



Signature électronique à clé publique


Rappel sur la signature électronique

□ La signature numérique :

- Indique qui a signé le document (**authenticité**)
- Ne peut pas être imitée ou copiée (**infalsifiable**)
- Est indissociable du document (**inaltérable**)
- ne peut pas être reniée (**non-répudiation**)
- Rend le document non modifiable (**intégrité**)
- La signature électronique dépend du document (**unicité**)

Généralités

- Un procédé de signature est un quintuplet (P, A, K, S, V) où :
 - P est un ensemble fini de messages
 - A est un ensemble fini de signatures
 - K est un ensemble fini de clés
 - Pour chaque $k \in K$, il y a une fonction de signature $sig_k \in S$ et une fonction de vérification $ver_k \in V$ correspondante



□ sig_k et ver_k doivent vérifier

$$sig_k : P \rightarrow A \text{ et } ver_k : P \times A \rightarrow \{vrai, faux\}$$

$$ver_k(x, y) = \begin{cases} vrai \text{ si } y = sig_k(x) \\ faux \text{ si } y \neq sig_k(x) \end{cases}$$

Les principales méthodes

❑ La signature RSA

- Basée sur le cryptosystème RSA
- Standard de fait

❑ La signature DSA

- Basée sur le cryptosystème El Gamal
- Standard proposé par le NIST

La signature RSA

Soit $n = pq$ où p et q sont premiers,
et soit $P = A = \mathbb{Z}_n$

$K = \{(n, p, q, e, d) : n = pq, ed \equiv 1 \bmod \Phi(n)\}$
 (n, e) est public, et (p, q, d) sont privés

$$sig_k(x) = x^d \bmod n$$

et

$$ver_k(x) = \text{vrai} \Leftrightarrow x \equiv y^e \bmod n$$

- Alice envoie un message chiffré avec sa clé privée
- Tout le monde peut déchiffrer le message avec la clé publique et vérifier que Alice en est bien l'émetteur
- Si Alice veut envoyer un message signé uniquement à Bob, alors :

Alice


$$y = \text{sig}_{k_{\text{Alice}}}(x) = d_{k_{\text{Alice}}}(x)$$


$$z = e_{k_{\text{Bob}}}(x, y)$$

Bob :

$$(x, y) = d_{k_{\text{Bob}}}(z)$$

$$\text{ver}_{k_{\text{Alice}}}(x, y) \Leftrightarrow e_{k_{\text{Alice}}}(y) = x$$

- 
- ❑ Alice signe son message avec sa clé privée
 - ❑ Alice chiffre le message et sa signature avec la clé publique de Bob et envoie le tout à Bob
 - ❑ Bob déchiffre avec sa clé privée (c'est le seul qui puisse le faire)
 - ❑ Bob vérifie la signature avec la clé publique d'Alice
-
- ❑ **Chiffrer avant de signer est vivement déconseillé, pourquoi ?**

- 
- ❑ Chiffrer tout le message x avec RSA (ou avec un autre cryptosystème à clé publique) est coûteux
 - ❑ Alice construit plutôt une empreinte $h(x)$ et signe l'empreinte $sig_k(h(x))$.
 - ❑ Bob reçoit x et $sig_k(h(x))$
 - Il recalcule $h(x)$
 - Il peut vérifier $ver_k(h(x)) = h(x)$