Université de M'sila
Faculté des MI
Département d'informatique *Dimanche 29/05/2022*
Niveau: *3ème Année Licence* *Durée: 1h30min*
Module : *Sécurité Informatique*

Examen du Semestre – Corrigé type

Important: Dans les exercices 2, 3 et 4, la justification des réponses est obligatoire.

Exercice N°01 (06 points):

1. Pour envoyer un message chiffré en utilisant le chiffrement asymétrique, on utilise:
   a. Ma clé publique
   b. Ma clé privée
   a. La clé publique de destinataire
   b. La clé privée de destinataire
2. Quand une technique assure l'authentification, elle assure automatiquement l'intégrité:
   a. Oui.
   b. Non
3. Dans l'algorithme AES-128:
   a. Nb= 4, Nr= 8
   b. Nb= 6, Nr= 10
   c. Nb= 4, Nr= 10
   d. Nb= 6, Nr= 12
4. Le chiffrement par flot peut être utilisé pour assure les communications suivantes:
   a. Internet.
   b. Wi-Fi.
   c. GSM.
   d. Bluetooth.
5. Lesquelles des algorithmes suivants sont des algorithmes de chiffrement symétriques?
   a. AES
   b. RSA
   c. DES
   d. SHA-1
6. Dans l'opération de chiffrement avec l'algorithme AES, on utilise les transformations suivantes:
   a. SubBytes
   b. SubRows
   c. ShiftRows
   d. InvSubBytes
7. Un attaquant réussi à utiliser la carte bancaire d'une personne et se fait payer mobile sur un site web de e-commerce. Le service de sécurité touché est:
   a. Confidentialité
   b. Intégrité
   c. Authentification
   d. Disponibilité
8. Les conditions de choisir la clé publique e de chiffrement ESA sont:
   a. $1 \leq e \leq \varphi(N)$,
   b. PGCD(e, $\varphi(N)$)=1
   c. PGCD(e,N)=1
   d. Pas de réponse correcte
9. Un cheval de Troie peut:
   a. voler des mots de passe
   b. copier des données sensibles
   c. arrêter le pare-feu
   d. faire déni le service
10. Les avantages de chiffrement symétrique sont:
    a. Il est plus rapide.
    b. Il utilise des petites clés.
    c. Faciliter de distribution des clés.
    d. Il est lent à l'exécution.
11. La méthode de cryptanalyse qui utilisé pour casser le chiffrement de Vigenère a été découverte par:
    a. Al-Kindi
    b. Blaise de Vigenère
    c. Charles Babbage
    d. Vincent Rijmen
12. Résistance à la collision signifie:
    a. Étant donné x et H(x), il est dur de trouver $x \neq y$ vérifiant (x)=H(y).
    b. Il est difficile de trouver deux entrées différentes x et x' tel que : h (x) = h (x').
    c. Étant donné y il est difficile de trouver x, tel que y=h(x)

Exercice N°02 (06 points): Chiffrement classique

1) Déchiffrer le message «**ERGFIPCMRI**» en utilisant le chiffrement de Vigenère avec la clé: **KEY**.
On utilise la table de déchiffrement.
On trouve le texte clair suivant: **UNIVERSITY** **(1.5 pt)**

2) Ecrire un pseudo-code de la fonction de déchiffrement pour le chiffrement Affine. **(1 pt)**

```
int a,b
char c[]
l = length(c);
for (i:=0; i< l; i=i+1 )
p[i]= indtolettre ( invmod(a) *(lettretoind (c[i]) – b + 26 ) % 26)
```

3) Déchiffrer le message " **FWLPSMP** " avec le chiffrement Affine en utilisant la clé.
La fonction de déchiffrement: $11^{-1}(y-5) \bmod 26 = 19(y-5) \bmod 26$ **(0.5 pt)**
On utilise la table pour calculer le texte clair: ALKINDI **(1 pt)**

4) Enumérer toutes les valeurs possibles de "a" (une partie de la clé) dans le chiffrement Affine. **(1 pt)**
Tous les éléments de Z26 non divisibles par 2 et 13 sont premiers avec 26.
a ={1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25}

5) Quelles sont les différences entre le chiffrement classique et moderne? **(1 pt)**
Classique: Utiliser les lettres de la langue, symétrique seulement, applications limitées
Moderne: Utiliser le langage binaire, tous les types de données, symétrique et asymétrique, plusieurs applications.

Exercice N°03 (03 points): Chiffrement symétrique

1) Ecrire les fonctions de chiffrement et de déchiffrement de mode EBC. **(1 pt)**
Ci = E(Pi)
Ci = D(Ci)

2) Soient le message en clair M = 1011000101001 et une clé K = = (f(3)=1, f(2)=3, f(1)= 2) par un décalage à gauche de 1 bit. Chiffrez le message M. **(1 pt)**
On découpe le texte clair en blocs. Nous avons une clé de taille 3 bits, alors la taille du bloc est 3 bits.
P1=101 ➔ C1=011
P2=100 ➔ C2=001
P3=010 ➔ C1=100
P4=100 ➔ C1=001
P5=100 ➔ C1=001 (ajouter deux bits dans les bits de poids faible (LSB) de valeur 0)
Alors le texte chiffré est: 011001100001001

3) Quel est l'inconvénient de ce mode. **(1 pt)**
Le problème de reconnaitre du message en clair dans celui chiffré. i.e. les fragments répétés dans le texte en clair ne sont pas masqués.

Exercice N°04 (05 points): Chiffrement asymétrique

1) En utilisant l'algorithme de chiffrement RSA:
- Montrer que D(E(m)) = m. **(1 pt)**

$D(E(m))= D(m^e \bmod n)= (m^e)^d \bmod n= m^{ed} \bmod n$
sachant que $ed= 1 \bmod \Phi(n) = k\Phi(n)+1$

alors $D(E(m))= m^{k\Phi(n)+1} \bmod n = m$

- Soit N= 91 et e= 11, calculer d.

N=91 & N=pq ➔ alors p=13 & q=7 **(0.5 pt)**

$\Phi(n)= (p-1)(q-1) = 12*6= 72$ **(0.5 pt)**

$ed=1 \bmod \Phi(n)$ ➔ $d= e^{-1} \bmod \Phi(n)$ ➔ $d=11^{-1} \bmod 72$

On utilise l'algorithme d'Euclide étendu pour calculer l'inverse modulaire de $11^{-1} \bmod 72$

Alors, **d=59** **(0.5 pt)**

- Chiffrer le message m=5.

$C= E_{pk}(m)= m^e \bmod N= 5^{11} \bmod 91$ **(0.25 pt)**

$= 73$ **(0.25 pt)**

- Déchiffrer le message c=4.

$m= D_{sk}(c)= c^d \bmod N=4^{59} \bmod 91$ **(0.25 pt)**

= 23 (on utilise l'algorithme d'exponentiation rapide) **(0.25 pt)**

2) À quoi sert l'échange de clés de Diffie et Hellman et pourquoi joue-t-il un rôle central en cryptographie. **(0.5 pt)**

L'échange de clés permet d'obtenir une clé de session K commune à partir d'un couple (clef publique, clef privée). On utilise la cryptographie à clé publique pour cet échange de clé, la clé générée K sert ensuite à faire de la cryptographie symétrique entre A et B.

3) Soit p =17, g= 3 des données globales partagés entre Alice et bob. Alice choisit a= 7, et Bob choisit b= 4. Appliquer ces valeurs pour proposer un scénario d'attaque sur le protocole de Diffie-Hellman. **(1 pt)**

$A= g^a \bmod p = 3^7 \bmod 17 = 11$

$B= g^b \bmod p = 3^4 \bmod 17 = 13$

L'attaquant génère un nombre c=2 et calcule $C= 3^2 \bmod 17 = 9$.

La clé de session de côté A est: $K=B^a \bmod p = 13^7 \bmod 17= 4$

La clé de session de côté B est: $K=C^b \bmod p = 9^4 \bmod 17 = 16$

Alors, les clés générées par les deux entités sont différentes.