Sécurité des systèmes d'information

TD 1 : Cryptographie

Exercice 1

Un utilisateur, qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clé privée, mais dispose encore de la clé publique correspondante.

1. Peut-il encore envoyer des courriers électroniques chiffrés ? En recevoir ?
2. Peut-il encore signer les courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?
3. À quoi peut encore servir la clé publique de notre utilisateur ?
4. Que doit-il faire pour être à nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

Exercice 2

On considère la clef publique RSA (11, 319), c'est-à-dire pour n = 319 et e = 11.

1. Quel est le chiffrement avec cette clé du message M = 100 ?
2. Calculer d la clé privée correspondant à la clé publique e.
3. Déchiffrer le message C = 133.
4. Le message chiffré 625 peut-il résulter d'un chiffrement avec la clé publique ?

Exercice 3

Un professeur envoie ses notes au secrétariat de l'École par mail. La clé publique du professeur est (e = 3, n = 55 = 5 × 11), celle du secrétariat (e = 3, n = 33 = 3 × 11).

1. Déterminer la clé privée du professeur et celle du secrétariat de l'Ecole (on peut remarquer que : $3 \times 27 = 81 \equiv 1 \bmod 40$ et $3 \times 7 = 21 \equiv 1 \bmod 20$)
2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clé RSA du secrétariat. Quel message chiffré correspond à la note 12 ?
3. Pour assurer l'authenticité de ses messages, le professeur signe chaque note avec sa clé privée et chiffre le résultat avec la clé RSA du secrétariat. Le secrétariat reçoit ainsi le message 23. Quelle est la note correspondante ?

Exercice 4

1 Installation

```
sudo apt-get install openssl
```

2 Questions

1. Générer une paire de clés RSA.
2. Pouvez-vous déterminer les paramètres RSA utilisés par la clé génénrée ?
3. Chiffrer votre clé (si cela n'a pas été fait lors de la génération).
4. Chiffrer et déchiffrer n'importe quel petit fichier.
5. Demander à votre binôme sa clé publique. Chiffrer un court message avec celle-ci. Transmettez-le lui, et demandez-lui de le déchiffrer.
6. Signer le fichier de votre choix, puis vérifier la signature.
7. Utiliser AES pour chiffrer puis déchiffrer un petit fichier.
8. Créez trois messages. Calculer l'empreinte de chaque message. Modifiez-en un légèrement. Transmettez à votre binôme les messages ainsi que les empreintes. Demandez-lui de déterminer quel est le message qui a été modifié.
9. On considère deux personnes $P1$ et $P2$. Chacune des deux personnes possède une clé publique et une clé privée. $P1$ souhaite envoyer le message m à $P2$.
   (a) Décrire comment $P1$ doit procéder pour à la fois garantir la confidentialité du message m ainsi que son authenticité ($P2$ est sur que c'est bien $P1$ qui a envoyé m).
   (b) Décrire comment $P2$ doit procéder pour récupérer m.
10. Mettre en œuvre le protocole défini à la question précédente pour envoyé un message à votre binôme en préservant à la fois la confidentialité et l'authenticité. Demander à votre binôme de récupérer le message envoyé.