TD1 : sécurité informatique

1. Quelle est la différence entre un virus, un ver, et un espion ?

Qu'est-ce qu'un virus ?

Un virus est un programme qui s'accroche à un autre programme ou à un fichier pour se propager et se reproduire à l'insu (en cachette) de l'utilisateur. Normalement, un virus entre dans votre ordinateur par un e-mail de spam avec des pièces jointes (images ou fichiers). Un virus peut endommager des fichiers ou faire en sorte que votre ordinateur affiche un comportement étrange.

Qu'est-ce qu'un ver informatique ?

Il s'agit d'un virus qui se reproduit en se répliquant à travers un réseau de systèmes informatiques. Un ver peut nuire à un réseau, consommer une énorme largeur de bande et éteindre un ordinateur.

Qu'est-ce que le logiciel espion ?

Il s'agit d'un programme pouvant être secrètement accroché à des fichiers que vous téléchargez d'Internet. Dès que le fichier est téléchargé, il s'installe sur votre ordinateur à votre insu et commence à surveiller vos activités sur Internet. Les informations ainsi obtenues sont alors transmises à un tiers, dans la plupart des cas une société intéressée souhaitant créer votre profil personnel. Par la suite, vous recevrez alors des publicités ou d'autres données.

Les trojans : Ce programme utilise la même technique que celle employée par les Grecs pour entrer dans Troie. En effet, il se dissimule dans un logiciel ou un fichier utile qui paraît sain et par la suite il va infecter votre ordinateur afin d'en prendre le contrôle à distance. Cependant contrairement au ver, il ne peut pas se reproduire. Malgré tout, si vous ne détectez pas un cheval de Troie à temps, il fera de votre ordinateur un véritable mort vivant. Voici quelques exemples de ce que peut faire un cheval de Troie.

– Interception de vos mots de passe ainsi que de vos données personnelles
– Prendre possession de votre ordinateur et l'utiliser à des fins malveillantes (spam ou autres…)
– Utilisez votre ordinateur et en faire une arme en attaquant d'autres PC.

2. **Citez trois algorithmes de chiffrement symétriques ? quelle est l'algorithme le plus utilisé actuellement ?**

AES, DES, RC4, RC5. Le plus utilisé est AES

3. Citez trois algorithmes de chiffrement asymétriques ? quelle est l'algorithme le plus utilisé actuellement ?

RSA, El gamal, ECC. Le plus utilisé RSA et ECC.

4. Dans la cryptographie asymétriques chaque entité possède une paire de clés (Kpub_i/ Kpriv_i) avec i : identité de l'entité i.
   a. Expliquez la différence entre ces deux clés ?

Kpub utilisé pour le chiffrement connu pour tout le monde

Kpriv utilisé pour la signature et le déchiffrement connu seulement par son propriétaire

b. Quelle clé j'utilise pour chiffrer un message destiné à R ? Qui peut lire ce message ?

J'utilise la clé publique de R pour chiffrer un message. Seulement R peut lire ce message

c. Quelle clé j'utilise pour signer un message destiné à R ? Qui peut vérifier la signature du message ?

la clé privé de R, j'utilise pour signer un message destiné à R. Tout le monde peut verifier.

5. Expliquez la différence entre : Le **chiffrement de flux** (en anglais *stream cipher*) et Le **chiffrement par bloc** (en anglais *block cipher*) ? (2 points)

Expliquez la différence entre : Le **cryptage symétrique et asymétrique**

La différence fondamentale qui distingue le **cryptage symétrique et asymétrique** est que le **cryptage symétrique** permet le cryptage et le décryptage du message avec la même clé.Tandis que, le **cryptage asymétrique** utilise la clé publique pour le chiffrement et une clé privée pour le déchiffrement.

Table de comparison:

	Cryptage Symétrique	**Cryptage Asymétrique**
Définition	Le cryptage symétrique utilise une seule clé pour le cryptage et le déchiffrement.	Le cryptage asymétrique utilise une clé différente pour le cryptage et le décryptage.
Performance	Le cryptage symétrique est rapide en exécution.	Le cryptage asymétrique est lent à l'exécution en raison de la charge de calcul élevée.
Algorithmes	AES, DES, 3DES et RC4.	Diffie-Hellman, RSA.
Objectif	Le cryptage symétrique est utilisé pour la transmission de données en masse.	Le cryptage asymétrique est souvent utilisé pour l'échange de clés secrètes.

Différences clés entre le chiffrement symétrique et asymétrique

- Le **cryptage symétrique** utilise toujours une seule clé pour le cryptage et le décryptage du message. Cependant, dans le cryptage asymétrique, l'expéditeur utilise la clé publique pour le cryptage et la clé privée pour le déchiffrement.
- L'exécution d'algorithmes de **cryptage asymétrique** est plus lente par rapport à l'algorithme de **cryptage symétrique**. C'est parce que les algorithmes de **cryptage asymétriqu**e sont plus complexes et ont la charge de calcul élevée.
- Les algorithmes de **cryptage symétrique** les plus couramment utilisés sont DES, 3DES, AES et RC4. Tandis que, Diffie-Hellman et RSA représentent l'algorithme le plus commun utilisé pour le **cryptage asymétrique**.
- Le **cryptage asymétrique** est généralement utilisé pour l'échange de clés secrètes alors que le **cryptage symétrique** est utilisé pour échanger une masse de données.

6. Ver vs virus :

Ce qui différencie les **vers** des **virus** informatiques, c'est que les **virus** nécessitent un programme hôte actif ou un système d'exploitation actif et déjà infecté pour s'exécuter, causer des dommages et infecter d'autres fichiers exécutables ou documents, tandis que les **vers** sont des logiciels malveillants autonomes