|  |  |  |
| --- | --- | --- |
| **Niveau :** 03ème Licence SI |  | Dimanche 28 Mai 2017 |
| **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**

1. Définir la sécurité informatique, la vulnérabilité et la menace.
* ***La sécurité informatique :*** *l’ensemble de* ***moyens*** *mis en œuvre pour* ***minimiser*** *la* ***vulnérabilité*** *d’un système contre les* ***menaces******accidentelles*** *ou* ***intentionnelles****.*
* ***La vulnérabilité*** *est définit comme une* ***faute accidentelle ou intentionnelle*** *introduite dans la spécification, conception ou la configuration d’un système et qui* ***peut être exploité pour créer une intrusion.***
* ***Un attaque*** *est une* ***faute d’interaction malveillante*** *vise à* ***violer une ou plusieurs attributs*** *de la sécurité informatique.*
1. Quelle est la différence entre un algorithme de cryptage inconditionnellement sûr et un algorithme invulnérable par le calcul ?
* *Un algorithme inconditionnellement sûr si peu importe la quantité de texte chiffré dont le cryptanalyste dispose, il ne peut pas décrypter le message. Cependant, un algorithme invulnérable par le calcul si on peut pas décrypter le texte en utilisant les ressources disponibles.*
1. Supposant qu’il existe un logiciel téléchargeable sur le web et qui offre un service important aux utilisateurs. Ce logiciel est d’une source inconnue. Après être installé sur des milliers d’appareils informatiques et à une date spécifique, le logiciel installé commença au cryptage des données des utilisateurs en demandant une rançon. La méthode de cryptage utilisée est DES.
	1. Quel est le type de ce logiciel malveillant ? justifier.
* *Une bombe logique parce que le logiciel est utile mais à un évènement donné, il commence une fonction nuisible.*
	1. Quel est l’attribut de la sécurité informatique visé par cette menace ? justifier.
* *Ce menace vise la disponibilité parce qu’il rend les données indisponibles.*
	1. Est-ce qu’il faisable de trouver la clé de cryptage par une recherche exhaustive ? Justifier.
* *Il est impossible de trouver la clé de cryptage par une recherche exhaustive parce qu’il faut qu’on essaye 256 clés (soit 7,2 \* 1016). A titre d’exemple, si on essaye 1 milliard clé par seconde, il nous faudra presque 2.5 ans.*
	1. Parmi les techniques de cryptanalyse de DES, on cite le précalcul exhaustive. Expliquer le principe de cette technique et calculer l’espace de stockage nécessaire à l’application cette technique.
* Le principe de cette technique consiste à stocker les résultats de cryptage d’un texte connu. Ensuite, il suffit de vérifier si le texte crypté est identique au texte connu crypté. Ainsi, nous identifions la clé de cryptage.
* Pour appliquer cette technique il faut avoir 256 \*64 bits = 536 870 912 GB.
1. En ignorant le critère de la faisabilité technique, quel est l’algorithme de cryptage le plus sûr ? Justifier.
* Cryptage de Vernam parce que la clé est jetable, choisi au hasard avec une taille supérieur à la taille de message.
1. Présenter l’algorithme de cryptage AES en expliquant ses étapes principales.
* Algorithme vu au cours.
1. Les techniques de cryptage symétrique souffrent du problème d’échange de clé. Expliquer une solution à ce problème.
* Algorithme de Déffie-Hellman
1. Plusieurs pays empêchent leurs citoyens d’accéder à certains sites sur Internet. Cependant, les utilisateurs actuellement utilisent les réseaux privés virtuels (VPN) pour accéder à ces sites.
	1. Expliquer une technologie permettant de bloquer des sites spécifiques ?
* Technique de filtrage ou firwalls
	1. Comment peut-on considérer les réseaux privés virtuels une solution à ce problème?
* Basé sur le cryptage des paquets (principe de Tunneling).

 Bon courage !

Dr. Toufik MARIR