SUJET REVISION SECURITE

BELFODIL AYMEN

EXERCICE 1 (8 PTS):

Soit l'annuaire des clés publiques suivant :

Entité	Clé publique (e , n)
Bob	(**x** , 33)
Alice	(17 , 33)

1. x peut-il être égale à 8 ? justifier **(1 pts)**

Note : Dans ce qui suit $x = 3$.

PARTIE 1 : CHIFFREMENT RSA (4 PTS)

Oscar est entrai d'écouter le canal, a un instant t il reçoit le message $M = 5$ se dirigeant vers **Alice**.

1. Déterminer le message clair (**3 pts)**
2. Où réside-t-elle la complexité de l'algorithme **RSA** ? (**1 pts)**

PARTIE 2 : SIGNATURE RSA (4 PTS)

1. Rappeler le fonctionnement de la signature **RSA**. (**0.5 pts)**
2. **Bob** a pour clé privé $d = 7$. Vérifier que ce choix convient. (**0.5 pts)**
3. **Bob** signe le message $m = 30$ par la signature $\sigma = 24$. Vérifier que cette signature est correcte (**2 pts)**

EXERCICE 2 (6 PTS):

I. Deux personnes **Alice** et **Bob** désirent échanger **une clé de session**, pour cela ils utilisent **l'algorithme d'échange de deffie Hellman**

1. Rappeler le schéma d'échange **(1 pts)**
2. Quelle sont les informations que peut récupérer **Oscar** ? (**1 pts)**
3. On suppose que le générateur $g = 16$ et $p = 157$ et que **Alice** génère le nombre aléatoire $a = 4$ et **Bob** génère le nombre aléatoire $b = 79$.
    a. calculer la clé de session (**1 pts)**.

II. On utilise maintenant **El-Gamal**

1. Rappeler le schéma d'envoi d'un message m de **Bob** vers **Alice** (**1 pts)**
2. On suppose que le générateur $g = 16$ et $p = 157$ et que **Alice** génère le nombre aléatoire $a = 4$ et **Bob** génère le nombre aléatoire $b = 79$, et **Bob** désire communiquer le message $m = 100$. **Décrire tout le processus** (calculer les valeurs intermédiaire). (**2 pts)**

EXERCICE 3 (3 PTS):

Note : La clé publique RSA est (e, n), la clé privé est (d, n)

PARTIE 1 : SIGNATURE RSA SANS HACHAGE

Alice envoie à **Bob** deux couples (message, signature) : (m_1, σ_1) et (m_2, σ_2).
Montrer qu'**Oscar** (en récupérant ses deux couples) peut construire une signature valide σ du message $m1 * m2$ **(1 pts)**

PARTIE 2 : SIGNATURE RSA AVEC HACHAGE

Alice envoie à **Bob** un couple (message, signature) : (m, σ).

1. Donner σ en fonction du haché du message $H(m)$, d et n **(1 pts)**
2. On suppose que H n'est pas résistante à la seconde pré-image. **Oscar** récupère la signature valide σ d'un message m. Montrer comment Oscar peut construire une signature valide pour un message différent de m. **(1 pts)**

EXERCICE 4 (3 PTS)

1. Donner les propriétés que doit satisfaire une fonction d'hachage ? **(1 pts)**
2. Expliquer brièvement l'algorithme d'hachage MD5 **(2 pts)**