

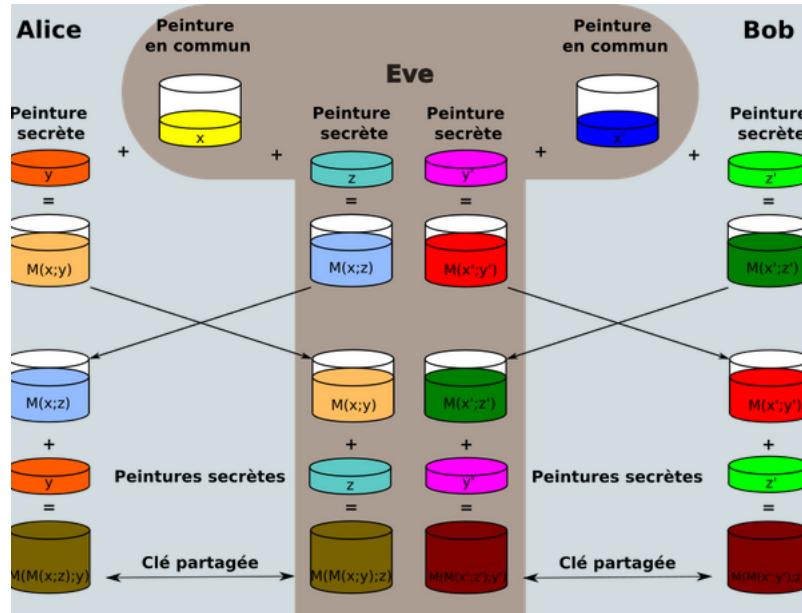
15.4

Authentification des participants

NSI TERMINALE - JB DUTHOIT

15.4.1 Attaque de l'homme du milieu

Imaginons qu'Ève ne se contente pas d'intercepter la couleur commune, mais qu'elle se fasse passer pour Bob auprès d'Alice, et d'Alice auprès de Bob. Ève peut alors choisir une couleur commune avec Alice, et une autre avec Bob. Le protocole d'échange se poursuit normalement, mais Ève intercepte et décode chaque message transmis, avant de le retransmettre à son tour, modifié ou non :



Attaque de l'homme du milieu, ou Main in the middle attack (MITM)

15.4.2 Authentification

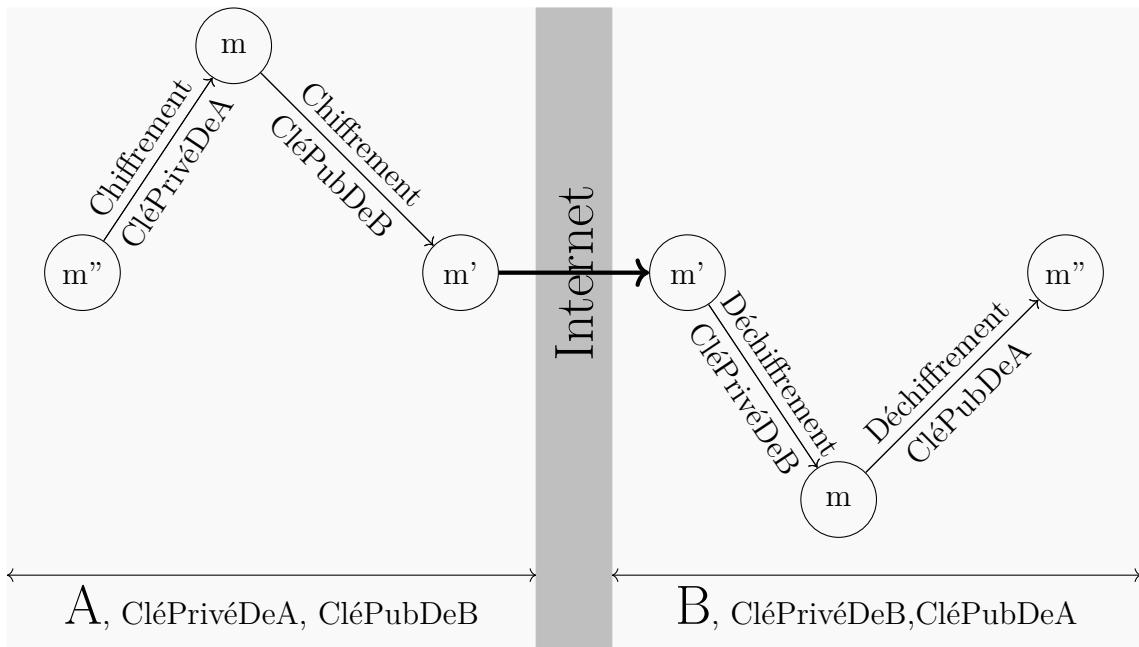
Le chiffrement asymétrique peut servir à authentifier l'expéditeur d'un message :

Analogie : La boîte à deux serrures...suite !

Pour signer un message, Alice le place dans la boîte et ferme celle-ci à l'aide de sa clef privée. Ainsi n'importe qui ayant récupéré la clef publique pourra ouvrir la boîte. Mais comme la boîte a été fermée par la clef privée, cette personne sera assurée que c'est bien Alice, seule détentrice de cette clef, qui aura placé le message dans la boîte et fermé ladite boîte.

Principe

Authentification de l'émetteur



Si le récepteur (B) ici) peut déchiffrer grâce à la clé publique de (A), c'est bien que le message a été envoyé par (A) (le seul à avoir ClePrivéDeA).

☞ Le concept de signature numérique est basé sur cette technique de chiffrement asymétrique.

☞ Le chiffrement asymétrique repose sur des problèmes très difficiles à résoudre dans un sens et faciles à résoudre dans l'autre sens.

15.4.3 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 :

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

☞ Un tel fichier s'appelle un **certificat**.

☞ On dit que 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) $K_{publique}^{Théo}$, et elle calcule $K_{publique}^{Théo}(s)$:

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

donc $K_{publique}^{Théo}(s) = K_{publique}^{Basile}$ car $K_{publique}^{Théo}(K_{privé}^{Théo})$ 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 a 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.