INFO3 -2023/2024
Module : Administration des systèmes
Prof : Samiri Mohamed Yassine

UNIVERSITÉ PRIVÉE DE MARRAKECH
UNIVERSITÉ RECONNUE PAR L'ÉTAT
جامعة معترف بها من طرف الدولة

TD2 – Signature et certificat électronique

Exercice 0 :

Soit A et B deux entités désirant échanger des messages chiffrés en utilisant l'algorithme RSA. A détient la clé publique PubA et la clé privée PrivA. B détient la clé publique PubB et la clé privée PrivB.

1. **Quelle clé B doit-il utiliser pour envoyer un message MSG chiffré à A ?**
2. **Quelle clé A doit-il utiliser pour décrypter un message provenant de B ?**
3. **A peut-il se rendre compte que le message MSG chiffré provient de B ?**
4. **Quelles clés A doit-il utiliser pour signer et chiffrer un document pour B ?**
5. **Quelles clés B doit-il utiliser pour déchiffrer le document et vérifier la signature**

Exercice 1 :

On suppose que toutes les personnes intervenant dans cet exercice ont chacune un couple (clef privée, clef publique).

Répondez aux questions suivantes :

1. **Ahmed veut envoyer un message chiffré à Imane, avec quelle clef doit-il le chiffrer ? A l'arrivée, quelle clef, Imane doit-elle utiliser pour déchiffrer le message ?**

2. **Ahmed veut envoyer un message signé à Imane, avec quelle clef doit-il le signer ? A l'arrivée, quelle clef, Imane doit-elle utiliser pour vérifier la signature du message ?**

3. **Ahmed veut envoyer un message chiffré et signé à Imane, avec quelle clef doit-il le chiffrer ? Le signer ? A l'arrivée, quelle clef, Imane doit-elle utiliser pour déchiffrer le message ? Pour vérifier la signature ?**

4. **Ahmed veut envoyer un message chiffré et signé à Imane, Amina, Hicham, Mariam, ... (25 destinataires) avec quelle clef doit-il le chiffrer ? Le signer ?**

Exercice 2:

Un Professeur P envoie, par mail, les notes de ses étudiants au service examen SE de l'école. Les clés publique de P et SE sont PubP est PubSE.

1. **Afin d'assurer la confidentialité, avec quelle clé le professeur doit-il chiffrer chaque note ?**
2. **Pour assurer l'authenticité et la confidentialité, avec quelles clés le professeur doit-il signer et chiffrer chaque note ?**

Exercice 3 :

1. **Quel est le problème principal résolu par une infrastructure à clé publique ?**
2. **Pourquoi les certificats numériques sont-ils publiés dans un annuaire**
3. **Pourquoi les listes de révocations sont-elles publiées dans un annuaire ?**
4. **Discuter les scénarios suivants en termes de sécurité :**
   a. **Deux certificats différents sont signés par la même clé privée**
   b. **Deux certificats différents contiennent la même clé publique**
   c. **Deux certificats différents ont le même émetteur**
   d. **Deux certificats différents ont le même numéro de série**

Exercice 4

Un responsable a obtenu un certificat X.509 pour un site web auprès d'une autorité de certification.

1. **Quel est le but de ce certificat ?**

2. **Outre la signature de l'autorité de certification, quelles sont les deux informations essentielles que l'on trouve de manière générale dans un certificat ?**

3. **Lorsque Alice se connecte sur le site web, son navigateur vérifie la validité du certificat fourni.**
   Quelle clef sera utilisée par son navigateur ? comment est-elle obtenue ?

Exercice 5 :

Une autorité de certification CA a généré un certificat pour soi-même et un certificat pour un utilisateur user1.

1. **Justifier par un exemple d'attaque le besoin d'utiliser les certificats pour la délivrance des clés publiques.**

2. **Par quelle clé privée ont été signés les certificats du CA et du user1**

3. **Par quel moyen un utilisateur user2 peut vérifier le certificat de user1 en local (sans faire la vérification chez le CA)**
4. **Comment user2 peut s'assurer que la clé publique du CA appartient bien à ce dernier.**