| Université M’hamed Bougara Boumerdès / Faculté des Sciences / Département d’Informatique |
| --- |
| **Module :** Sécurité informatique **Niveau :** L3 SI/ISIL (S6) **Date :** 15.07.2021  **Examen :** ETLD **Documents :** non autorisés **Durée :** 1h00 |

Matricule : Nom : Prénom : Groupe :

**Questions de cours (10 points)** : Cochez la ou les bonnes réponses

1. Une méthode de signature numérique :

* Permet d’envoyer la clé à son interlocuteur pour que celui-ci puisse décrypter les données
* Permet de hacher les données en plus du chiffrement
* Est utilisée pour assurer la non répudiation des messages
* Peut être utilisée dans les certificats numériques

**2**. Un certificat numérique permet de :

* S’assurer de la clé publique du destinataire
* S’assurer de la clé publique de la source
* S’assurer que le message n’a pas été modifié
* S’assurer qu’un client communique avec le bon serveur

**3**. La politique de sécurité permet de :

* Protéger les actifs selon leurs importances
* De répondre aux incidents de sécurité selon leur fréquence et coût
* Préparer une analyse de situation
* Faire des audits de sécurité.

**4.** La non répudiation est :

* Un principe qui permet de garder la trace de qui a fait quoi
* Un principe qui permet de garder la vie privée des personnes
* Un principe qui utilise les signatures numériques
* Un principe qui utilise la cryptographie hybride

**5.** Une attaque par statistique pour casser une clé de chiffrement :

* Teste tous les cas possibles
* Analyse la fréquence d’apparition des lettres du texte chiffré
* Fait correspondre les fréquences des lettres d’une langue avec celles du texte à déchiffrer
* Utilise la force brute

**6.** Les fonctions de hachage sont utilisées pour

* Les certificats numériques
* Stocker les mots de passes dans des bases de données
* Assurer la confidentialité des messages
* Assurer l’intégrité des messages

**7.** Pour un système informatique, en quoi consiste la procédure d'authentification d'un utilisateur

* Vérifier l'identité de l'utilisateur avant de lui donner accès à des ressources
* Demander à l'utilisateur d'entrer son mot de passe à intervalles réguliers au cours de sa session.
* Établir une correspondance entre le pseudo entré par l'utilisateur et son véritable nom
* Demander d'entrer une seconde fois son mot de passe à l'utilisateur qui souhaite en changer
* Garder la trace de la visite de l'utilisateur sur le système (identifiant, dates de connexion, ...)

**8**. L’inconvénient de la cryptographie symétrique est :

* Le temps de calcul
* L’espace de stockage des clés
* La difficulté de partager un secret
* La vulnérabilité aux attaques classiques

**9**. Une autorité de certification est utilisée :

* Pour délivrer des certificats numériques
* Pour délivrer des clés de sessions
* Pour associer une personne à une clé privée
* Pour associer une personne à une clé publique

**10**. L’analyse de situation (ou du contexte) dans le processus de sécurisation d’un système d’information permet de :

* Définir le périmètre de sécurité
* Analyser le risque de sécurité
* Installer les logiciels antivirus
* Essayer certaines attaques sur le système

**Exercice 01** **(5 points):**

La cryptographie hybride est un système de cryptographie faisant appel aux deux grandes familles de systèmes cryptographiques : la cryptographie asymétrique et la cryptographie symétrique.

1. Donner le schéma général caractérisant la cryptographie hybride.
2. Comment profite ce schéma des avantages de la cryptographie symétrique et asymétrique ?

**=================== Choisir l’exercice 02 OU l’exercice 03 ======================**

**Exercice 02** **(5 points):**

Considérons un chiffrement de César où l'alphabet est constitué des dix premières lettres de l'alphabet français, c'est-à-dire les lettres de ***A*** à ***J***.

1. Chiffrer le Message M = **ACIDE**, sachant que la clé = **G**.

**fiche**

1. Qu’est est le nombre de clés possibles dans ce chiffrement de César ?

Considérons un chiffrement de Vigenère avec le même alphabet (de ***A*** à ***J***).

1. Déchiffrer le Message ***C*** = **GGEIC**, sachant que la clé = **BIC**.
2. Supposons que la taille de la clé du déchiffrement du message ***C*** est inconnue. Quel est le nombre maximal de combinaisons possibles qu’un cryptanalyste aura à essayer pour trouver la clé? Justifier.

**Exercice 03** **(5 points):**

Le système d’information regroupe l’ensemble des moyens humains, techniques et organisationnels visant à assurer le traitement, le stockage et l’échange d’informations nécessaires aux activités d’une entreprise.

1. Quelle est la démarche à suivre par un RSSI (Responsable de la sécurité informatique) pour sécuriser un système d’information ? Expliquer.