Polynésie – 2025 – sujet1 - Correction

Exercice 3 (8 points)

Partie A – Python

1. Appel à la fonction `gen_mdp`

Site :

- minimum 8 caractères
- uniquement minuscules et majuscules

```
gen_mdp(8, True, True, False)
```

---

2. Initialisation des listes (lignes 8 à 10)

```
minuscules = [chr(i) for i in range(97, 123)]
majuscules = [chr(i) for i in range(65, 91)]
caracteres_speciaux = [chr(i) for i in range(33, 48) if chr(i) in ['!',
'"', '#', '$', '%', '&', "'", '(', ')', '*', '+', ',', '-', '.', '/',
':', ';', '<', '=', '>', '?', '@']]
```

👉*Commentaire:*

- 97 à 122 → lettres minuscules
- 65 à 90 → lettres majuscules
- On respecte l'énoncé en utilisant une compréhension de liste.

---

3. Création de la variable `jeu_caracteres`

Ligne 13 :

```
jeu_caracteres = []
```

Puis :

```
if cont_min:
    jeu_caracteres = jeu_caracteres + minuscules
```

```
if cont_maj:
    jeu_caracteres = jeu_caracteres + majuscules

if cont_spe:
    jeu_caracteres = jeu_caracteres + caracteres_speciaux
```

👉*Commentaire:*

- On concatène les listes selon les paramètres booléens.
- L'opérateur + concatène les listes.

---

4. Ligne 21 – utilisation de randint

```
indice = randint(0, len(jeu_caracteres) - 1)
```

👉*Commentaire: Attention : borne supérieure incluse.*

---

5. Pourquoi le mot de passe peut ne pas respecter les contraintes ?

Le site exige :

- ≥ 12 caractères
- au moins 1 caractère spécial
- au moins 1 minuscule

Problème :

La fonction choisit les caractères **aléatoirement dans le jeu autorisé**,
mais ne garantit pas qu'au moins un caractère de chaque type apparaisse.

👉*Commentaire:*

- On peut générer 12 majuscules sans aucun caractère spécial.
- Il faudrait forcer au moins un caractère de chaque type requis.

Partie B – SQL

6. Pourquoi Alice ne peut pas avoir le même mot de passe pour deux sites ?

`mot_de_passe` est **clé primaire**.

Une clé primaire doit être :

- unique
- non nulle

👉*Commentaire: Impossible d'avoir deux lignes avec le même mot de passe.*

---

7. Afficher toutes les URL

```
SELECT url
FROM site;
```

👉*Commentaire: Requête simple sans condition.*

---

8. Modifier le mot de passe Banque Perso

```
UPDATE compte
SET mot_de_passe = 'yhTS?d@UTJe'
WHERE mot_de_passe = '@rDfohpj!&';
```

---

9. Liste des id_site non renouvelés depuis plus d'un an (au 20 mars 2025)

Date limite :
20 mars 2024 → `'2024-03-20'`

```
SELECT DISTINCT id_site
FROM compte
WHERE renouvellement < '2024-03-20';
```

---

10. Pourquoi choisir AAAA-MM-JJ ?

Parce que l'ordre lexicographique correspond à l'ordre chronologique.

11. Utilisateurs et mots de passe du site "Votremailp"

```
SELECT utilisateur, mot_de_passe
FROM compte
JOIN site ON compte.id_site = site.id
WHERE nom_site = 'Votremailp'
ORDER BY renouvellement;
```

👉*Commentaire:*

- Jointure nécessaire.
- ORDER BY pour ordre chronologique croissant (par défaut).

---

12. Avantage d'utiliser deux tables

- Évite la redondance des URL.
- Respecte la normalisation.
- Meilleure cohérence des données.

Partie C – Sécurité

13. Appel de la fonction chiffrement

Depuis `Documents` :

```
chiffrement("../gestionnaire.db", "../Perso/secret.db", "../cle")
```

👉*Commentaire:*

- On remonte d'un niveau avec . . .
- Chemins relatifs au répertoire courant.

---

14. XOR entre A3 et 59

A3 = 10100011
59 = 01011001

XOR : `11111010`

En hexadécimal : `FA`

---

15. Montrer que (a XOR b) XOR b = a

Table de vérité :

Si b = 0 → a XOR 0 = a
Puis a XOR 0 = a

Si b = 1 → a XOR 1 inverse a
Puis inverse(a) XOR 1 redonne a

Donc propriété vraie.

---

16. Chiffrement symétrique ou asymétrique ?

Symétrique.

👉*Justification:*

- Même clé utilisée pour chiffrer et déchiffrer.
- Propriété précédente le montre.

---

17. Pourquoi le fichier est vulnérable ?

Permissions : `-rw-r--r--`

Cela signifie :

- propriétaire : lecture + écriture
- groupe : lecture
- autres : lecture

👉*Justification:*

- *Tout utilisateur peut lire le fichier.*
- *Un attaquant peut tenter un déchiffrement.*

Correction : chmod `600 secret.db`

Restreindre les droits au propriétaire uniquement.

Partie D – Bonnes pratiques

18. Analyse des pratiques

P1 – mot de passe différent

❌ Non respecté.

👉 Clé primaire = mot de passe unique →
elle ne peut pas avoir le même mot de passe sur deux sites (imposé par la base, mais pas par sécurité réfléchie).

P2 – mot de passe complexe

✔ Partiellement respecté.

👉 Génération aléatoire OK.
👉 Mais pas de garantie de présence obligatoire des différents types.

P3 – ne pas communiquer

✔ Respecté.

👉 Aucun partage mentionné.

P4 – gestionnaire de mots de passe

✔ Respecté.

👉 Elle a justement créé un gestionnaire.