La signature numérique

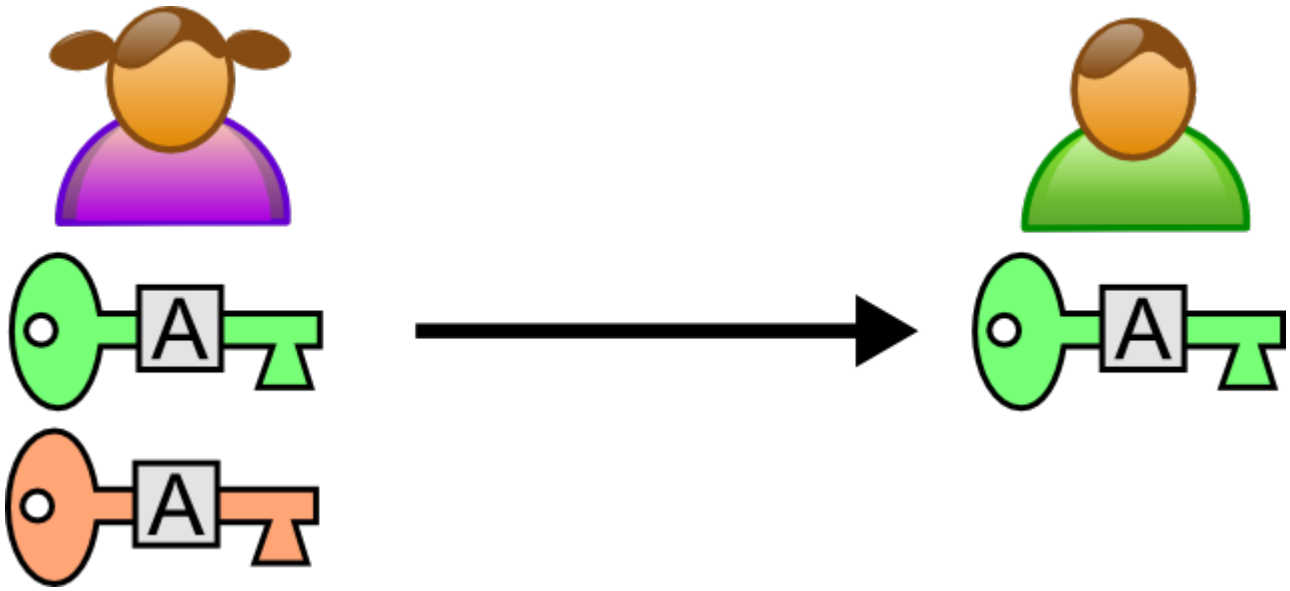
Fonctionnement de la signature numérique

Cryptographie asymétrique

Les concepts de signature numérique sont principalement basés sur la cryptographie asymétrique. Cette technique permet de chiffrer avec un mot de passe et de déchiffrer avec un autre, les deux étant indépendants.

Par exemlpe, imaginons que Bob souhaite envoyer des messages secret à Alice. Ils vont pour cela utiliser la cryptographie symétrique.

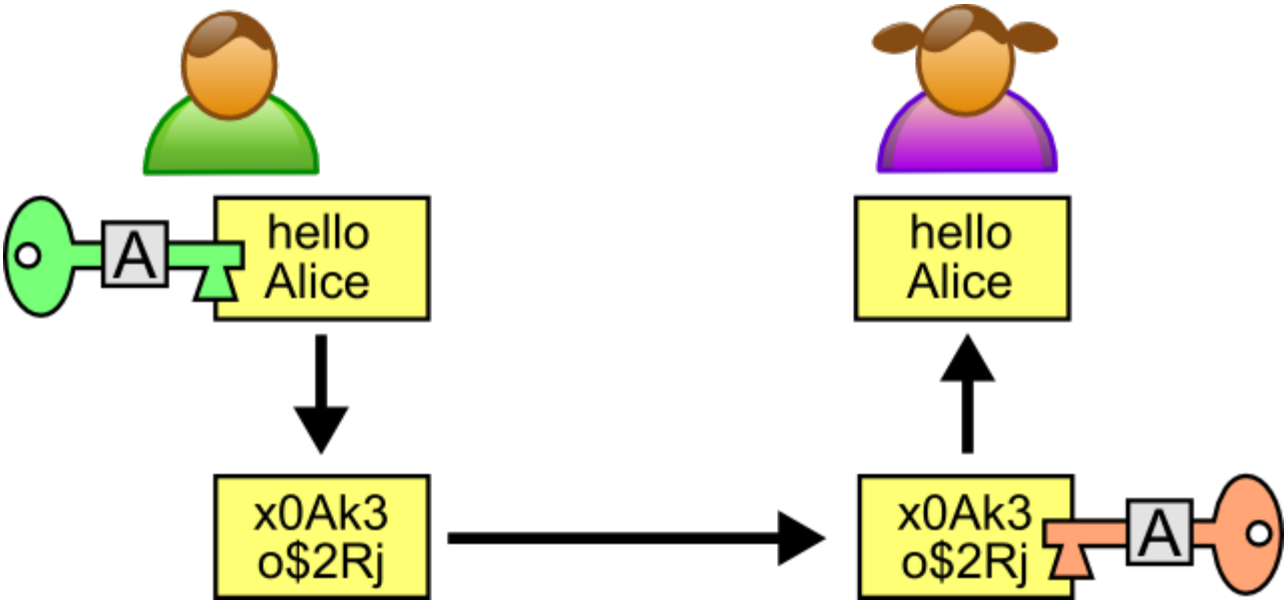
Alice génère tout d'abord un couple de clés. Une clé privée (en rouge) et une clé publique (en vert). Ces clés ont des propriétés particulière vis à vis des algorithmes utilisés. En effet, un message chiffré avec une clé ne peut être déchiffré qu'avec l'autre clé. Il s'agit de fonctions à sens unique.



source : wikipédia (http://commons.wikimedia.org/wiki/Image:Asymetric_crypto_step1.png)

Alice transmet ensuite la clé publique (en vert) à Bob.

Grâce à cette clé, Bob peut chiffrer un texte et l'envoyer à Alice.



source : wikipédia (http://commons.wikimedia.org/wiki/Image:Asymetric_crypto_step2.png)

En utilisant la clé publique d'Alice, Bob est certain de deux choses :

- Personne ne peut lire le message, puisqu'il est crypté
- Seule Alice peut déchiffrer le message, car elle est la seule a possèder la clé privée.

Nous venons de répondre au besoin de confidentialité des données.

Mais la cryptographie asymétrique peut être utilisée d'une autre façon. En effet, on peut également utiliser la clé privée pour chiffrer, la clé publique servant alors à déchiffrer.

Le message ainsi chiffré est lisible par toute personne disposant de la clé publique. Ceci n'est pas très utile si l'on cherche la confidentialité. En revanche, une seule personne est susceptible d'avoir chiffré ce message : Alice. Ainsi, si l'on peut déchiffrer un message avec la clé publique d'Alice, c'est forcément la personne à avoir chiffré ce message. ()

Fonctions de hachage

Je vais maintenant décrire les mécanismes permettant de s'assurer que des données n'ont pas été modifiées : les fonctions de hachage.

Une fonction de hachage est un procédé à sens unique permettant d'obtenir une suite d'octets (une empreinte) caractérisant un ensemble de données. Pour tout ensemble de données de départ, l'empreinte obtenue est toujours la même.

Dans le cadre de la signature numérique, nous nous intéresseront tout particulièrement aux fonctions de hachage cryptographiques. Celles-ci assurent qu'il est impossible de créer un ensemble de données de départ donnant la même empreinte qu'un autre ensemble.

Nous pouvons donc utiliser ces fonctions pour nous assurer de l'intégrité d'un document.

Les deux algorithme les plus utilisées sont MD5 et SHA. A noter que MD5 n'est plus considéré comme sûr par les spécialistes. En effet, une équipe chinoise aurait réussi à trouver une collision complète, c'est à dire deux jeux de données donnant la même empreinte, sans utiliser de méthode de force brute.

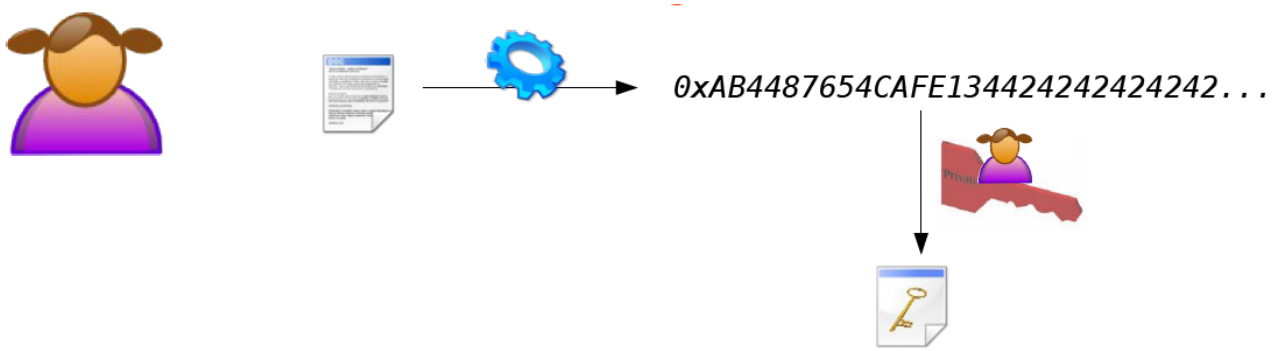
Aujourd'hui, il serait notamment possible de créer deux pages html au contenu différent, ayant pourtant les mêmes empreintes MD5 (en utilisant notamment les balises <meta>, invisibles dans le navigateur). La falsification de documents pourrait donc être possible.
()

Signer un document

La signature d'un document utilise à la fois la cryptographie asymétrique et les fonctions de hachage. C'est en effet par l'association de ces deux techniques que nous pouvons obtenir les 5 caractéristiques d'une signature (authentique, infalsifiable, non réutilisable, inaltérable, irrévocable).

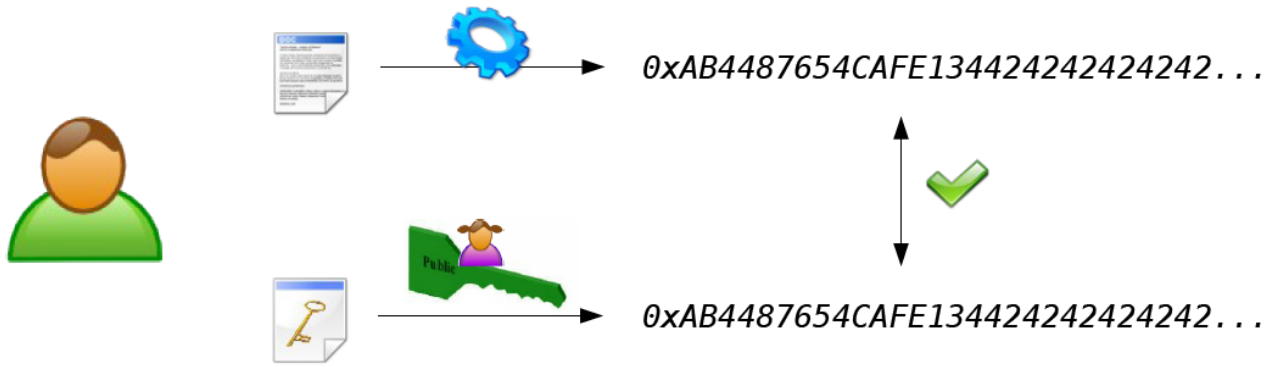
Imaginons que Alice souhaite envoyer un document signé à Bob.

- Tout d'abord, elle génére l'empreinte du document au moyen d'une fonction de hachage.
- Puis, elle crypte cette empreinte avec sa clé privée.



- Elle obtient ainsi la signature de son document. Elle envoie donc ces deux éléments à Bob

- Pour vérifier la validité du document, Bob doit tout d'abord déchiffrer la signature en utilisant la clé publique d'Alice. Si cela ne fonctionne pas, c'est que le document n'a pas été envoyé par Alice.
- Ensuite, Bob génère l'empreinte du document qu'il a reçu, en utilisant la même fonction de hachage qu'Alice (On supposera qu'ils suivent un protocole établi au préalable).
- Puis, il compare l'empreinte générée et celle issue de la signature.



- Si les deux empreintes sont identiques, la signature est validée. Nous sommes donc sûr que :
  - C'est Alice qui a envoyé le document,
  - Le document n'a pas été modifié depuis qu'Alice l'a signé.
- Dans le cas contraire, cela peut signifier que :
  - Le document a été modifié depuis sa signature par Alice,
  - Ce n'est pas ce document qu'Alice a signé