

Exercice 3 : Gestionnaire de mots de passe

Partie A

1. La CNIL recommande d'avoir des mots de passe d'au moins 12 caractères :

```
gen_mdp(12, True, True, False)
```

2. D'après la table ASCII, les minuscules vont de 97 (a) à 122 (z), les majuscules de 65 (A) à 90 (Z) et les caractères spéciaux de 33 à 47 et de 58 à 64 :

```
8   minuscules = [chr(i) for i in range(97, 123)]
9   majuscules = [chr(i) for i in range(65, 91)]
10  caracteres_speciaux = [chr(i) for i in range(33, 48)]
    + [chr(i) for i in range(58, 65)]
```

```
3.      11  jeu_caracteres = []
        12  if cont_min:
        13      jeu_caracteres += minuscules
        14  if cont_maj:
        15      jeu_caracteres += majuscules
        16  if cont_spe:
        17      jeu_caracteres += caracteres_speciaux
```

```
4.      21  mot_de_passe = mot_de_passe + jeu_caracteres[randint(0, n-1)]
```

5. Les caractères composants le mot de passe sont piochés au hasard dans une liste de majuscules, minuscules et caractères spéciaux mais rien ne vérifie qu'il y a bien une minuscule et un caractère spécial qui ont été sélectionnés.

6. L'attribut mot_de_passe étant défini comme clé primaire de la table compte, la contrainte de relation impose des valeurs différentes de cet attribut pour chaque enregistrement.

Partie B

```
7.      SELECT url FROM site;
```

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

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

10. Le format AAAA-MM-JJ permet d'assurer que l'ordre lexicographique des dates est équivalent à l'ordre des dates elle-même.

En effet **2025-03-21** est bien supérieur à **2025-02-23**
alors que **21-03-2025** est inférieur à **23-02-2025**.

11.

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

12. La solution à deux table a un avantage dans le cas où Alice possède plusieurs comptes sur un même site car cela évite la redondances des informations des sites concernés.

Partie C

13.

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

14. **Rappel :** Un caractère hexadécimal correspond à 4 caractères binaires : $A_{(16)} = 1010_{(2)}$.

$A3_{(16)} = 10100011_{(2)}$

$59_{(16)} = 01011001_{(2)}$

XOR $11111010_{(2)} = FA_{(16)}$

15. Pour démontrer $(a \text{ XOR } b) \text{ XOR } b = a$, il faut établir la table de vérité :

a	b	a XOR b	(a XOR b) XOR b
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

16. Ce chiffrement est symétrique car la clé de déchiffrement est la même que celle de chiffrement.

17. Tous les utilisateurs -rw-r--r-- possèdent le droit de lecture sur le fichier secret.db et peuvent donc notamment l'ouvrir et tenter une attaque.

Alice peut corriger ce problème en supprimant ce droit à tous les utilisateurs.

Partie D

18.

P1 : Alice a choisi mot_de_passe comme clé primaire de la table compte, ce qui impose l'unicité des mots de passe pour chaque site.

P2 : L'outil d'Alice lui permet de générer des mots de passe suffisamment long même si cela n'est pas imposé.

P3 : Alice a décidé de chiffrer sa base de donnée de mot de passe, ce qui ajoute un niveau de sécurité mais l'humain reste toujours le maillon faible. Alice doit s'appliquer cette règle et ne rien communiquer à d'autres concernant son système de mot de passe.

P4 : Alice a développé son projet dans le but de réaliser cette consigne : créer un gestionnaire de mot de passe.