Université d'Oum El Bouaghi

Département des Mathématiques et de l'Informatique

Niveau : 03ème Licence informatique SI +ISIL — Dimanche 29 Mai 2022

Remarque : *Les réponses doivent être brèves, claires et concises* — **Durée**: 1h30'

Matière: Sécurité Informatique

Examen Final

Corrigé Type

1) Définir la sécurité informatique.

Définition de la sécurité informatique : l'ensemble de moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

01

2) Expliquer les attributs de la sécurité informatique.

- La confidentialité : qui consiste à protéger les informations de lecture non-autorisée ;
- L'intégrité : c'est-à-dire un tiers ne peut pas changer ou détruire les informations qui existent dans un ordinateur ou qui traversent un réseau. Au pire de cas, l'utilisateur de système informatique peut détecter le changement de ces informations.
- Disponibilité : cet attribut signifie que les gens autorisés à l'utilisation d'un système informatique ne seront pas empêché de le faire.
- No-répudiation : Cela signifie que quelqu'un qui a manipulé le système informatique, ne peut pas dénier de cet acte.

(05+05) * 4= 04pts

3) Quelle est la relation entre les politiques de sécurité et les procédures de sécurité?

Les politiques de sécurité sont implémentées (réalisées) par des procédures de sécurité.

01

4) Expliquer trois types de logiciels malveillants (Malware).

Il suffit d'expliquer trois types de logiciels malveillants expliqués déjà dans le support de cours (Virus, vers, cheval de Troie, Bombe logique, les portes dérobées, …etc.)

(0.5+0.5) *3 = 03 Pts

5) Est-ce qu'il vaut mieux de publier les points vulnérables dès qu'ils sont découverts ou retarder cette publication? Justifier.

La publication des points vulnérables dès qu'ils sont découverts permet aux utilisateurs d'être plus vigilants et peut être considérée comme une force de pression sur les développeurs pour corriger cette vulnérabilité, **mais** elle permet aussi aux hackers d'attaquer le système. Donc, il faut choisir le bon moment pour publier cette vulnérabilité.

01+01 =02 pts

6) Expliquer les opérations effectuées dans une ronde de l'algorithme DES.

04 Pts

Une ronde est composée d'opérations suivantes :

- Mettre le bloc gauche dans la partie droite.
- Une opération d'expansion sur la partie droite pour transformer un bloc de 32 bits à un bloc de 48 bits.
- Une opération d'OU exclusif (XOR) entre le bloc précédent et la clé (K_i).
- Une opération de sélection pour transformer le bloc de 48 bits à un bloc de 32 bits.
- Une opération de permutation.
- Une opération d'OU exclusif (XOR) avec la partie gauche.
- Le résultat est considéré la partie gauche.

7) On veut sauvegarder les noms d'utilisateurs d'un système donné et leurs mots de passe de façon sécurisée. Ainsi, les noms d'utilisateurs et les mots de passe sont cryptés dans la base de données. Nous avons choisi de crypter les noms d'utilisateurs avec la technique de Vignère (avec la clé: user). Par contre, les mots de passe sont cryptés par la technique affine. On note que les noms d'utilisateurs et les mots de passe sont composés seulement de lettres latines. Bien entendu, les noms d'utilisateurs ne sont pas sensibles à la casse (c'est-à-dire on ne distingue pas les lettres majuscules et minuscules). En revanche, les mots de passe sont sensibles à la casse.

01.5

   a) Crypter le nom d'utilisateur "Utilisateur".

   Après l'application correcte de la technique, on trouve le mot «olmcckekymv »

01

   b) Proposer une clé pour le cryptage des mots de passe.

   Il suffit de proposer une clé (a, b) sachant que a est premier avec 52 (comme (7, 3), (5, 8),..etc.)

01.5

   c) Crypter le mot de passe "PasseWord" en utilisant la clé (9, 5).

   On doit utiliser les lettres minuscules et majuscules (donc N = 52), le résultat est lié à la manière d'ordonnancement des lettres (minuscules suivis par majuscules, majuscules

01pts

suivis par minuscules ou une lettre majuscule/minuscule suivi par une lettre minuscule/majuscule). Après l'application correcte de la technique on trouve (kfllPvBcG) ou (MHNNRsDEI)

d) Pourquoi on n'applique pas la méthode de VERNAM malgré sa fiabilité?

On n'applique pas la technique de VERNAM parce qu'il est impossible de l'implémenter en utilisant l'informatique moderne vu ses conditions exigées sur la clé.

Bon courage
Dr. Toufik MARIR