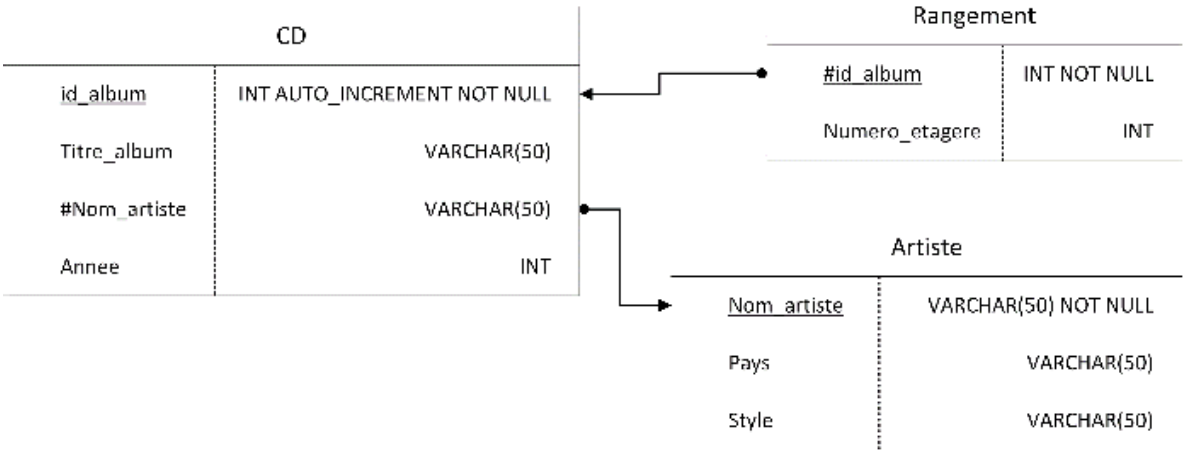
EXERCICE 1 (6 points)

Cet exercice porte sur la notion de bases de données relationnelles, le langage SQL et les protocoles de sécurisation.

Partie A – Bases de données

L'énoncé de cette partie utilise les mots du langage SQL suivants : SELECT, FROM, WHERE, JOIN, UPDATE, SET, DELETE. L'attribut AUTO_INCREMENT permet d'incrémenter automatiquement un entier dans une table à l 'insertion d'un nouvel élément.

Bob, qui dispose d'une très grande collection de CDs rangés sur plusieurs étagères numérotées, a mis en place une base de données. Voici la description des trois relations de cette base dont les clés primaires ont été soulignées et les clés étrangères indiquées par un # :



1. Indiquer, avec justification, s'il aurait été possible de choisir l'attribut Nom_artiste comme clé primaire dans la relation CD.

Dans la suite, on considère les clés étrangères suivantes :

- CD.Nom_artiste qui référence l'attribut Artiste.Nom_artiste ;
- Rangement.id_album qui référence l'attribut CD.id_album.

Voici un extrait des enregistrements des relations CD, Artiste et Rangement définies plus haut :

CD			
id_album	Titre_album	Nom_artiste	Annee
1	‘Master of Puppets’	‘Metallica’	1986
2	‘The Marshall Mathers LP’	‘Eminem’	2000
3	‘Wasting Light’	‘Foo Fighters’	2011
4	‘Wishmaster’	‘Nightwish’	2001
5	‘Dead Letters’	‘The Rasmus’	2003
6	‘Somewhere in Time’	‘Iron Maiden’	1986

Artiste		
Nom_artiste	Pays	Style
‘Nightwish’	‘Finlande’	‘Metal’
‘Foo Fighters’	‘Etats-Unis’	‘Rock’
‘Metallica’	‘Etats-Unis’	‘Metal’
‘Iron Maiden’	‘Royaume-Uni’	‘Metal’
‘Eminem’	‘Etats-Unis’	‘Rap’
‘The Rasmus’	‘Finlande’	‘Rock’

Rangement	
id_album	Numero_etagere
1	2
2	1
3	1
4	3
5	3
6	2

2. Écrire ce que renvoie la requête suivante lorsqu'on l'applique aux extraits ci-dessus.

```
SELECT Nom_artiste
FROM Artiste
WHERE Pays = "Finlande";
```

3. Écrire à présent ce que renvoie la requête suivante.

```
SELECT CD.Annee
FROM CD
JOIN Artiste
ON CD.Nom_artiste = Artiste.Nom_artiste
WHERE Artiste.Style = "Metal";
```

Bob se rend compte que l'album Wishmaster est en réalité sorti en 2000.

4. Donner la requête qu'il doit écrire pour mettre à jour sa base de données.

5. Donner la requête qu'il doit écrire pour afficher les titres de tous les albums de "Metal" rangés sur l'étagère dont le numéro est 1.

Bob a vendu l'album Dead Letters du groupe The Rasmus. Puisqu'il s'agissait du seul album de ce groupe qu'il possédait, il veut supprimer tous les enregistrements qui sont à présent inutiles dans les trois relations.

6. Donner l'ordre dans lequel il doit les supprimer en expliquant pourquoi, puis écrire la requête correspondant à la suppression de l'album dans la relation CD.

Partie B – Sécurisation

La base de données de Bob est hébergée sur un serveur auquel il accède depuis un client sur son ordinateur personnel. Pour sécuriser la connexion, un algorithme de chiffrement symétrique est utilisé.

7. Expliquer brièvement ce qu'est un algorithme de chiffrement symétrique.

La clé de chiffrement, notée C dans la suite, est choisie aléatoirement par le serveur à chaque connexion depuis un client. Afin que le chiffrement et le déchiffrement puisse se faire sans problème, le serveur doit envoyer au client la clé C de façon sécurisée.

8. Rappeler brièvement ce qu'est un algorithme de chiffrement asymétrique.

On suppose à présent que Bob possède une clé publique et une clé privée. La clé publique de Bob est supposée connue par le serveur.

9. Proposer alors une solution pour que le serveur puisse envoyer la clé C à l'ordinateur de Bob de façon sécurisée, c'est-à-dire pour que seul Bob puisse déchiffrer la clé envoyée.