

ÉPREUVE REGROUPEE

Discipline: INFORMATIQUE

Cours: 2 IN DP 08 / 09 / 10

Date: 15/6/2023

Durée: 105 minutes

Maître: Juan-Carlos Barros

Matériel autorisé: aucun (aide-mémoire inclus à la fin de l'épreuve)

Consignes de travail:

- Ecriture lisible et présentation soignée
- Mise en évidence des résultats

Nom et prénom:

CORRIGE

Total: 55 pts

points	note
8,5	2
14	2,5
19,5	3
25	3,5
30,5	4
36	4,5
41,5	5
47	5,5
52,5	6

BASES DE DONNÉES:

Ex 1: (3 pts)

Indiquer les deux principaux types de bases de données et mentionner une différence fondamentale entre les deux.

1 relationnelle : données stockées sous forme de tables avec relations

1 NoSQL : données stockées autrement.

1

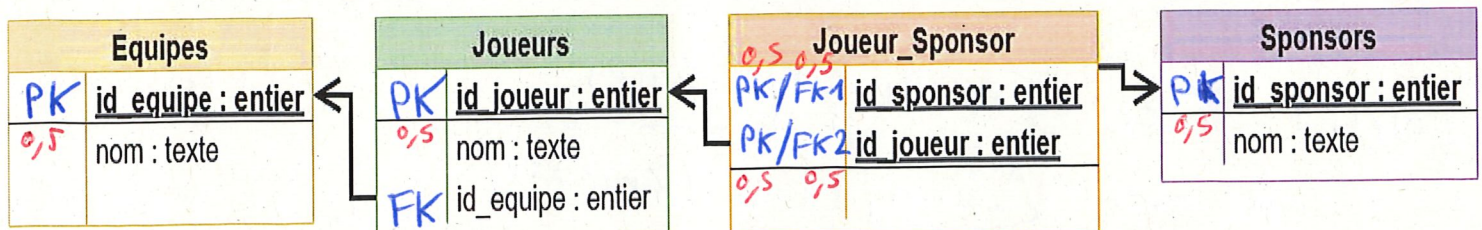
Ex 2: (6 pts)

a. Expliquer à quoi servent une clé primaire (primary key) et une clé étrangère (foreign key). (2 pts)

clé primaire : sert à identifier de manière unique un enregistrement dans la table où elle est employée.

clé étrangère : fait le lien avec la clé primaire d'une autre table.

b. Dans le schéma des tables suivant, indiquer quelles sont les clés primaires et étrangères de chaque entité: (ajouter simplement PK et / ou FK dans la colonne vide, là où c'est utile). (4 pts)



-0,5 pour clefs indiquées à tort à d'autres emplacements

Ex 3: (3 pts)

Dans une base de données correspondant au schéma ci-dessus, à quoi servent les requêtes suivantes ?

a) `SELECT nom FROM Equipes;` (1 pt)

affiche le nom de chaque équipe présente dans la table Equipes.

b) `SELECT * FROM Equipes;` (1 pt)

idem que a) mais :
affiche tous les champs (pas seulement le nom).
Donc : id équipe et nom

c) `SELECT * FROM Joueurs WHERE id_joueur=4;` (1 pt)

affiche tous les champs (id-joueur, nom, id-equipe)
du joueur dont l'id-joueur est égal à 4.

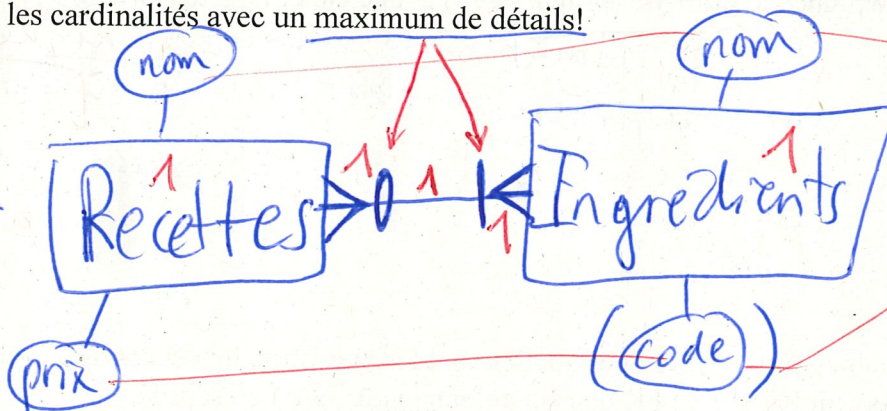
Ex 4: (6 pts)

La "Compagnie des rôtisseurs" propose des plats sous vide à réchauffer pour les restaurants de son réseau. Elle souhaite créer une base de données pour gérer les informations sur ses plats.

Voici la description des données à stocker :

- La recette de chaque plat est créée par un ou plusieurs auteurs. Elle comporte un nom, un prix et un ensemble d'ingrédients.
- Chaque ingrédient comporte un nom et un code. Un ingrédient peut bien sûr être utilisé dans différentes recettes.
- Chaque auteur de recettes est identifié par un code et comporte un nom et un prénom.
- Un restaurant du réseau est identifié par un code et comporte une adresse, un téléphone et un email.

À partir de cette description, on voit qu'il existe plusieurs entités. Parmi celles-ci, proposer un modèle abstrait partiel (sous forme de diagramme) comportant **deux** entités et **une** association qui les relie. Indiquer les cardinalités avec un maximum de détails!



• schéma des tables + modèle abstrait : (-1)

• schéma des tables au lieu du modèle abstrait : (-3)

• + de 2 entités : (-1)

• entités au lieu de entités : (-1)

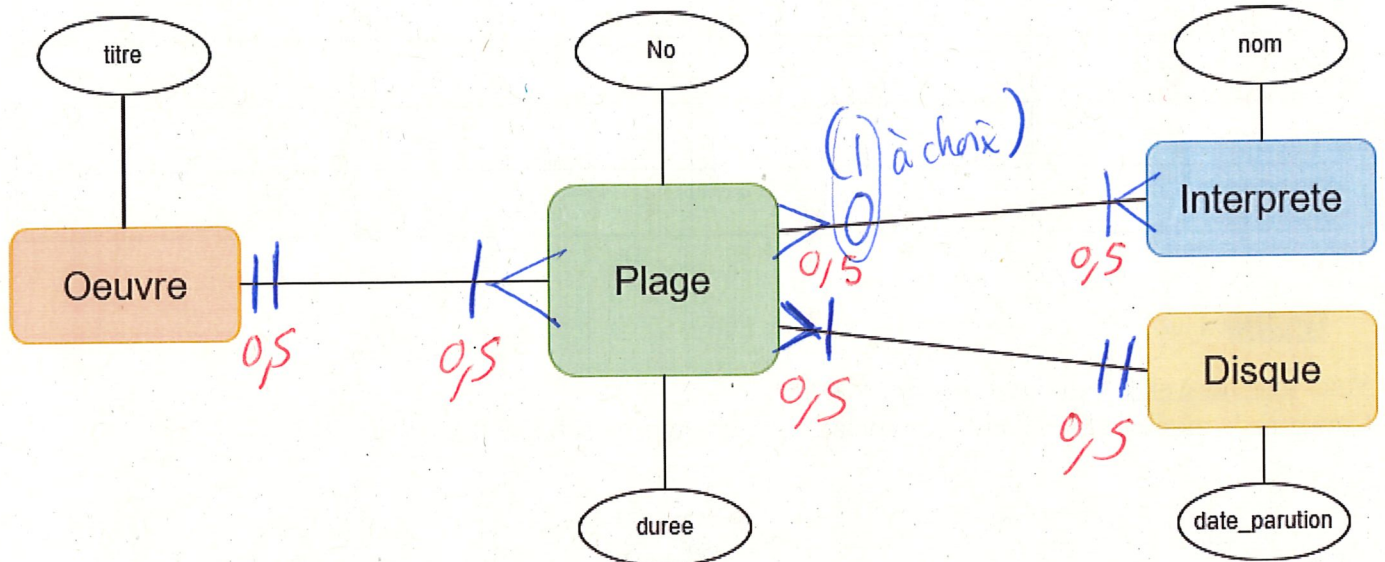
Ex 5: (3 pts)

Voici le début d'un modèle abstrait entité-association pour la gestion d'une médiathèque. La spécification des besoins est la suivante :

Un disque est constitué d'un ensemble de plages. Chaque plage correspond à une œuvre et une seule, mais une œuvre peut s'étendre sur plusieurs plages (par exemple une symphonie en 4 mouvements). De plus, pour chaque plage, on connaît le(s) interprète(s).

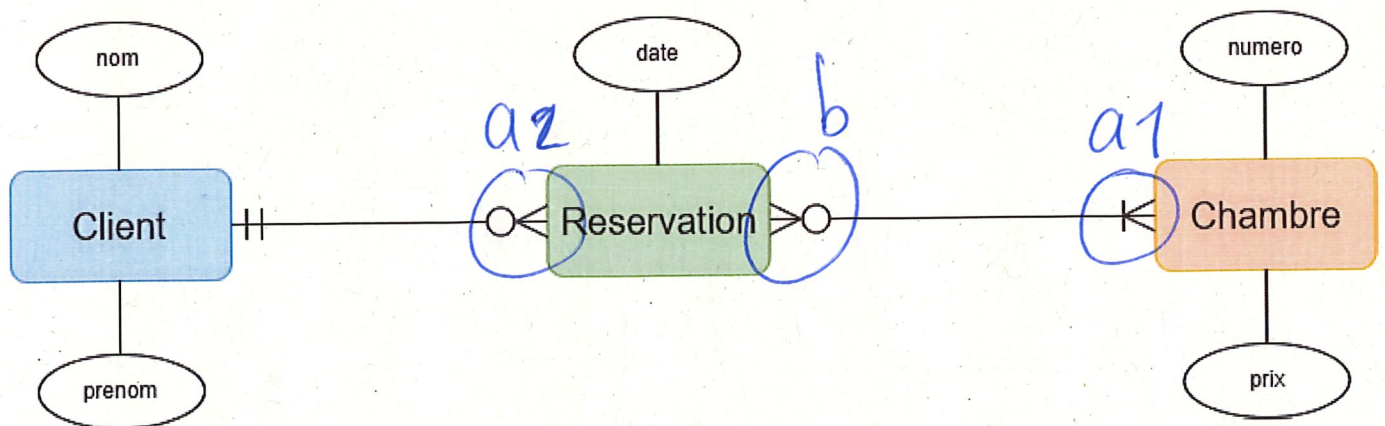
Compléter le schéma en ajoutant les cardinalités avec un maximum de détails d'après la description.

donc : min et max (que max : 0,25)



Ex 6: (6 pts)

On souhaite gérer des réservations dans un hôtel. Dans ce but, on considère le modèle abstrait entité-association ci-dessous:



À partir de ce diagramme, répondre aux questions suivantes :

a. Un client peut-il réserver plusieurs chambres à une date donnée ? (2 pts)

oui / non Justifier : (entourer une cardinalité avec la mention **a**, si c'est utile pour la justification)

1 **oui** / **non** en une seule réservation (a1) **1**
ou en plusieurs réservations (a2)

b. Est-il possible qu'une chambre n'ait jamais été réservée d'après le modèle ? (2 pts)

oui / non Justifier : (entourer une cardinalité avec la mention **b**, si c'est utile pour la justification)

1 **oui** / **non** b dit qu'il peut y avoir 0 réservation pour une chambre donnée. **1**

c. Est-il possible d'avoir des clients homonymes ? (2 pts)

1 **oui** / non

Si oui, compléter la table **T_Client** avec deux clients homonymes.

Sinon, compléter la table **T_Client** avec deux exemples de clients.

Attention : il y a plus de lignes et de colonnes que nécessaire.

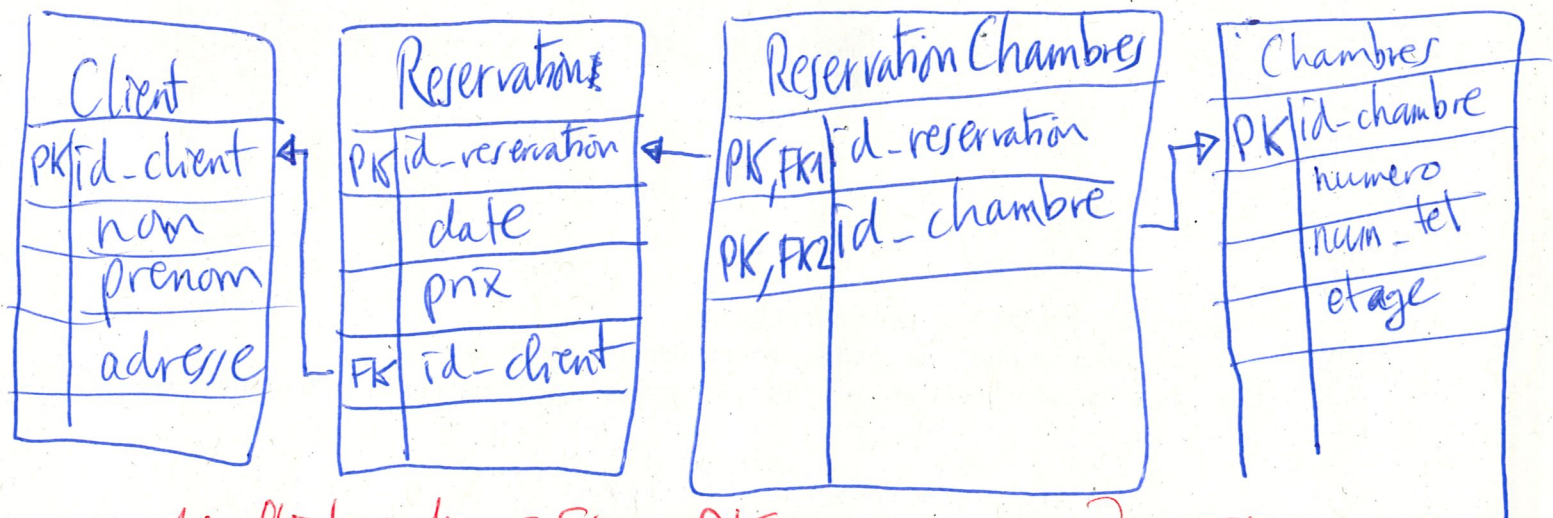
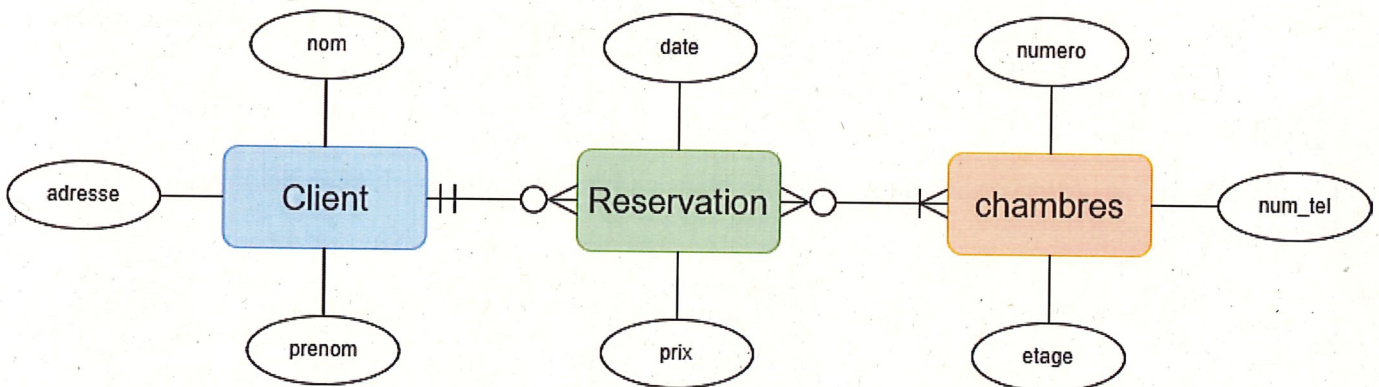
T_Client

<i>id_client</i>	<i>nom</i>	<i>prenom</i>	
1	Barros	Juan-Carlos	
2	Barros	Juan-Carlos	
3	Gainsbourg	Serge	
4	Brel	Jacques	

Ex 7: (6 pts)

Voici une autre situation dans une autre BDD.

Convertir le modèle abstrait entité-association ci-dessous en schéma des tables :



- 1: flèches depuis FK → PK
- 1: PK ajoutées dans chaque table
- 1: une table pour chaque entité
- 1: champs complétés, corrects
- 1: FK indiqués et corrects
- 1: table ~~Reservation Chambres~~ correcte

0,5 par erreur pour chaque catégorie

Ex 8: (2 pts)

Décrire un exemple de technique permettant de normaliser les données.
Expliquer pourquoi cela permet d'éviter des problèmes.

- 1 • incorporer une clef primaire dans chaque table
- 1 → cela permet de s'assurer qu'il ne peut pas y avoir d'ambiguïté entre deux enregistrements (comme les clients homonymes)

SÉCURITÉ:

Ex 9: (2 pts)

Chiffrer la phrase suivante à l'aide de la méthode César avec un décalage de +3 caractères :

"ASSEZ"

2 DVVHC

(-1 par lettre fausse)

Ex 10: (4 pts)

Chiffrement de Vigenère:

- a. Déchiffrer le message chiffré suivant sachant que la clef de chiffrement est "ABC": (2 pts)

CPWCPW

2 COUCOU

(idem ↑)

- b. Est-il facile de décrypter ce message si on ne connaît pas la clef de chiffrement? (2 pts)

Argumenter la réponse

1 • non

→ car il existe un nombre énorme de combinaisons pouvant former une clef. Donc la force brute ne peut pas suffire (contrairement au chiffrement de César qui n'a que 25 clefs différentes).

Ex 11: (2 pts)

Supposons que nous voulions chiffrer l'octet suivant (8 bits) à l'aide de la méthode Vernam (= Vigenère binaire) et d'une clé de chiffrement aléatoire :

Octet original : 1010 1001 (2)

Clé aléatoire : 1100 1000 (2)

Pour effectuer le chiffrement, on effectue une opération XOR ("ou exclusif") entre chaque bit de l'octet original et le bit correspondant de la clé dans la même position. Par exemple, en effectuant l'opération XOR entre le premier bit de l'octet original (1) et le premier bit de la clé (1), on obtient : $1 \text{ XOR } 1 = 0$. Le résultat final du chiffrement sera l'octet obtenu après l'application de l'opération XOR.

L'octet chiffré est :

2 0110 0001

(-1 par bit faux)

Ex 12: (2 pts)

Quelles sont les différences entre un chiffrement symétrique et asymétrique ?

Donner deux différences importantes.

1	1. <u>Asymétrique</u> à deux clefs	<u>Symétrique</u> à une clef
1	2. ~~pas besoin de~~ création de secret partage facile	impossible de partager un secret (la clef) sur internet sans risque
	etc.	etc.

Ex 13: (2 pts)

Alice (A) veut envoyer un message chiffré à Bob (B) en utilisant un chiffrement asymétrique.

a. Quelle clef de chiffrement est utilisée par Alice ? (entourer ses caractéristiques) (1 pt)

propriétaire de la clef: Alice / Bob 0,5

type de la clef: privée / publique 0,5

b. Quelle clef est utilisée par Bob pour déchiffrer le message chiffré ? (idem) (1 pt)

propriétaire de la clef: Alice / Bob 0,5

type de la clef: privée / publique 0,5

Ex 14: (2 pts)

On utilise une application de messagerie qui nous assure que les conversations sont chiffrées de bout en bout.

a. Quelle notion de sécurité est assurée grâce à ce chiffrement? (1 pt)

1 confidentialité

b. Pourquoi? (1 pt)

1 car même si un man-in-the-middle ou l'entreprise qui gère la messagerie intercepte notre message, il ne pourra pas le décrypter.

Ex 15: (2 pts)

Donner un protocole de chiffrement symétrique et un autre asymétrique utilisés sur internet pour sécuriser nos échanges.

1 symétrique: AES

1 asymétrique: RSA / El Gamal

Ex 16: (4 pts)

Expliquer en quelques lignes ce qu'est le protocole **HTTPS** (au moins 4 informations importantes)

1 HTTPS est une contraction de HTTP et TLS.
HTTP est un protocole servant à échanger des pages web.
TLS " " " " sécuriser ces échanges.
1 TLS permet d'authentifier le serveur auquel nous nous connectons et de chiffrer nos échanges, ce qui assure l'authenticité et la confidentialité.

au delà des 4 points max, chaque info pertinente ajoute 0,5 points bonus!

FIN DE L'ÉPREUVE
(aide-mémoire suit)