher toutes les URL enregistrées dans la base de données.

8. La Banque Perso a demandé à Alice de renouveler son mot de passe. Elle remplace le mot de passe `'@rDfohpj!&'` par `'yhTS?d@UTJe'`. Écrire la requête SQL permettant de faire la modification dans la base de données. Dans cette question, on ignorera l'attribut `renouvellement` et on ne cherchera pas à le mettre à jour.

On rappelle que le langage SQL utilise l'ordre lexicographique (ordre du dictionnaire) pour comparer deux éléments de type texte. Selon cet ordre, on a par exemple `'3'` supérieur à `'1'` et `'python'` est inférieur à `'sql'`.

9. À la date du 20 mars 2025, Alice a décidé de lister tous les mots de passe qui n'ont pas été renouvelés depuis plus d'un an. Écrire la requête SQL permettant de donner la liste des `id_site` concernés.

10. Donner une raison pour laquelle Alice a préféré choisir le format AAAA-MM-JJ pour l'attribut `renouvellement` plutôt que le format JJ-MM-AAAA.

11. Écrire une requête SQL permettant d'afficher tous les utilisateurs et les mots de passe du ou des sites de nom `'Votremailp'` dont l'identifiant est supposé non connu. Le résultat devra être affiché par ordre chronologique de date de renouvellement de mot de passe.

12. Pour réaliser le projet, il aurait été possible de regrouper toutes les informations dans une seule table mais Alice a choisi d'utiliser deux tables : les tables `site` et `compte`. Donner un avantage impliqué par le choix d'Alice.

Partie C

Dans cette partie, on s'intéresse à la sécurité du gestionnaire de mots de passe d'Alice. Alice utilise un système d'exploitation multi-utilisateurs basé sur Linux et elle a les droits de lecture, d'écriture et d'exécution dans son répertoire personnel `/home`.

La base de données est stockée dans un fichier `gestionnaire.db`. Alice décide de chiffrer ce fichier. Elle crée un fichier `chiffrement.py` dans lequel elle écrit le code d'une fonction Python `chiffrement` dont la documentation est donnée ci-après.

```
1 def chiffrement(f_source, f_dest, f_cle):
2     '''Crée un fichier f_dest contenant les données
3     du fichier f_source chiffrées selon la clé
4     contenue dans le fichier f_cle.
```

```
5       f_source (str) : chemin vers le fichier à chiffrer
6       f_dest (str) : chemin vers le fichier chiffré
7       f_cle (str) : chemin vers le fichier contenant la clé
8       '''
```

On donne l'arborescence de fichiers utilisée par Alice sur la Figure 2.

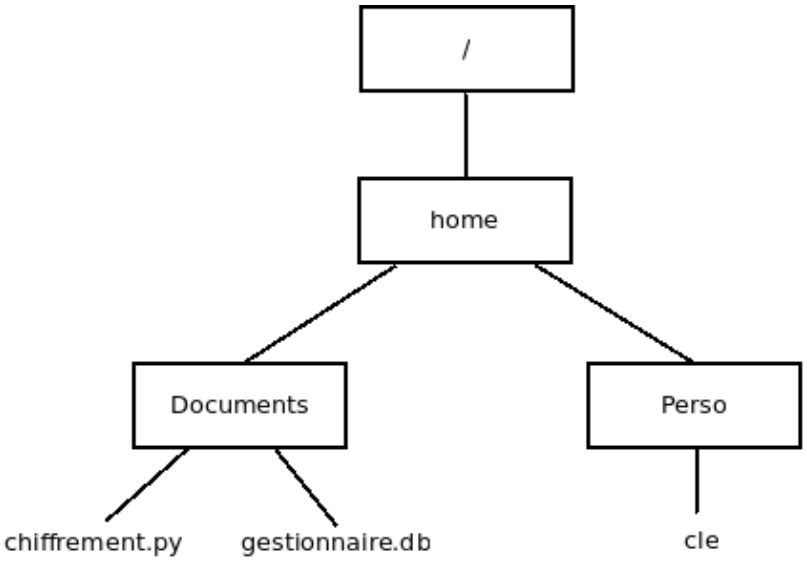

Figure 2. Arborescence de fichiers

Alice ouvre un interpréteur Python dans le répertoire `Documents`, qui est ainsi le répertoire courant (ou répertoire de travail) et exécute le contenu du fichier `chiffrement.py`.

13. Écrire l'appel à la fonction `chiffrement` permettant, à l'aide de la clé contenue dans le fichier `cle`, de chiffrer le fichier `gestionnaire.db` en créant le fichier chiffré `secret.db` dans le répertoire `Perso`.

L'algorithme de chiffrement consiste à appliquer l'opération OU-exclusif bit à bit entre le fichier source et le fichier contenant la clé de chiffrement.

Le premier bit du fichier chiffré est le résultat du OU-exclusif entre le premier bit du fichier source et le premier bit du fichier clé. De même, le deuxième bit est obtenu par le OU-exclusif entre les deuxièmes bits de ces deux fichiers et ainsi de suite.

On suppose, pour simplifier, que le fichier contenant la clé est de la même taille que le fichier source, qui est donc aussi la taille du fichier chiffré.

On rappelle ci-après la table de vérité du OU-exclusif, noté XOR.

Table de vérité du XOR		
a	b	a XOR b
0	0	0
0	1	1
1	0	1
1	1	0

On rappelle que l'hexadécimal correspond à l'écriture des entiers dans la base 16. Les chiffres de cette base sont notés `0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F`.

14. Donner le résultat, en écriture hexadécimale, de l'opération OU-exclusif bit à bit entre deux octets dont les écritures hexadécimales sont respectivement `A3` et `59`.

15. Montrer que, pour tous bits `a` et `b`, on a la propriété suivante : `(a XOR b) XOR b = a`.

16. Indiquer, en justifiant, si le chiffrement utilisé par Alice est symétrique ou asymétrique.

Alice exécute la commande `ls -l secret.db` et obtient la réponse donnée ci-dessous :

```
-rw-r--r-- 1 alice eleves 42480 mars 25 11:57 secret.db
```

17. Justifier le fait qu'un attaquant a le champ libre pour tenter un déchiffrement du fichier `secret.db` et expliquer ce que devrait faire Alice pour corriger ce problème.

Partie D

On donne ci-dessous quatre bonnes pratiques proposées par le gouvernement en matière de gestion des mots de passe.

- P1 : Utilisez un mot de passe différent pour chaque accès (messagerie, banque en ligne, comptes de réseaux sociaux, etc.) : en cas de compromission de l'un de vos comptes, cela évitera l'effet boule de neige.
- P2 : Créez un mot de passe suffisamment long, complexe et inattendu, de 8 caractères minimum, contenant des minuscules, des majuscules, des chiffres et des caractères spéciaux.
- P3 : Ne communiquez jamais votre mot de passe à un tiers : aucune organisation ou personne de confiance ne vous demandera de lui communiquer votre mot de passe.

- P4 : Utilisez un gestionnaire de mots de passe : pas simple de retenir tous ses codes de connexion ! Heureusement des outils de type « coffres forts de mots de passe » existent. Ces derniers mémorisent tous vos mots de passe et vous permettent d'en générer de manière aléatoire.

Source : d'après https://cyber.gouv.fr/bonnes-pratiques-protegez-vous

18. En justifiant votre réponse, préciser en quoi les choix d'Alice dans la conception de son gestionnaire de mots de passe respectent ou non chacune des quatre bonnes pratiques mentionnées.