

CORRIGÉ ÉPREUVE REGROUPEE**Discipline : INFORMATIQUE****Date :** 12.06.2025**Cours : 2 IN DP 03 / 04 / 0****Durée :** 105 minutes**Maître: JC Barros****Matériel autorisé: aucun (aide-mémoire inclus à la fin d'épreuve)****9 pages (dont 2 d'aide mémoire)****Nom et prénom: CORRIGÉ****Total: 70 points****Sécurité****Ex 1.**

/ 7 pts

Voici un programme Python:

```

1 def chiffre_cesar(texte, decalage):
2     resultat = ""
3     for caractere in texte:
4         if caractere.isalpha():
5             # Déterminer la base (majuscule ou minuscule)
6             base = ord('A') if caractere.isupper() else ord('a')
7             # Appliquer le décalage et reste dans l'alphabet
8             nouveau = chr((ord(caractere) - base + decalage) % 26 + base)
9             resultat += nouveau
10        else:
11            # Laisser les caractères non alphabétiques inchangés
12            resultat += caractere
13    return resultat
14 # Exemple d'utilisation
15 print("Texte chiffré :", chiffre_cesar("Bonjour", -3))

```

barème

points	note
0	1,5
10,5	2
17,5	2,5
24,5	3
31,5	3,5
38,5	4
45,5	4,5
52,5	5
59,5	5,5
66,5	6

- `print`, `chr`, `ord` et `chiffre_cesar` sont des... **fonctions**
- Expliquer comment ce programme Python gère les caractères qui ne font pas partie de l'alphabet
A la ligne 4, si caractere est alphabétique, on applique la méthode de chiffrement. Sinon, on le laisse tel quel (signes de ponctuations, chiffres, etc.)
- Quelle est l'utilité de la fonction `ord()` dans le code ? Et `chr()`?
Ces fonctions transforment un caractère en code ASCII (ord) ou l'inverse (chr).
- Que montre exactement le programme ci-dessus dans la console lorsqu'il est exécuté ?
Texte chiffré : Ylkglro

Ex 2.

/ 6 pts

Chiffrer les messages suivants avec les algorithmes / clés indiqués:

algorithme →	César	Vigenère	Vernam
message clair →	EPREUVE	REGROUPEE	1001 1001
clef →	C (+2)	AZUR	0110 0110
message chiffré →	GRTGWXG	RDAIOTJVE	1111 1111

Ex 3.

/ 6 pts

Remplir chaque case vide comme il faut:

algorithme →	César	Vigenère	Vernam
message clair →	ELEVER	REGROUPEE	1010 1010
clef →	* Y (-2)	AB	0000 0000
message chiffré →	CJCTCP	RFGSOVPFE	1010 1010

★ **Expliquer:** On peut essayer les 25 possibilités jusqu'à obtenir un résultat qui est du français ou on peut gagner du temps en partant de l'idée que la lettre la plus fréquente en français est le "E". Il y a donc des chances pour que le "C" dans le message chiffré (présent à 3 exemplaires) représente le "E". Cela correspond à un décalage de -2 ou + 24 (Y).

Ex 4.

/ 3 pts

Placer dans les ensembles ci-dessous les techniques suivantes:

Chiffrement	symétrique	asymétrique
César	X	
AES	X	
Vernam	X	
ElGamal		X
RSA		X
Vigenère	X	

Ex 5.

/ 4 pts

Alice veut envoyer un message à Bob en utilisant un chiffrement asymétrique.

Elle va utiliser la clef **publique** de **Bob** pour le chiffrer.

Quand Bob le reçoit, il va utiliser la clef **privée** de **Bob** pour le déchiffrer.

Alice veut signer numériquement un document. Elle va donc chiffrer un hash du document avec la clef **privée** de **Alice** puis envoyer ce hash chiffré avec le document, comme preuve d'authenticité.

Ensuite, Bob veut vérifier la signature d'Alice. Il va donc déchiffrer le hash chiffré en utilisant la clef **publique** de **Alice** qu'il pourra comparer avec le hash du document calculé par ses soins.

Ex 6.

/ 4 pts

Authenticité: **TLS permet de garantir l'authenticité d'une page web. La signature numérique permet de garantir l'authenticité de toute donnée binaire (fichier, message, document, etc.).**

Confidentialité: **TLS permet de garantir la confidentialité des échanges entre notre navigateur (client web) et le serveur web qui nous livre les informations des pages demandées. Le chiffrement (qu'il soit symétrique ou asymétrique) permet d'assurer la confidentialité car il rend des données illisible à quiconque n'a pas la clef pour le déchiffrer.**

Base de données

Ex 7.

/ 7 pts

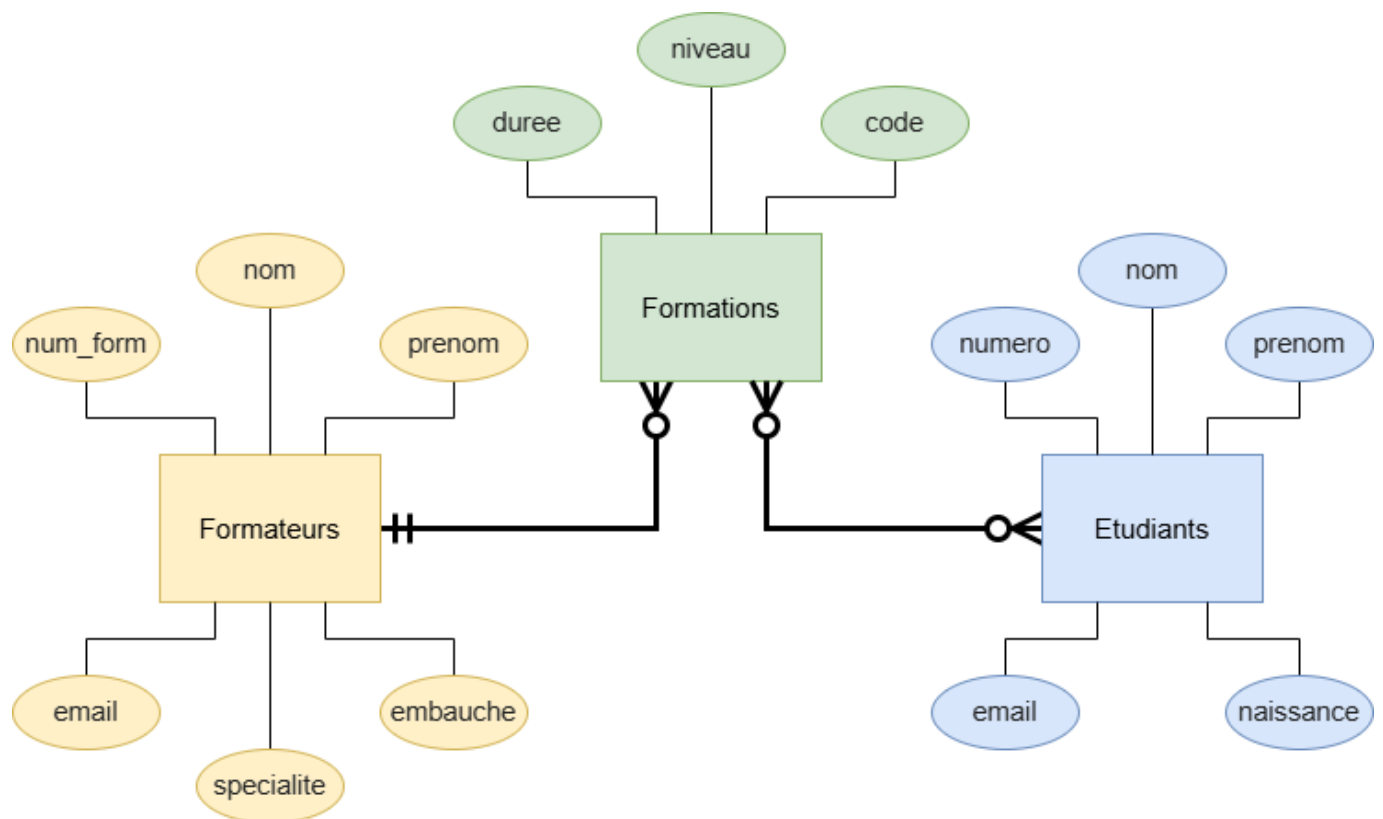
Un centre de formation souhaite informatiser la gestion de ses formations, de ses formateurs et de ses étudiants. Voici la description :

- Un formateur est identifié par un numéro, avec son nom, prénom, email, spécialité et date d'embauche.
- Le centre propose plusieurs formations, chacune ayant un formateur, une durée (en jours), un niveau (débutant, intermédiaire, avancé) et un code de formation unique.
- Un étudiant est inscrit à une ou plusieurs formations. Il est identifié par un numéro, avec un nom, un prénom, une date de naissance et un email.

En se référant à la description, on souhaite construire le **diagramme Entité-Relation (ERD)** du système.

Pour cela, répondre aux questions suivantes :

- Ajouter les attributs dans le schéma ci-dessous selon la description.
- Ajouter les relations entre les entités et indiquer leurs cardinalités.



- Est-ce que le formateur est un attribut de l'entité formation ?

Non, c'est un lien vers une autre entité (Formateurs) qui correspond donc à une clef étrangère dans la table formation

Ex 8.

/ 1 pt

Quelle instruction SQL permet de supprimer des enregistrements dans une table ? **b. DELETE**

- DROP
- DELETE**
- TRUNCATE
- REMOVE

Ex 9.

/ 4 pts

Comment sélectionner uniquement les noms et prénoms dont le nom commence par "M" ?

Clients	
PK	<u>id_client</u>
	nom prenom email adresse date_naissance

```
SELECT nom, prenom
FROM Clients
WHERE nom > "M" AND nom < "N";
```

Ex 10.

/ 4 pts

a. Qu'affiche la requête SQL suivante ?

```
SELECT
    titre,
    annee_sortie,
    note
FROM
    Films
ORDER BY
    note DESC
LIMIT 5;
```

Elle affiche le titre, l'année de sortie et la note des 5 films les mieux notés.

b. Qu'est-ce qui change si on modifie DESC en ASC ?

Elle affichera le titre, l'année de sortie et la note des 5 films les moins bien notés.

Ex 11.

/ 1 pt

Vrai ou **Faux** : La clé primaire peut contenir des valeurs dupliquées, mais pas de valeurs nulles.
Une clef primaire est obligatoirement UNIQUE: pas de valeurs dupliquées.

Ex 12.

/ 1 pt

Laquelle des affirmations suivantes décrit le mieux une clé étrangère (foreign key) ?

- a. Identifie de manière unique un enregistrement dans sa propre table
b. Permet de relier des enregistrements entre deux tables

Ex 13.

/ 2 pts

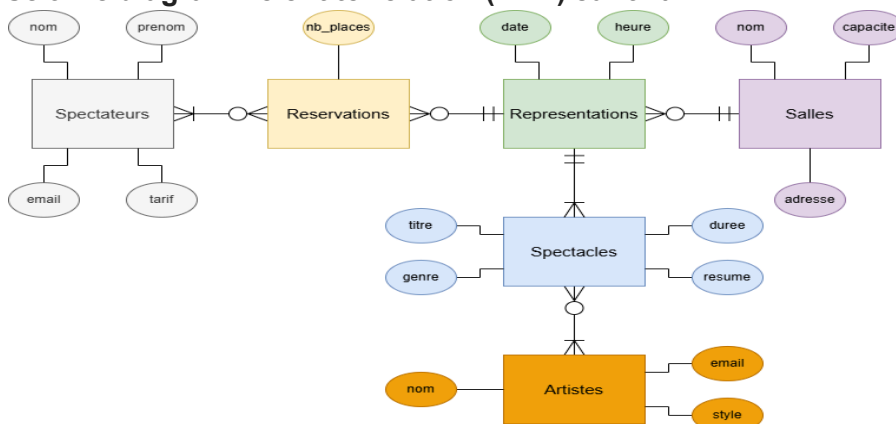
Quelle différence fondamentale entre une base de données relationnelle et NoSQL ?

Relationnelle est normalisée, donc très structurée dans des tables liées par des relations. Elle garantit l'intégrité et la disponibilité des données. Fiable -> banques, écoles, magasins, etc.
NoSQL est moins rigide et donc moins fiable mais plus rapide -> les réseaux sociaux, statistiques sur beaucoup de données qui changent très vite, etc.

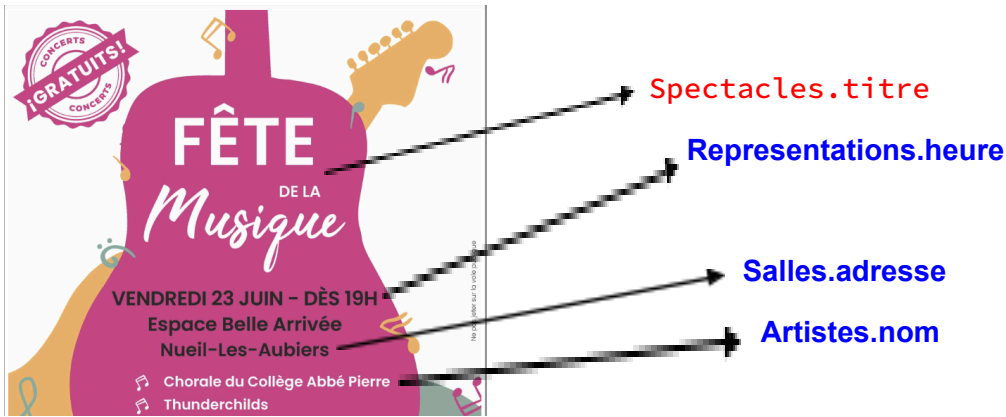
Ex 14.

/ 12 pts

Selon le **diagramme entité-relation (ERD)** suivant :



- a. Observer l'affiche de concert ci-dessous et écrire la table et le champ où doit être enregistrée chacune des informations indiquées par une flèche. Suivre l'exemple de la première:



- b. D'après le structure de cette base de données, est-ce qu'un même spectacle peut être joué plusieurs soirs de suite ? **NON**
Justification avec un élément pertinent du diagramme ERD:
La cardinalité du lien entre Spectacles et Représentations montre qu'un spectacle ne peut avoir qu'une et une seule représentation!
- c. Est-ce que le système permet d'enregistrer un même spectateur qui achète des billets pour plusieurs spectacles différents ? **NON mais...**
Si on assimile un billet à une réservation, vu qu'il ne peut faire une réservation que pour une seule représentation à la fois (voir cardinalité entre Réservations et Représentations), la réponse serait NON. Mais:
- Il peut faire plusieurs réservations, chacune pour une représentation différente (donc potentiellement pour un spectacle différent).
- Une représentation peut contenir plusieurs spectacles différents (cardinalité entre Représentations et Spectacles)
Donc OUI et NON...
- d. Comment obtenir tous les emails des spectateurs ? Écrire la requête SQL.
SELECT email FROM Spectateurs;
- e. Expliquer à quoi sert cette requête SQL:

```
SELECT
    Spectacles.titre
FROM
    Spectacles
JOIN
    Représentations USING(id_représentation)

WHERE
    Représentations.date = '2025-06-12';
```

Réponse: **Affiche le titre de tous les spectacles ayant lieu le 12 juin 2025**

Dessiner le schéma relationnel des tables correspondant à cet ERD:

ERD:

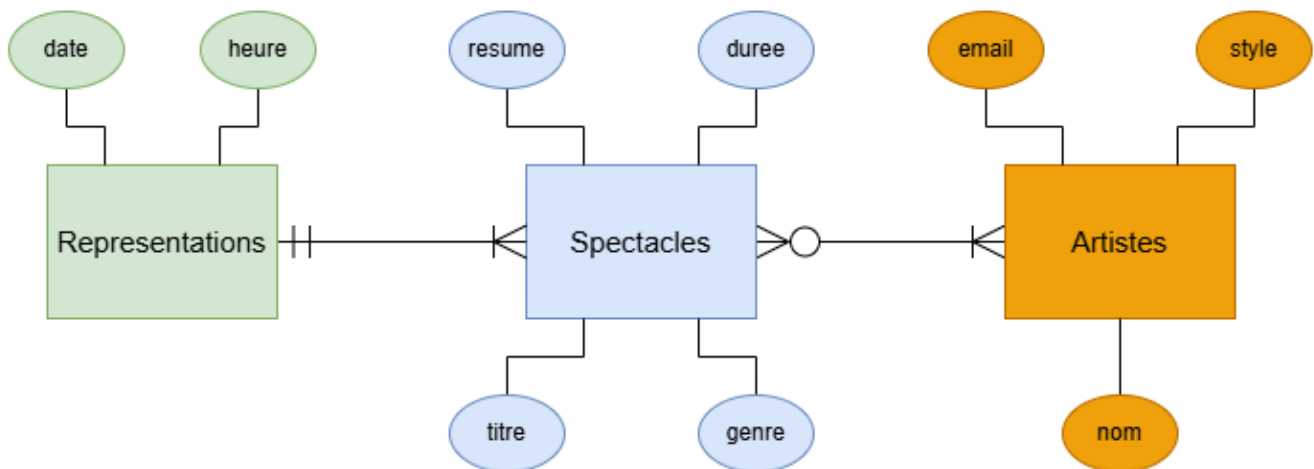


Schéma relationnel des tables:

