UNIVERSITE DE ZIGUINCHOR

♦◊♦♦◊♦♦◊♦◊♦

UFR Sciences et Techniques

♦◊♦♦◊♦

DÉPARTEMENT D'INFORMATIQUE

Master 1 Informatique: Option Réseaux & Systèmes

♦◊♦♦◊♦

Année 2020-2021

Nom:.....

Prénom:.....

N° C.E:.....

Examen de : Sécurité des Réseaux

durée 2h00mn)

Documents non autorisés

Questions : ***(10 points)***

1) Donner l'ordre d'exécution des quatre étapes suivantes relatives à l'analyse et la gestion des risques:
   a. Apporter une réponse face au risque,
   b. Evaluer le Risque
   c. Identifier le risque
   d. Suivre le risque
2) Quels sont trois objectifs (ou service de sécurité) majeurs de la sécurité informatique
3) Quel peut être l'objectif d'un hacker au chapeau blanc ?
4) Avec le chiffrement de César par décalage de 3 lettres (la clé égale à 3), un texte chiffré C (ou cryptogramme) donne AZUC.
   a. Quel est le texte clair correspondant ?
   b. Donner une formule mathématique F permettant de trouver la position d'une lettre du texte chiffré en fonction de la position i d'une lettre du texte claire ?
5) Sur un système d'exploitation OS1, lors de la création des comptes, les mots de passe des utilisateurs sont stockés après application d'une fonction de hachage, alors que le OS2 les stocke directement. Donner un exemple d'attaques sur l'OS1 et auquel l'OS2 est épargné?
6) Un ordinateur est connecté à Internet via un point d'accès wifi, donner un exemple d':
   a. une de ses vulnérabilités
   b. un des risques encourus
   c. une des attaques auxquelles il est exposé
   d. une contre-mesure pour contrecarrer l'attaque correspondante
7) On considère un système de chiffrement par Vigenère utilisant la clé K= MRS. Trouvez la clé de déchiffrement K^{-1}.
8) On considère les systèmes de chiffrement suivants sur des lettres alphabétiques où la robustesse est mesurée en fonction du nombre maximum de clés possibles :
   a. Un système de chiffrement utilisant la méthode de César.
   b. Un système de chiffrement utilisant la substitution mono-alphabétique.
   c. Un système de chiffrement utilisant une clé de transposition de 6 lettres.
   d. Un système de chiffrement utilisant une clé de Vigenère de 5 lettres.

   Remplir le tableau suivant :

Cryptosystèmes	Nombre maximum de clés
César	
Mono-alphabétique	
Transposition à 6 lettres	
Vigenère à 5 lettres	

   Lequel est plus robuste ?

9) Expliquer une faille de sécurité ou vulnérabilité dans le cryptosystème EBC qu'on ne retrouve pas de CBC ? Il est permis de justifier la réponse par un exemple.

Répondre sur l'épreuve aux questions suivantes, une question peut avoir une seule ou plusieurs réponses. ***(10 points)***

1) Quel objectif de sécurité signifie que les actifs du système informatique ne peuvent être modifiés que par des parties autorisées
    a. Authenticité
    b. Confidentialité
    c. Intégrité
    d. Disponibilité
    e. Contrôle d'accès
2) **Amadou** chiffre un message avec sa clé publique et l'envoie à **Blaise**, lequel des objectifs de sécurité est atteint ?
    a. Authenticité
    b. Confidentialité
    c. Intégrité
    d. La disponibilité
    e. Le contrôle d'accès
3) Lequel des algorithmes est asymétrique
    a. Blowfish en mode CBC
    b. Chiffrement de César
    c. RSA
    d. MD5
    e. Blowfish en mode OFB
    f. AES
4) Par quel mécanisme de sécurité peut on réaliser l'intégrité?
    a. Le chiffrement
    b. Le déchiffrement
    c. Le hachage
    d. Blowfish en mode CBC
5) Quel(s) énoncé(s) sont vrais pour le protocole https?
    a. Il utilise la cryptographie symétrique uniquement
    b. Il utilise la cryptographie asymétrique uniquement
    c. Il utilise la cryptographie symétrique et asymétrique
    d. Il n'utilise pas de cryptographie
    e. C'est un protocole sécurisé
6) Quel(s) énoncé(s) sont vrais pour le protocole http?
    a. Il utilise la cryptographie symétrique uniquement
    b. Il utilise la cryptographie asymétrique uniquement
    c. Il utilise la cryptographie symétrique et asymétrique
    d. Il n'utilise pas de cryptographie
    e. C'est un protocole non sécurisé
7) Lesquelles des propositions décrivent le chiffrement symétrique ?

a. Le chiffrement est très rapide
b. Il est facile de partager les clés
c. Deux clés différentes son utilisées pour le chiffrement et le déchiffrement
d. Une seule clé est utilisée pour le chiffrement et le déchiffrement
e. Il est généralement utilisé pour chiffrer des clés privées

8) Lesquelles des propositions décrivent le chiffrement symétrique ?
   a. Le chiffrement est très rapide
   b. Il est facile de partager les clés
   c. Deux clés différentes son utilisées pour le chiffrement et le déchiffrement
   d. Une seule clé est utilisée pour le chiffrement et le déchiffrement
   e. Il est généralement utilisé pour chiffrer des symétriques
9) Un certificat numérique permet de garantir
   a. L'authenticité de la clé symétrique
   b. L'authenticité de la clé privée
   c. L'authenticité de la clé publique
   d. L'intégrité des données
   e. La confidentialité des données