EPSI – B3

Sécurité - Chapitre 03 – Cryptographie symétrique & asymétrique

TP

Préparation

1. Connectez-vous sur un linux en ligne de commande

Openssl - Chiffrement

1. Créer un fichier secret.txt contenant un cours texte (ex : Hello World !!!)
2. Chiffrer ce fichier avec la commande openssl en AES-256-CBC

Quelles options pour la commande openssl avez-vous utilisé ?

Openssl - Déchiffrement

1. Déchiffrer le fichier secret.aes en un fichier decrypt.txt

Openssl - STDIN

1. Chiffrer STDIN en aes-256-cbc bits grâce à la commande openssl

Openssl - STDOUT

1. Déchiffrer le fichier secret.aes vers STDOUT (sans passer par un fichier en clair)
2. Quel est l'intérêt de la 2nd méthode, celle ou on ne passe pas un fichier en clair, ni pour chiffrer ni pour déchiffrer ?

Openssl - Sécurisation

1. Quel est le protocole le moins sécurisé ?

   AES-256-ECB AES-256-CFB AES-256-OFB AES-256-CBC

2. Pourquoi ?
3. Quel est la différence entre ECB et CBC ?

RSA – Mode Manuel

1. Chiffrez le mot SOS avec du RSA, vous présenterez chaque étapes de la création des clés aux chiffrement

RSA – Openssl

1. Générez une pair de clé RSA avec la commande openssl
2. Chiffrez le message du fichier secret.txt
3. Signer le message du fichier secret.txt
4. Vérifiez la signature et déchiffrez le message

RSA – GPG

1. Reprenez les 5 questions précédente mais cette fois ci avec GPG

SSH

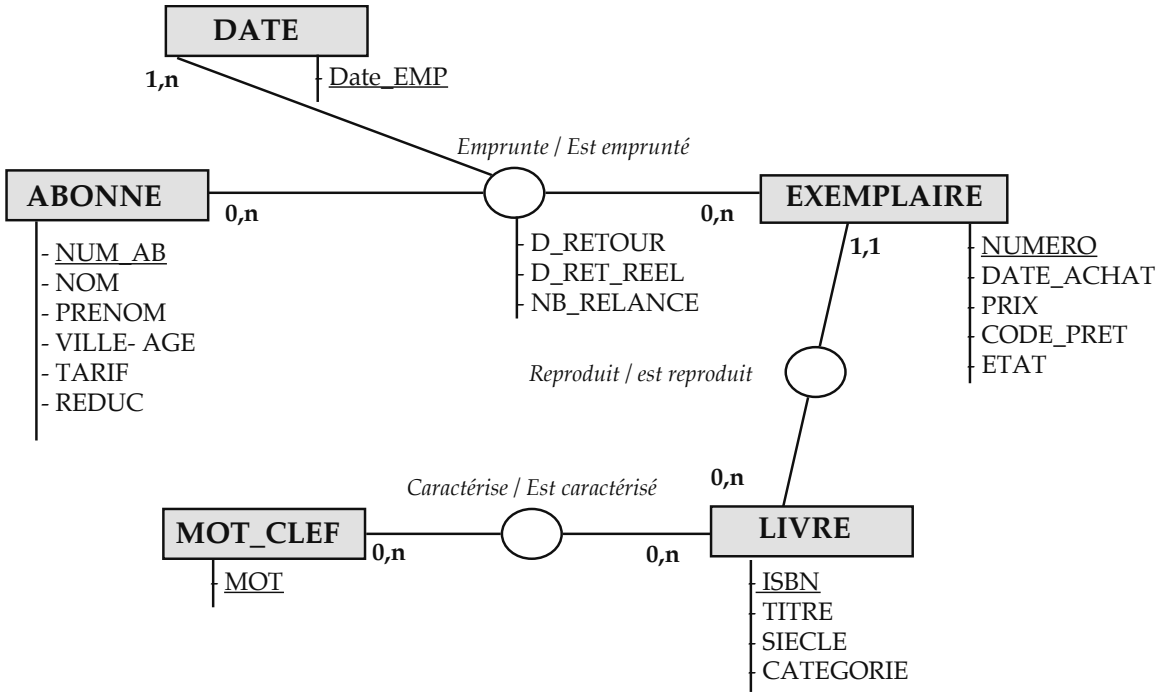
1. Comment ssh assure-t-il sa sécurité sans autorité de certification ?

TP BDA n° 1 : Oracle Prise en main et requête SQL

Objectifs du TP :
L'objet de cette première séance de TP est de se familiariser avec l'environnement d'Oracle et le schéma relationnel utilisé.

La base de données exemple

La base de données exemple, sur laquelle vous allez travailler, permet d'effectuer la gestion très simplifiée d'une bibliothèque. Elle a été élaborée à partir du schéma conceptuel suivant, selon le modèle Entité/Association :



Le schéma relationnel normalisé de la base exemple est le suivant (Par convention les clefs primaires sont soulignées et les clefs étrangères sont indiquées en italique) :

ABONNE (NUM_AB, NOM, PRENOM, VILLE, AGE, TARIF, REDUC)
EXEMPLAIRE (NUMERO, DATE_ACHAT, PRIX, CODE_PRET, ETAT, *ISBN*)
LIVRE (ISBN, TITRE, SIECLE, CATEGORIE)
MOT_CLEF (MOT)
EMPRUNT (*NUM_AB*, *NUM_EX*, D_EMPRUNT, D_RETOUR, D_RET_REEL, NB_RELANCE)
CARACTERISE (*ISBN*, *MOT*)

Remarques : Les attributs NUM_EX dans EMPRUNT et NUMERO dans EXEMPLAIRE représentent le numéro identifiant un exemplaire de livre.
Le domaine D_MOT est un sur-ensemble de D_CATEGORIE.

Création des tables

Récupérer les fichiers à l'adresse suivante :
http://textmining.biz/Staff/Teisseire/creation.sql
http://textmining.biz/Staff/Teisseire/remplissage.sql

Lancer le client SQL developer d'Oracle

Attendre son numéro avant de se connecter

1.Utilisateur : B3_GRAx ou B3_GRBx **(x de 1 à 25)**
2.Mot de passe : B3C2_GR**x (x de 1 à 19)**

Service : bdaolap
Exécuter les fichiers pour créer les relations et insérer les données correspondantes ou copier les dans l'éditeur.

Pour utiliser Oracle de l'extérieur :

Si vous voulez vous connecter à la base de données Oracle depuis l'extérieur, vous devez utiliser les informations suivantes :

Nom d'hôte: oracle.montpellier.epsi.fr
Port externe : 4521
SID : bdaolap

Les requêtes

Q1 Quels sont les nom, prénom des abonnés domiciliés à Montpellier ?

Q2 Donner toutes les informations sur les exemplaires dont le code de prêt est : « EMPRUNTABLE ».

Q3 Donner la liste des livres (leur titre et catégorie) de toutes les catégories sauf Médecine, Sciences et Loisirs. Cette liste sera donnée triée par ordre alphabétique selon la catégorie.

Q4 Donner toutes les informations sur les emprunts pour lesquels la date de retour effective (attribut D_RET_REEL) n'est pas renseignée dans la base de données.

Q5 Donner, pour l'abonné Jean Dupont, la liste des exemplaires empruntés (leur numéro et la date d'emprunt), par ordre croissant de date d'emprunt.

Q6 Donner la liste des exemplaires empruntés (leur numéro, code prêt et état) du livre de titre « LE MUR».

Q7 Quels sont les exemplaires (numéro) reproduisant le même livre que l'exemplaire de numéro 4112 et dont l'état est : « BON » ?

Q8 Existe-t-il une catégorie pour laquelle aucun livre n'a été emprunté ?

Q9 Quel est le nombre d'emprunt en cours de l'abonné Renard Albert ?

Q10 Quel est le tarif d'abonnement le plus faible ?

Q11 Existe-t-il des exemplaires dans l'état « Abimé » et qui sont actuellement empruntés ? Si oui, donner leur numéro.

Q12 Existe-t-il des mots clefs ne caractérisant aucun livre ?

Q13 Donner le nombre d'emprunts effectués par chacun des abonnés (numéro, nom) pour chacune des catégories de livres proposées.

Q14 Donner, pour chaque livre (numéro ISBN) ayant plus de deux exemplaires, le prix moyen d'achat des exemplaires.

Q15 Quels sont les livres caractérisés par exactement les mêmes mots clefs que l'ouvrage de numéro ISBN 0-8-7707-2.

Q16 Existe-t'il des catégories de livres empruntées par tous les abonnés ?