Université de M'sila
Faculté des MI
Département d'informatique
Niveau: *3ème Année Licence*

Dimanche 13/05/2024
Durée: 1h30min
Module : *Sécurité Informatique*

Nom : ……..…….. Prénom : ……..…… Spécialité: ….… Groupe: ……

Corrigé-type de l'examen du Semestre

Exercice N°01 (0.5*12=6 pts): *Q*uestions à *C*hoix *M*ultiple (Correcte: +0.5 ; Sans réponse : 0)

1. **RSA développent les algorithmes suivants**
   - Algorithme de chiffrement
   - Algorithme de signature
   - Protocole d'échange de clés
   a. Algorithme d'encapsulation
2. **« Un pirate bombarde un serveur de BD par des requêtes sans arrêt ». Le service touché est :**
   a. Confidentialité
   b. Intégrité
   c. Authentification
   d. Disponibilité
3. **Dans la signature RSA, le récepteur utilise:**
   a. Sa clé privée.
   b. Sa clé publique.
   c. La clé publique de l'émetteur.
   d. La clé privée de l'émetteur.
4. **Lesquelles des algorithmes suivants sont des algorithmes de chiffrement asymétriques?**
   a. AES
   b. DSA
   c. Affine
   d. RSA
5. **Soit une fonction HMAK basée sur SHA-1. la taille de son empreinte est:**
   a. 256 bits
   b. 160 bits
   c. 128 bits
   d. Selon la taille de la clé K.
6. **Soient 5 entité utilisent le chiffrement symétrique pour transmettre des données. Quel est le nombre minimal de clés symétriques nécessaires ?**
   a. 5 b. 10
   b. c. 15 c. 20
7. **Le chiffrement symétrique**
   a. Garantie la confidentialité du message chiffré
   b. Utilise une paire de clés publique/privée
   c. Assure la non-répudiation.
   d. Repose sur la confidentialité de la clé utilisée
   e. Repose sur la confidentialité de l'algorithme de chiffrement utilisé.
8. **Pour calculer la clé de la signature de RSA, on utilise:**
   a. Algorithme d'Euclide étendu.
   b. Algorithme de factorisation.
   c. Théorème des restes chinois.
   d. Pas de réponse correcte.
9. **Avec la signature numérique, on assure:**
   a. La confidentialité
   b. L'intégrité
   c. L'authentification
   d. Non-répudiation
10. **L'algorithme qui utilise le schéma de Feistel est :**
    a. AES
    b. DES
    c. RSA
    d. RC4
11. **L'avantage de chiffrement asymétrique:**
    a. Il est très rapide.
    b. Il n'y a pas besoin de s'échanger de clé secrète
    c. Il possède des petites clés.
12. **Les moyens de protection contre spyware:**
    a. anti-spyware b. pare-feu personnel
    c. anti-spam d. IPSec

Exercice N°02 (06 pts): Chiffrement classique

Chiffrement par décalage : Supposons que un pirate ait intercepte le message suivant (sans espaces ni signes de ponctuation):

ALWLDETYPHTWWMPQCPPGPCJDZZY

1) Calculer le nombre d'occurrences de chacune des lettres de l'alphabet dans ce message.

P =5, W=3, L=2, D=2, T=2, Y=2, C=2, Z=2, A=1, E=1, H=1, M=1, Q=1, G=1, J=1 **(1 pt)**

2) Trouver la clé de déchiffrement.

Correspondance entre E et P ➔ 15-4= 11 **(0.5 pt)**

La clé est 11 (la lettre L)

3) Déchiffrer le texte chiffré avec l'algorithme par décalage. (on dessine la table de déchiffrement)

PALASTINE WILL BE FREE VERY SOON **(1 pt)**

Chiffrement Affine: Soit la clé de chiffrement de l'algorithme Affine K= (a, b), tel que a=7 et $b=11^{-1}$ mod 26.

4) Ecrire la fonction de chiffrement et la fonction de déchiffrement.

Tout d'abord, on calcule la valeur de $b = 11^{-1}$ mod 26 = 19 (par l'algorithme euclidien étendu) **(0.5 pt)**

$E(m)= 7m+19 \bmod 26$ **(0.5 pt)**

$D(c)= 7^{-1}(c-19) \bmod 26$ **(0.5 pt)**

On a $7^{-1} \bmod 26 = 15$

Donc $D(c)= 15(c-19) \bmod 26$ **(0.5 pt)**

5) Chiffrer le message M= «**SECURITE**» avec la clé K= (a, b)

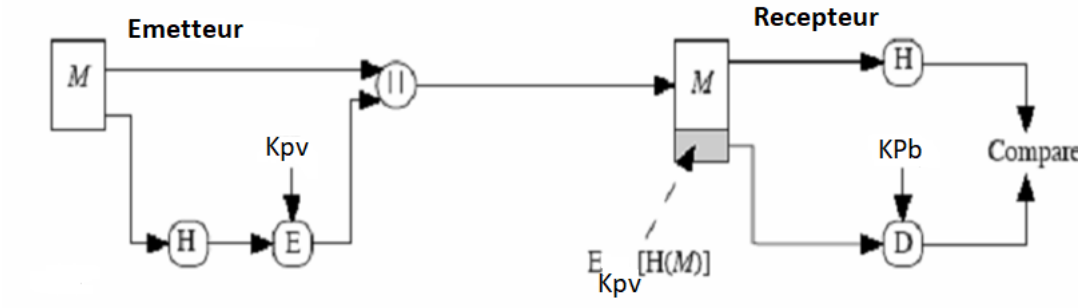
K=(7,19)

C= PVHDIXWV **(1 pt)**

6) Quel est le nombre des clés possibles ? et Pourquoi ?

Nombre clé possible est= 12*26= 312 **(0.25 pt)**. La variable a est premier avec 26 (PGCD (a, 26)=1) est une condition nécessaire et suffisance pour chiffrer un texte. **(0.25 pt)**

Exercice N°03 (4 pts):



Soient Kpv et Kpb les clés privées et publique de l'émetteur, respectivement.

1) Ecrire formellement le message émis $M||E_{Kpv}(H(M))$ **(0.5 pt)**

2) Expliquer brièvement le processus exécuté par le récepteur. **(1 pt)**

- Il déchiffre $E_{Kpv}(H(M))$ par la clé publique de destinataire.
- Il calcule H(M) à partir de message M reçu.

- Il compare H(M) calcule est H(M) obtenu. Si elles sont égales, alors la signature est authentique.

3) Quelles sont propriétés de sécurités validées par ce schéma? Intégrité, authentification, non-répudiation, **(0.75 pt)**

4) Que système cryptographique représente ce schéma ? signature numérique **(0.5 pt)** parce que H(M) est chiffré par la clé privée de l'émetteur. le message est envoyé clairement avec sa signature numérique

1) Quel est le type de la fonction de hachage utilisée? MDC (*fonction de hachage sécuritaire sans clé*) **(0.5 pt)**

5) Est-ce que la fonction SHA-1 est sûre ? et pourquoi ? Non **(0.25 pt)**, car les chercheurs découvert que cette fonction ne résiste pas la collision. **(0.5 pt)**

Exercice N°04 (04 pts):

1. A quoi sert l'échange de clefs de Diffie et Hellman et pourquoi joue-t-il un rôle central en cryptographie? **(0.5 pt)**
   L'échange de clefs permet, à partir d'un couple (clef publique, clef privée) pour *A* et *B* d'obtenir une clé de session *K* commune pour que *A* et *B* puissent communiquer par un réseau non sure sans que la clef *K* soit jamais transmise sur ce réseau. On utilise la cryptographie asymétrique pour cet échange de clé, la clé *K* sert ensuite à faire de la cryptographie symétrique entre *A* et *B*.

2. Sur quel(s) problème(s) difficile(s) est basé le protocole Diffie-Hellman ?
   Problème de logarithme discret **(0.5 pt)**
3. Présenter un scenario d'attaque pour la version de base de Diffie-Hellman. (Voir le cours) **(1 pt)**
4. Si on veut utiliser le système de chiffrement AES-256 pour chiffrer les messages par la clé de session générée, quelle est la meilleure solution proposée pour réduire la taille de la clé de session? SHA-256