Université d'Oum El Bouaghi

Département des Mathématiques et de l'Informatique

Niveau : 03ème Licence SI — Dimanche 18 Octobre 2020

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

Module: Sécurité Informatique

Examen Final – Corrigé Type

1. Définir la sécurité informatique. (01.5)

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

2. Quels sont les objectifs de la sécurité informatique (avec explication) ? (04)

- **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.

3. Parmi les attributs de la sécurité informatique, quel est l'attribut le plus important ? justifier (01.5)

La spécification de l'attribut le plus important est directement liée au système.

4. Expliquer les techniques antivirales. (03)

- **L'analyse de forme** : consiste à détecter la présence d'un virus dans un fichier par des caractères statiques qui permettent de le reconnaître. Cette technique utilise, à titre d'exemple, les signatures (qui sont des suites de bits qui caractérisent un virus donné) ou l'analyse spectrale qui consiste à identifier les virus grâce à la présence d'un ensemble d'instructions rarement existent dans des logiciels ordinaires.
- **Le contrôle d'intégrité** : cette méthode consiste à détecter les modifications anormales d'un fichier. Donc, l'anti-virus calcule pour les fichiers sensibles une empreinte infalsifiable. Ainsi, en cas de modification de contenu de fichier, l'anti-virus peut conclure l'existence d'un virus.

- **L'analyse comportementale** : consiste à identifier le virus grâce à un ensemble d'activités suspects comme : l'accès à la table d'interruption, l'accès à des zones spécifiques de système d'exploitation, la tentative d'écriture dans un fichier exécutable, …etc. Donc, un programme qui essaie d'exécuter l'une de ces actions est probablement un virus.

5. Citer les principes de Kerckhoffs. (03)

- **La méthode est basée sur le secret de la clé, mais pas de l'algorithme**
- **Trouver le message clair sans clé (dans un temps raisonnable) est impossible.**
- **Trouver la clé à partir de message clair et message crypté (dans un temps raisonnable) est impossible.**

6. Comment peut-on connaitre le message clair dans la cryptanalyse à message clair connu. (02)

A partir des parties connues dans le message (comme les en-têtes des documents, les adresses, etc).

7. Comment peut-on utiliser les techniques de cryptage pour assurer les différents objectifs de la sécurité informatique. (03)

On peut utiliser le cryptage pour assurer :

- **La confidentialité : pour lire le message crypté, il faut avoir la clé.**
- **L'intégrité : on ne peut pas changer un message crypté, sauf si on a le décrypté.**
- **Non-répudiation : en utilisant le cryptage a clé publique dont la clé privé est connu seulement par la personne qui a le droit d'envoyer un message. Cette personne ne peut pas dénier de l'envoie d'un message.**

8. Soit le message crypté suivant, sachant que les lettres du message sont de type alphanumérique (les lettres majuscules suivis par les chiffres de 0 – 9)

RFELW8C

Décrypter ce message crypté par la technique ***affine*** avec la clé **(5, 7)**, en utilisant (si nécessaire) les informations suivantes :

	Mod 16	Mod 26	Mod 36	Mod 46
a^{-1}	13	21	29	37
b^{-1}	7	15	31	33

Technique de décryptage : $\mathbf{X = a^{-1} * Y - a^{-1} * b}$ (sachant que $a^{-1} = 29$ et b =7, parce qu'on a 36 caractères).

Après l'application on trouve le message : **COVID19**.

Bon courage !

Dr. Toufik MARIR