Master 1 R&S
♦◊♦♦◊♦
Année 2021-2022

Université Assane Seck de Ziguinchor

♦◊♦♦◊♦♦◊♦◊♦
UFR Sciences & Technologies
♦◊♦♦◊♦
Département d'Informatique

Nom:.....
Prénom:.....
N° C.E:.....

Examen de rattrapage : Introduction à la Sécurité

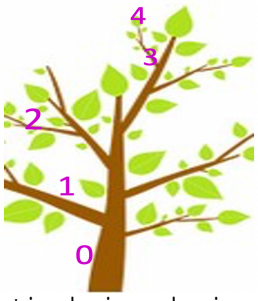
durée 2h00mn)
Documents non autorisés

Questions : (12 points)

1) Pour analyser un risque on le quantifie avec les valeurs : l'occurrence, la gravité et la criticité.

Exemple : on se fixe comme objectif de grimper sur l'arbre dont le schéma est donner ci-après :

- la vulnérabilité est relative à la fragilité des branches
- La menace est de tomber
- Le risque encouru est de se casser un membre ou de succomber à ses blessures



Faire la matrice de niveau des risques et y placer les risque 0, 1, 2, 3 et 4 **(2 points)**

2) Pour chacun des services de sécurité suivant, citer un mécanisme de sécurité permettant de le mettre en œuvre : l'authentification, la confidentialité et l'intégrité. **(2 points)**

3) Avec le chiffrement par transposition utilisant la clé K=[3-1-4-2], un texte chiffré C (ou cryptogramme) donne AZUC.
   a. Quel est le texte clair correspondant ?
   b. Donner la clé inverse K^{-1} permettant de déchiffrer. *(2 points)*

4) Analyser et trouver les propriétés (services ou objectifs de sécurité) que comporte ce protocole suivant sachant que : pkA et pkB sont respectivement les clés publiques de A et B ; prkA et prkB les clés privées de A et B ; Kab une clé symétrique à partager entre A et B et **m** un message. *(2 points)*

A ⟶ B : {Na.A}pkB.
B ⟶ A : {Na.Nb}pkA.
A ⟶ B : {Nb,Kab}pkB
B ⟶ A : {**m**}Kab

XLY

5) On considère un système de chiffrement par Vigenère utilisant la clé K=BNA. Trouvez la clé de déchiffrement K^{-1}. *(2 points)*

6) On considère les systèmes de chiffrement suivants sur des lettres alphabétiques où la robustesse est mesurée en fonction du nombre maximum de clés possibles : *(2points)*
   a. Un système de chiffrement utilisant la méthode de César avec un décalage de 3.
   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 6 lettres.

   Remplir le tableau suivant :

Crypto-systèmes	Nombre maximum de clés
César	
Mono-alphabétique	
Transposition à 6 lettres	
Vigenère à 6 lettres	

7) Quelle faiblesse trouve-t-on sur CBC avec vecteur d'initialisation constante qu'on ne retrouve pas dans CBC avec vecteur d'initialisation variable ? *(1 points)*

Nom:.....
Prénom:.....
N° C.E:.....

Répondre sur l'épreuve aux questions suivantes, une question peut avoir une ou plusieurs réponses. (8 points)

1) Quel objectif de sécurité signifie que l'entité communicante (avec laquelle on communique) est bien celle qu'elle prétend être.
    a. Authenticité
    b. Confidentialité.
    c. Intégrité.
    d. Disponibilité
    e. Contrôle d'accès
2) **Amadou** chiffre un message avec la clé publique de **Blaise** et l'envoie à Cheikh, lequel des services de sécurité est atteint ?
    a. Authenticité.
    b. Confidentialité
    c. Intégrité
    d. La disponibilité
    e. Le contrôle d'accès
    f. Aucun
3) Le(s)quel(s) des algorithmes est/sont asymétrique(s)
    a. Blowfish en mode CBC.
    b. EL-Gammal
    c. RSA
    d. MD5
    e. Blowfish en mode OFB.
    f. Diffie-Hellman
    g. Blowfish en mode CBC
4) 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.
5) Lesquelles des propositions décrivent le chiffrement symétrique ?
    a. Le chiffrement est très rapide.
    b. Il est facile de partager la clé
    c. Une seule clé est utilisée pour le chiffrement et le déchiffrement.
    d. Il est généralement utilisé pour chiffrer des clés symétriques.
6) Lesquelles des propositions décrivent le chiffrement asymétrique ?
    a. Le chiffrement est très rapide
    b. Il est facile de partager les clés.
    c. Une seule clé est utilisée pour le chiffrement et le déchiffrement
    d. Il est généralement utilisé pour chiffrer des clés symétriques.
7) 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