Université Badji Mokhtar Annaba
Département d'informatique

Licence **Module :** Sécurité informatique
Semestre : 06 **Durée :** 1H 00

Nom (en Majuscule svp**):** ……. **Prénom :** ……. **Groupe :** ……..

Micro interrogation

Documents non autorisés, Clarté de la copie exigée
Important : une ou plusieurs des propositions de réponse sont correctes

Exercice 1 : (06 points)

1) Quel service de sécurité informatique est chargé de garantir que les utilisateurs sont véritablement qui ils prétendent être avant de leur permettre l'accès aux ressources système ou aux données sensibles ?
   a. Disponibilité
   b. Authentification
   c. Intégrité
   d. Non-répudiation
2) Quel type d'attaque vise à perturber la disponibilité d'un service en submergeant sa capacité à répondre aux demandes légitimes avec un trafic excessif provenant de multiples sources ?
   a. Attaque par phishing
   b. Attaque par force brute
   c. Attaque DDoS
   d. Injection SQL
3) Quel mesure de sécurité informatique est principalement utilisé pour détecter et prévenir les attaques en temps réel sur un réseau ?
   a. Firewall
   b. Antivirus
   c. IDS (Intrusion Detection System)
   d. VPN (Virtual Private Network)
4) Quelle méthode de chiffrement classique consiste à déplacer chaque lettre du texte clair d'un certain nombre de positions dans l'alphabet, comme dans le chiffre de César ?
   a. Chiffrement par transposition
   b. Chiffrement à clé publique
   c. Chiffrement par substitution
   d. Chiffrement à clé secrète
5) Dans la cryptographie asymétrique, le chiffrement se fait avec :
   a. La clé publique de l'émetteur
   b. La clé publique de la destination
   c. La clé privée de l'émetteur
   d. La clé privée de la destination
6) Quel concept de sécurité informatique permet de vérifier l'intégrité et la non-répudiation d'un message ou d'un document électronique ?
   a. La signature numérique
   b. Les certificats numériques
   c. La cryptographie asymétrique
   d. L'autorité de certification
7) La méthode de Hashage génère :
   a. Une empreinte dont la taille dépend de la donnée en entrée.
   b. Une clé privée.
   c. Un condensat (hash) de taille fixe.

8) La signature numérique consiste en :
   a. Condensat (hash) du message chiffré avec la clé privée de la destination.
   b. Condensat (hash) du message chiffré avec la clé privée de la source.
   c. Condensat (hash) du message chiffré avec la clé publique de la source.
   d. Condensat (hash) du message chiffré avec la clé publique de la destination.

9) Le certificat numérique contient ***(plus d'une réponse)***:
   a. La clé publique de l'autorité de certification
   b. La clé publique du propriétaire du certificat
   c. La clé privée de l'autorité de certification
   d. La signature du certificat

10) Un certificat numérique est signé avec :
   a. La clé publique du possesseur du certificat
   b. La clé privée du possesseur du certificat
   c. La clé publique de l'autorité de certification
   d. La clé privée de l'autorité de certification

11) Pour vérifier la validité d'un certificat électronique on doit vérifier
   a. Uniquement la date de validité
   b. Uniquement la signature du certificat
   c. La date de validité et la signature du certificat
   d. La clé publique

Exercice 2 (06 points): Déchiffrement par Transposition

Cryptogramme à Déchiffrer : "ARGDCSPTAPSIEEHV"
Clé de Transposition : "31425"
Déchiffrez le cryptogramme en utilisant la clé de transposition donnée.

M= PAS DE TRICHAGE SVP

Matrice

Exercice 3 (8 points) : RSA

Bob choisit comme nombre premier p = 17 et q = 19.
Alice et lui se fixent un protocole RSA dans lequel les messages sont des nombres en base 10 que l'on code par bloc de 2 chiffres.
Alice veut envoyer le message "46 27 39".

1. Donnez la clé publique de Bob : (N, e) : (323, 5)
2. Donnez la clé secrète d de Bob : (N, d) : (323, 173) « Veuillez regarder la vidéo que j'ai envoyée pour calculer D»
3. Ecrivez le message chiffré qu'Alice envoie à Bob.

$46^{5} \bmod 323 = 88$
$27^{5} \bmod 323 = 278$
$39^{5} \bmod 323 = 286$

4. Déchiffrez le message qu'a reçu Bob et vérifiez que c'est bien celui qu'a envoyé Alice.

$88^{173} \bmod 323 = 46$
$278^{173} \bmod 323 = 27$
$286^{173} \bmod 323 = 39$