4 Authentification des participants

4.1 Attaque de l'homme du milieu

Supposons qu'Alice soit cliente de l'établissement BasileBanque.com.
Les communications entre Alice et sa banque doivent bien évidémment être confidentielles. Les communications entre Alice et sa banque sont donc chiffrées. Est-ce suffisant ?

Considérons maintenant Martine (la malveillante), qui veut procéder à l'attaque suivante :
Elle envoie à Alice un email (qui ressemble à la page d'accueil du site BasileBanque.com) , et lui demande de se connecter au site BasileBanque.com :

```
<html>
<body>
Veuillez vous connecter d'urgence au site
<a href="http:martine.com"> BasileBanque.com </a>
</body>
</html>
```

Si Alice n'est pas méfiante, elle peut ne pas se rendre compte qu'elle est connectée au mauvais site !Martine pourra ainsi recevoir tous les messages envoyés par Alice.
Martine aura donc une position intermédiaire entre Alice et sa banque. Martine pourra ainsi se faire passer pour Alice, et modifier les requêtes avant de les envoyer à la banque.

☞ Le chiffrement n'est ici d'aucune aide ! Même si Alice établit une liaison sure avec Martine, et que Martine fait de même avec la banque, l'attaque peut quand même avoir lieu !
On appelle cela une ***attaque de l'homme du milieu***.

4.2 Certificats et tiers de confiance

Les communications sur Internet sont authentifiées de la façon suivante :
L'entité qui veut prouver son identité présente un ***certificat***. Ce dernier a été délivré par une autre entité, en laquelle les deux participants ont confiance. On appelle cela un ***tiers de confiance***.

Alice, qui veut communiquer avec BasileBanque.com va demander à sa banque un ***certificat***.

Ce ***certificat*** sera délivré par un tiers de confiance, Théo.

1. Basile va voir Théo. Théo vérifie qu'il est bien le propriétaire de BasileBanque.com.
   Une fois les vérifications faites, Théo chiffre la clé publique de Basile avec sa clef privée :

   $$s = K_{privé}^{Théo}\left(K_{publique}^{Basile}\right)$$

   ☞ Un tel fichier s'appelle un ***certificat***.
   ☞ On dit qque Théo signe la clé publique $K_{publique}^{Basile}$ avec sa clé privée.

2. Alice veut se connecter à BasileBanque.com.
   Lors de la connexion, le site BasileBanque.com envoie la clé publique $K_{publique}^{Basile}$ de Basile et le ***certificat*** s.

3. Alice récupère alors la clé publique de Théo (en qui elle a confiance) $K^{Théo}_{publique}$, et elle calcule $K^{Théo}_{publique}(s)$:

$$K^{Théo}_{publique}(s) = K^{Théo}_{publique}\left(K^{Théo}_{privé}\left(K^{Basile}_{publique}\right)\right)$$

donc $K^{Théo}_{publique}(s) = K^{Basile}_{publique}$ car $K^{Théo}_{publique}\left(K^{Théo}_{privé}\right)$ s'"annule".

4. Alice compare ensuite la clé publique envoyée par Basile avec la clé qui résulte du calcul précédent. Si les deux sont identiques, Alice à la *garantie* que Basile est bien passé voir Théo (et à confiance en Théo pour avoir fait toutes les vérifications nécessaires).

5. Alice a donc maintenant authentifié BasileBanque.com comme étant bien le site détenu par Basile, et elle peut commencer avec lui une communication sécurisée.