الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Saad Dahlab-Blida-1
Faculté des Sciences - Département d'Informatique
وزارة التعليم العالي و البحث العلمي
جامعة سعد دحلب البليدة-1
كلية العلوم-قسم الإعلام الآلي

Concours d'accès à la formation doctorale 3éme cycle 2021/2022

(05/03/2022)
Filière : Informatique
Spécialité : Data Science
Épreuve 2 : Sécuritésujet N°02, Durée : 02h00

Partie I: Sécurité Base de Données

Administration BD « L'Agence de l'Amélioration et du Développement du Logement»

L'Agence de l'Amélioration et du Développement du Logement (AADL) dispose d'un ensemble de directions régionales s'occupant du suivi des projets de réalisation de logement dans leurs zones respectives. Pour simplifier notre étude de cas, nous supposons que nous disposons de quatre directions à savoir : Centre, Est, Ouest et Sud.

Pour un meilleur contrôle de conformité, l'Agence mis en place dans ses directions régionales un service AUDIT qui se charge de contrôler les chantiers et vérifier la conformité des logements construits ou en cours de construction avec les cahiers des charges et les normes internationales de construction.

Dans ce service d'AUDIT, trois employés sont affectés, un chauffeur, un Architecture et un juriste. Chaque service suit un calendrier hebdomadaire pour faire ses tournées, à la fin de chaque tournée un compte rendu est rempli par chantier. Le compte rendu comporte un champ état ou l'expert décrit l'état d'avancement du chantier, et un champ booléen appelé conforme. Dans le cas de non-conformité une notification est envoyée au juriste, elle est enregistrée dans la table Notification.

Voici la base de données globale du système d'Audit.

Direction (Code, Siege, Region, Tel, Fax, site_web)
Ville(Code_Ville, Nom_Ville, #Direction)
Employé_Audit(NSS, Nom, Prenom, Fonction, Ville_Residence, #Direction).
Chantier(NumChantier, Adresse, Ville, Entrepreneur)
Rapport(#Chantier, Date, Etat, Conformité)
Notification(#Chantier,#NSS, Date)

Partie 1 : Vues et Triggers

1) Créer une vue « Statistique » permettant d'afficher pour chaque direction régionale le nombre d'audit effectués durant une période D1 et D2, et parmi ces audits le nombre de non conformités. **(2 pts)**
2) Créer un Trigger « Ajout_Notification » qui à chaque insertion d'un rapport dont la conformité n'est pas respectée, il insert une notification dans la table Notification après avoir recherché le numéro de sécurité du juriste qui devra la recevoir. **(2 pts)**

Partie 2 : Bases de données réparties

1) Proposez une fragmentation pour les tables Direction, Ville et Chantier par Région. **(3 X 1= 3 pts)**
2) Est-t-il intéressant de fragmenter la table Employé_Audit ? Justifiez **(1 pts)**

Partie II: Cryptographie

Sélectionner la ou les bonnes réponses (0.25 X 12 = 3 pts)

1. Le déchiffrement est :
   A. : Art de casser des cryptosystèmes
   B. Cacher le message pour que l'ennemi ne le trouve pas
   C. La fonction permettant de retrouver le texte clair à partir du texte chiffré.

2. Pretty Good Privacy de Philip Zimmermann (1991) PGP :
   A. cryptographie symétrique
   B. Cryptographie asymétrique
   C. Cryptographie hybride

3. Une « fonction de hachage » :
   A. Permet d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous.
   B. Permet de chiffrer et de déchiffrer un contenu avec la même clé
   C. Suppose que le (futur) destinataire est muni d'une paire de clés (clé privée, clé publique) et qu'il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique.
   D. Aucune réponse

4. Citer les Un standard en matière de fonction de hachage :
   A. SHA-1
   B. MD4
   C. MD5
   D. RSA
   E. RC4
   F. Aucune réponse

5. En utilisant le fait que $\varphi(187) = 160$ (protocole RSA), retrouver p et q :
   A. P=11 , q=16
   B. P=16 et q=17
   C. P=11et q=17
   D. P=23 et q =5
   E. Aucune réponse

6. Déterminez d tel que $7d = 1 \bmod 360$.
   A. 108
   B. 103
   C. 76
   D. 82

7. Le résultat de de 529^{436} mod 66
   A. 2
   B. 5
   C. 0
   D. 1

8. Considérer le système RSA avec p = 19 et q = 23.Calculer l'exposant *d* associé à *e* = 17.
   A. 89
   B. 143
   C. 47
   D. 233

9. Dans la méthode de signature EL GAMEL $y = g^x mod p$ représente :
   A. La clé privée
   B. La signature
   C. La clé publique
   D. Aucune réponse

10. Le chiffrement par le réseau de Feistel de message M= 1001 et soit f1(Entrée -Sortie) : (00 - 10),(01 -00)(10 -11) (11- 10) :
    A. G1=11 , D1=10
    B. G1= 10 , D1=01
    C. G1= 01, D1=10
    D. G1= 10, D1=11

11. Trouver la clé privée de l'algorithme RSA sachant que : p =5, q=11 et la clé publique est (7,55):
    A. (22.55)
    B. (23.55)
    C. (44.55)
    D. (22.56)
    E. Aucune réponse

12. Le certificat d 'authentification contient
    A. Une clé publique.
    B. Des informations sur le certificat
    C. Des informations sur le destinataire
    D. Une clé privée

Partie III: Sécurité des Systèmes d'Informations

EXERCICE 1 : (1 × 5 = 5 pts)

Parmi les expressions proposées, choisir **quatre (04) propositions** pour chaque modèle de contrôle d'accès.

Modèle	DAC	MAC	Muraille de chine	RBAC	ABAC
Réponses					

Choix

- **A.** Nécessite le regroupement des ressources (objets) en fonction des sujets qui l'ont accédé.
- **B.** Restreindre l'accès aux objets en fonction de l'identité des sujets ou des groupes auxquels ils appartiennent.
- **C.** L'accès à une ressource dépend de l'utilisateur tenant d'accéder, de la ressource, et du contenu de la ressource en question.
- **D.** Règles statiques et niveau de sécurité d'accès persistent.
- **E.** Le système autorise l'accès ou non selon la classification de la sensibilité de l'information.
- **F.** Conférer à l'utilisateur le pouvoir de décider qui peut accéder aux ressources qu'il possède.
- **G.** Dynamique, granulaire, et dépend du contexte au moment d'accès.
- **H.** Les sujets accèdent aux ressources en fonction des sessions qu'ils endossent.
- **I.** Un utilisateur peut avoir un accès à une ressource systématiquement, quand il a le droit d'accéder à une autre ressource.
- **J.** Savoir si d'un état sûr arbitraire on ne peut atteindre que des états sûrs est indécidable.
- **K.** Peut être utilisé pour implémenter le principe de la séparation des tâches.
- **L.** Offre un contrôle d'accès granulaire, mais sa mise en marche nécessite un paramétrage manuel.
- **M.** Un sujet ne peut lire aucun objet qui appartienne à un dataset de la même classe de conflits d'intérêts.
- **N.** Un utilisateur peut avoir plusieurs sous-ensembles d'autorisation en fonction de son rôle pendant la tentative d'accès.
- **O.** Utilise des règles qui définissent la politique d'accès en fonction du sujet, de l'objet, de l'action, et du contexte pendant la tentative d'accès.

*Les termes **objet/ressource** ainsi que **sujet/utilisateur** sont utilisés de manière interchangeable*

EXERCICE 2 : (1 + 1+ 2 = 4 pts)

Soit le protocole suivant appelé Andrew Secure RPC:

1. $A \rightarrow B : A, \{N_a\}K_{ab}$
2. $B \rightarrow A : \{N_a + 1, N_b\}K_{ab}$
3. $A \rightarrow B : \{N_b + 1\}K_{ab}$
4. $B \rightarrow A : \{K'_{ab}, N'_b\}K_{ab}$

K_{ab} : *Clé partagée de chiffrement initial*
N_a : *Nonce de l'utilisateur A*
N_b : *Nonce de l'utilisateur B*
K'_{ab} : *Nouvelle clé*

1. Ce protocole est vulnérable aux attaques par rejeu, définissez l'attaque.
2. Comment peut-on exploiter cette vulnérabilité sur ce protocole?
3. Proposez une correction à ce protocole pour remédier à sa vulnérabilité.