|  |  |  |
| --- | --- | --- |
| **Niveau :** 03ème Licence SI |  | Mardi 29 Mai 2018 |
| **Remarque :** Les réponses doivent être brèves, claires et concises | **Durée**: 1h30’ |

**Université d’Oum El Bouaghi**

**Département des Mathématiques et d’Informatique**

**Module : Sécurité Informatique**

**Examen Final - Corrigé Type**

01 Pt

0.75\*3=2.25

1.5

01.25

1. Définir la sécurité informatique.

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

1. Quels sont les attributs de la sécurité informatique qu’on peut assurer par les techniques de cryptage ? Expliquer.

En utilisant les techniques de cryptages on peut assurer les attributs suivants :

* 1. Confidentialité : seules ceux qui possèdent la clé peuvent consulter l’information ;
	2. Intégrité : lorsqu’on crypte l’information, quelqu’un qui n’a pas l’autorisation (clé de décryptage) ne peut pas la modifier.
	3. Non répudiation : en utilisant les technique de cryptage asymétrique avec les principes de signatures numériques, on soit sûr que l’information reçu est de la part de l’émetteur qui possède la clé privé.
1. Quelle est la différence entre la cryptographie, la cryptologie, la cryptanalyse ?
	1. Cryptographie : l’ensemble des procédures qui visent le cryptage des informations.
	2. Cryptanalyse : les techniques qui visent la déduction de texte clair sans utilisation de la clé.
	3. Cryptologie : science de cryptage.
2. Est-ce qu’il existe actuellement des algorithmes de cryptage inconditionnellement sûr ? lesquels ?

Le seul algorithme inconditionnellement sûr connu actuellement est l’algorithme de VERNAM mais il souffre de plusieurs difficultés pour l’implémenter.

1. Expliquer en détaille la technique d’attaque pour cartographie un réseau.

Cette technique à pour objectif de déterminer la topologie d’un réseau. Elle est basée sur la commande **tracert** qui permet des déterminer la route entre la source et la cible (c'est-à-dire les adresses des équipements intermédiaires). Cette commande exploite le protocole ICMP et l’information TTL (Time To Life) existante dans un paquet. Donc, en lançant la commande tracert avec l’adresse de diffusion comme paramètre ça nous permet de récupérer tous les équipements intermédiaires dans le réseau.

1. Expliquer le principe de l’analyse fréquentielle.

02

02

1.5

02

02

4.5

La technique d’analyse fréquentielle est une technique de cryptanalyse basée sur la fréquence d’apparition des lettres dans le message crypté. Généralement, dans chaque langue on trouve des lettres qui apparaissent avec certaine fréquence. Donc on peut identifier les lettres de texte clair en se basant sur cette information.

1. Pensez-vous que l’utilisation des techniques de cryptage seulement peut assurer la sécurité des systèmes informatiques ? Justifier.

Non, parce que le domaine de la sécurité des systèmes informatiques est un domaine pluridisciplinaire. Il faut qu’on ne néglige pas les façades humaines, juridiques et organisationnelles de ce domaine.

1. Crypter la phrase « Je suis un étudiant en Licence Informatique » par la technique de **Vigenère**  en utilisant la clé « ISIL ».

Le message crypté sera « RWAF QKCY MLCO QSVE MFTT KWVN MAVQ WJUL BAYFM»

1. Expliquer en détaille l’opération « subbytes » de la technique AES.

Chaque case d’un bloc de donnée est représentée sous forme de deux chiffres hexadécimaux. Donc le premier chiffre représente la ligne dans un tableau de substitution, alors que le deuxième représente la colonne. On remplace le contenu de cette case par la case correspondante à l’intersection de ligne et colonne identifiées précédemment.

1. Expliquer en détaille les opérations de la technique DES.

 Bon courage !

Dr. Toufik MARIR