

Sécurité des systèmes informatiques
Les signatures digitales

Olivier Markowitch

Signatures digitales

Pendant électronique à la signature manuscrite, mais la signature digitale :

- est liée au document signé
- n'est pas comparée à une signature témoin mais elle est vérifiée algorithmiquement
- est universellement vérifiable

Non-répudiation

Une signature digitale apporte la *non-répudiation* à *l'origine*

Le signataire ne peut convaincre un tiers qu'il n'est pas le signataire, il ne peut répudier sa signature

Une signature digitale est générée au moyen d'une clé secrète et est vérifiable, à priori, par tous, grâce à la clé publique correspondante

Définitions

Une **signature digitale** est produite par un **algorithme de génération de signatures digitales** et est vérifiée par un **algorithme de vérification de signatures digitales**

Un **schéma de signatures digitales** consiste en un algorithme de génération de signatures digitales associé à son algorithme de vérification

Il existe deux classes de schémas de signatures : avec **appendice** (où le message original doit être fourni à l'algorithme de vérification) et avec **recouvrement** (où le message original est récupéré à partir de la signature)

Signatures avec appendices

Chaque signataire a une clé privée pour signer et une clé publique correspondante pour vérifier les signatures produites

Soient M un ensemble fini de messages, S un ensemble fini de signatures et K un ensemble fini de paires de clés (publique et secrète)

Pour toute paire de clé publique et secrète (k, k') , il existe un algorithme de signature avec appendice $\text{Sig}_{k'}$ et un algorithme de vérification correspondant Ver_k tels que la signature d'un message x est

$$y = \text{Sig}_{k'}(x) : M \rightarrow S$$

et

$$\text{Ver}_k(x, y) : M \times S \rightarrow \{\text{vrai, faux}\}$$

Signatures avec recouvrement

Soient M un ensemble fini de messages, M_S un ensemble fini de messages signables, S un ensemble fini de messages signés et K un ensemble fini de paires de clés (publique et secrète)

Pour toute paire de clé publique et secrète (k, k') , il existe un algorithme de signature avec recouvrement $\text{Sig}_{k'}$ qui applique $M_S \rightarrow S$, une fonction de redondance $R : M \rightarrow M_S$ et un algorithme de vérification correspondant $\text{Ver}_k : S \rightarrow M_S$ tels que la signature d'un message x est

$$y = \text{Sig}_{k'}(R(x))$$

et

$$x' = \text{Ver}_k(x)$$

Si $x' \notin M_S$ alors la signature est rejetée, sinon la signature est acceptée et le message $x = R^{-1}(x')$ est récupéré

Attaques

Le but d'un adversaire est de **forger** une signature au nom d'un tiers

Si un adversaire forge ainsi toutes les signatures qu'il désire au nom d'un tiers, le schéma de signature est dit **totalelement cassé**

Si un adversaire peut forger des signatures pour certains messages, le schéma de signature est dit **sélectivement forgeable**

Si un adversaire peut forger au-moins une signature dont il ne contrôle par le contenu, le schéma de signature est dit **existentiellement forgeable**

Standards

ISO/IEC 9796, publié en 1991, est un standard de signatures avec recouvrement

ISO/IEC 9796, *Information technology - Security techniques - Digital signature scheme giving message recovery*. International Organization for Standardisation, Genève, Suisse, 1991

PKCS#1 est un standard de fait proposé par RSA lab, décrivant le processus de signature avec appendice, basé sur RSA.

[http ://www.rsa.com](http://www.rsa.com)

RSA

Génération des clés

- choisir p et q deux grands premiers approximativement de même taille
- soit $n = pq$
- choisir $e \in]1, \phi(n)[$ tel que $\text{pgcd}(e, \phi(n)) = 1$
- calculer d tel que $e \cdot d \equiv 1 \pmod{\phi(n)}$

La clé privée de génération de signatures est d , la clé publique de vérification de signatures est (n, e)

RSA avec recouvrement

Génération de la signature

Soit le message m à signer :

- $\tilde{m} = R(m)$ où R est la fonction de redondance
- $s = \tilde{m}^d \pmod n$ et s est la signature de m

Vérification de la signature

Soit la signature s fournie :

- $\tilde{m} = s^e \pmod n$
- si $\tilde{m} \in M_s$ alors $m = R^{-1}(\tilde{m})$, sinon la signature est rejetée

RSA avec appendice

Génération de la signature

Soit le message m à signer :

- $\tilde{m} = h(m)$ où h est un MDC (MD5 est recommandé)
- $s = \tilde{m}^d \pmod n$ et s est la signature de m

Vérification de la signature

Soit la signature s et le message original m fournis :

- $\tilde{m} = s^e \pmod n$
- si $h(m) = \tilde{m}$ alors la signature est acceptée

Rabin

Génération des clés

Soit n la clé publique telle que $n = pq$ avec p et q deux grands premiers formant la clé secrète

Génération de la signature

Soit le message m à signer :

- $\tilde{m} = R(m)$ où R est la fonction de redondance
- $s = \sqrt{\tilde{m}} \pmod n$ et s est la signature de m

Vérification de la signature

Soit la signature s fournie :

- $\tilde{m} = s^2 \pmod n$
- si $\tilde{m} \in M_s$ alors $m = R^{-1}(\tilde{m})$, sinon la signature est rejetée

El Gamal

Génération des clés

- choisir p un grand premier
- choisir α un générateur de \mathbb{Z}_p^*
- choisir $a \in [1, p - 2]$
- calculer $\beta = \alpha^a \pmod p$

La clé secrète de génération de signatures est a , et la clé publique de vérification de signatures est (p, α, β)

El Gamal (suite)

Génération de la signature

Soit le message m à signer :

- choisir aléatoirement $k \in [1, p - 2]$ tel que k est premier avec $p - 1$
- calculer $\gamma = \alpha^k \pmod{p}$
- calculer $\delta = (h(m) - a \cdot \gamma) \cdot k^{-1} \pmod{p - 1}$

La signature de m est formée par (γ, δ)

Vérification de la signature

Soit la signature s et le message m fournis :

Si $\gamma \in [1, p - 1]$ et si $\beta^\gamma \cdot \gamma^\delta \equiv \alpha^{h(m)} \pmod{p}$ alors la signature est acceptée

DSA

Génération des clés

- choisir q un grand premier $\in]2^{159}, 2^{160}[$
- choisir p premier de $512 + 64 \cdot t$ bits avec $t \in [0, 8]$, tel que q divise $p - 1$
- choisir α un générateur du sous-groupe cyclique d'ordre q dans \mathbb{Z}_p^*
- choisir aléatoirement $a \in [1, q - 1]$
- calculer $\beta = \alpha^a \pmod p$

La clé secrète de génération de signatures est a , et la clé publique de vérification de signatures est (p, q, α, β)

DSA (suite)

Génération de la signature

Soit le message m à signer :

- choisir aléatoirement $k \in]0, q[$ tel que k est premier avec $p - 1$
- calculer $\gamma = (\alpha^k \bmod p) \bmod q$
- calculer $\delta = (h(m) + a \cdot \gamma) \cdot k^{-1} \bmod q$

La signature de m est formée par (γ, δ)

DSA (suite)

Vérification de la signature

Soit la signature s et le message m fournis :

Si $\gamma \in]0, q[$ et $\delta \in]0, q[$ alors calculer :

– calculer $e_1 = h(m) \cdot \delta^{-1} \pmod q$

– calculer $e_2 = \gamma \cdot \delta^{-1} \pmod q$

et si $(\alpha^{e_1} \cdot \beta^{e_2} \pmod p) \pmod q = \gamma$ alors la signature est acceptée

Signatures jetables

M. Rabin, *Digitalized signatures*. Foundations of Secure Computation, Academic Press, 1978

L. Lamport, *Constructing digital signatures from one-way functions*. Technical report CSL-98, SRI International, Palo Alto, 1979

R. Merkle, *A certified digital signature*. Proceedings of Crypto'89, Lecture Notes in Computer Science, Vol 435, 1990

Signatures incontestable

D. Chaum et H. Van Antwerpen, *undeniable signatures*. Proceedings of Crypto'89, Lecture Notes in Computer Science, Vol 435, 1990

Signatures en aveugle

D. Chaum, *Blind signatures for untraceable payments*. Proceedings of Crypto'82, Plenum Press, 1983

D. Chaum, *Security without identification : transaction systems to make big brother obsolete*. Communication of the ACM, Vol 28, 1985

D. Chaum, *Blinding for unanticipated signatures*, Proceedings of Eurocrypt'87, Lecture Notes in Computer Science, Vol 304, 1988

J. Camenish, J-M Piveteau et M. Stadler, *Blind signatures based on the discrete logarithm problem*. Proceedings of Eurocrypt'94, Lecture Notes in Computer Science, Vol 950, 1995