REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ D'ALGER 1 - BEN YOUCEF BEN-KHEDDA
FACULTE DES SCIENCES
DEPARTEMENT MATHEMATIQUES ET INFORMATIQUE

Spécialité : Système Informatique (SI) **Module :** Sécurité Informatique **Durée :** 01h30

Examen Semestriel

Partie cours : (5 points 0.25 pour chaque QCM et 1 point pour chaque réponse)

I. Pour chacun des cas suivants, quel objectif de la sécurité a été compromis :

1. Bob connait la date de naissance d'Alice
   a. confidentialité b. Intégrité c. non-répudiation
2. Un employeur modifie son salaire dans le PC de comptable
   a. confidentialité b. disponibilité c. intégrité
3. Bob modifie les valeurs d'un attribut dans une base de données
   a. intégrité b. intégrité et contrôle d'accès c. contrôle d'accès
4. Un virus supprime les fichiers dans un flash disque et les remplace par des raccourcis
   a. disponibilité b. authentification c. intégrité
5. Vous voulez copier des fichiers dans un flash disque. Ce dernier contient un virus. Lors de la copie vous avez le message « Flash in read only »
   a. disponibilité b. non-répudiation c. authentification
6. Bob a envoyé un message à Alice contenant un lien malveillant. Le lien a permis de voler le mot de passe de session d'Alice. Lors du conseil discipline, Bob a nié qu'il a envoyé le message
   a. contrôle d'accès b. non-répudiation c. authentification

II. Choisissez la bonne réponse

1. La plupart des systèmes d'authentification sont basés sur le principe ''AAA''. Que signifie ce principe ?
   a. (Autorisation, Authentification, Accountability)
   b. (Authentification, Autorisation, Accountability)
   c. (Accountability, Authentification, Autorisation)
2. Dans le mode de chiffrement par bloc 'CBC', chaque bloc est chiffré par
   a. La clé de chiffrement b. Le bloc précédent c. Le chiffré de bloc précédent

III. Questions

1. L'administrateur veut choisir l'une des deux stratégies de mots de passe :
   a. Minimum 3 caractères, maximum 6 caractères, lettres majuscules, minuscules et chiffres
   b. Minimum 6 Maximum 15 : lettres majuscules, minuscules, chiffres, 15 caractères spéciaux
      - Combien y a-t-il de mots de passe possibles pour chacune des politiques ?
      - Donner deux exemples de mots de passes pour chaque stratégie
2. Expliquez le fonctionnement du chiffrement symétrique. Quels sont les inconvénients ?
3. Expliquez le fonctionnement du chiffrement asymétrique. Quels sont les inconvénients ?

Exercice 1 (cryptographie classique) (3 points 1.5 pour chaque réponse)

Soit le schéma de chiffrement de César modifié comme suit : Le premier caractère est chiffré avec la clé, ensuite le deuxième caractère est chiffré en utilisant le premier caractère clair, le troisième en utilisant le deuxième et ainsi de suite.

1. Chiffrez le message « je suis etudiant » avec la clé 'E'
2. Déchiffrez le message « ooxndbxyoiwjoh » avec la clé 'E'

N. B. : la numérotation des caractères commence par 1 jusqu'à 26

Exercice 2 (sécurité des bases de données) (4 points 0.25 pour chaque requete)

Soit une base de données contenant les tables suivantes :
soldat (nomS, date_naissance, section, adresse, num_tel, date_entrée)
chef_section (nomC, date_naissance, section, adresse, num_tel)
Affectation : une vue de la table soldat contient son nom et sa section
sold : une vue de la table soldat contient son nom, sa section, et sa date d'entrée
Soit la table des droites d'accès suivante : (les lignes désignent l'utilisateur, les colonnes désignent les tables, et les cases les droits de chaque utilisateur sur chaque table)

Utilisateur	Soldat	Chef_section	Affectation	Sold
soldat1	Select		Select	Select
Chef1	Select	Select		Select
Commandant		All	All	All
Medecin	Select (nomS, date_naissance, section)	Select (nomC, date_naissance, section)		

1. écrire les requêtes SQL permettant l'attribution des droits cités dans le tableau
2. supposant soldat1 avait été affecté à une autre section. Dans ce cas on doit enlever tous les droits qu'il possède. Ecrire les requêtes SQL permettant cette opération.

Exercice 3 (disponibilité) (2.5 points 0.5 pour chacune)

Considérons un système à 5 serveurs (S1, S2, S3, S4 et S5) dont la disponibilité de chacun est respectivement dans l'ordre : 90%, 65%, 88%, 99%, 87%. Calculez pour chacun des cas suivants la disponibilité du système global :

1. ((S1 // S2) - S3) // (S4 // S5)
2. S1 - S2 - S3 - S4 - S5
3. (S1 // S2 // S3) - (S4 // S5)
4. (S3 // S4) - S1 - S2 - S5
5. (S1 - S2) // (S3 - S4 - S5)

Exercice 4 (contrôle d'accès) (5.5 points)

Soit l'organisation de l'entreprise EXA :

- Direction Générale (DG) : Khaled
- Direction Marketing (Mark) : Karim*, Kamelia
- Direction Production (Prod) : Slimane*, Ahmed
- Direction Informatique (Info) : Ramzy*, Mouloud

Fonctionnement :

- ✓ Khaled est le DG il a accès en lecture à tous les dossiers mais personne n'a accès à ses dossiers, de plus il est le seul habilité à écrire dans le dossier Alltage accessible par tout le monde en lecture sauf à kamelia.
- ✓ Les Directeurs d'activité marqués par (*) ont accès en lecture aux dossiers de leurs collaborateurs de plus ils ont accès en écriture au dossier partage de leurs structures.
- ✓ Les collaborateurs ont uniquement accès aux dossiers dont les privilèges sont ceux décrits plus haut.
- ✓ Les utilisateurs n'ont pas accès aux dossiers de leurs hiérarchies ni ceux de leurs collègues.
- ✓ Les utilisateurs ont accès en lecture seule aux dossiers de partage de leurs structures respectives quand ils sont autorisés.

1. (1.5 pts) Ce système est-il un système DAC, MAC ou RBAC ? justifier votre réponse
2. (2pts) Donnez la matrice de contrôle d'accès correspondante.
3. (2pts) On suppose qu'on vise à contrôler l'accès aux fichiers dans un système linux en utilisant la commande « chmod ». Pour chacun des cas suivants donner les valeurs des droits et interprétez-les en illustrant par un exemple de votre choix

   a) chmod 775 b) chmod 652 c) chmod 112 d) chmod 476