VII. Digitale Signaturen

VII.1. Begriffe

- Authentizität (d.h. einer Person eindeutig zugeordnet)
- Integrität (d.h. unverändert)
- Unabstreitbarkeit (non repudiation)
- Praktikabilität (d.h. kurz im Vergleich zum Dokument)

VII.2. Beispiel: Signieren mit RSA (anschaulich)

Man „entschlüsselt“ das Dokument, als wäre es ein Chiffrat. Dies kann nur der Besitzer des Secret Keys. Prüfen kann aber jeder, der den Private Key kennt: „Verschlüsseln“ der Signatur ergibt die Nachricht.
Signatur zu m wäre dann $m^d \mod N = \sigma$ und überprüfen via $\sigma^e \mod N \stackrel{?}{=} m$.

So ist das aber noch nicht sicher:

1. zu zufälligem r wirkt r wie eine gültige Signatur von $r^e \mod N$
2. $\sigma_1 \cdot \sigma_2 \mod N$ ist eine gültige Signatur, da $(m_1^d) \cdot (m_2^d) = (m_1 \cdot m_2)^d \mod N$

Abhilfe: Hash-then-Sign (beweisbar sicher im Random Oracle Model)

VII.3. Definition Signatur

FIXME: Definition Signatur, S. 25

VII.4. Sicherheitsbegriff: EUF-CMA

VII.5. Beispiel: Elgamal-Signaturen

Sei G eine Gruppe mit Erzeuger g ($G = \mathbb{F}_p$ für p prim)[1]. Wähle x zufällig.

- öffentlicher Schlüssel (Verifikationsschlüssel): $vk = g^x$
- signing key: $sk = x$

Signatur „naiv“ :

- signieren: $M \equiv ax \mod (p-1) \rightarrow$ Signatur: a

[1] Rechnen: bei Gruppenelementen $\mod p$, im Exponenten $\mod (p-1)$

- prüfen: $g^M \equiv g^{ax} \equiv vk^a \mod (p-1)$
- aber: $x \equiv Ma^{-1} \mod (p-1)$ und jeder kann nun den sk ausrechnen

deshalb:

- signer Bob wählt k zufällig mit $ggT(k, p-1) = 1$
- $a :\equiv g^k \mod p$
- berechne b mit $m \equiv x \cdot a + k \cdot b \mod (p-1)$
- Signatur zu m ist (a, b)
- Prüfen der Signatur: $g^m \equiv g^{xa+kb} \equiv g^{xa} \cdot g^{kb} \equiv vk^a \cdot a^b \mod p$

VII.5.1. Probleme

1. niemals ein k zweimal verwenden → mit $m_1 = xa + kb_1$ und $m_2 = xa + kb_2$ lässt sich x berechnen
2. es ist möglich, gültige Signaturen zu (unsinnigen) Nachrichten zu generieren → Lösung: hash-then-sign

VII.6. Beispiel: DSA (Digital Signature Algorithm)

$g \in \mathbb{F}_p^\times$ erzeuge eine multiplikative Gruppe der Ordnung $q \in \mathbb{P}$, $(q|p-1)$.

- $sk = x$
- $vk = g^x$

Signieren:

- wähle $k \in \{0, dotsc, q-1\}$ zufällig
- berechne $r :\equiv g^k(\mod p) \mod q$
- berechne s mit $h(m) \equiv k \cdot s - x \cdot r \mod q$
- dann ist (r, s) eine Signatur zu m

Prüfen: $r \equiv (g^{s^{-1}h(m)} vk^{s^{-1}} r \mod p) \mod q$

VII.7. Beispiel: One-Time-Signaturen (aus Hashfunktionen)

sk besteht aus zufälligen Strings $\in \{0,1\}^k$

$$r_1^0\ r_2^0\ r_3^0\ \dots\ r_k^0$$
$$r_1^1\ r_2^1\ r_3^1\ \dots\ r_k^1$$

vk ist

$$h(r_1^0)\ h(r_2^0)\ h(r_3^0)\ \dots\ h(r_k^0)$$

$$h(r_1^1)\ h(r_2^1)\ h(r_3^1)\ \ldots\ h(r_k^1)$$

Beispielsignatur zu $01\ldots1$: $r_1^0\ r_2^1\ \ldots\ r_k^1$

One time signatures darf man nur einmal verwenden! Alternativ kann man einen doppelt so langen vk benutzen: Signiere die Nachricht und einen neuen public key (der wieder zwei Nachrichten signieren kann). Zum Verifizieren benötigt man eine Kette signierter vks, die zum ursprünglichen public key führen. Wenn die Nachrichten länger als k bit sind, verwendet man hash-then-sign.

VII.8. Ist EUF-CMA genug?

VII.8.1. Key Substitution Attacks

- Alice hat vk und signiert m mit σ
- Bob wählt (böse) einen vk', sodass seine Signatur zu m exakt σ ist

Beispiel (RSA)

1. Wähle $\bar{p}$ und $\bar{q}$ so, dass $\bar{p}-1$ und $\bar{q}-1$ in kleine Primfaktoren zerfallen und σ und $h(m)$ $\mathbb{F}_{\bar{p}}^{\times}$ und $\mathbb{F}_{\bar{q}}^{\times}$ generieren.
2. Pohlig-Hellman-Algorithmus löst den dlog $\mod \bar{p}$ und $\mod \bar{q}$.
3. Berechne x_1, x_2, sodass $\sigma^{x^1} \equiv h(m) \mod \bar{p}$ und $\sigma^{x^2} \equiv h(m) \mod \bar{q}$.
4. Ist $ggT(\bar{p}-1, \bar{q}-1) = 2$, so gibt es ein eindeutiges $\bar{e} < \varphi(\bar{p}\bar{q})$ mit $\bar{e} \equiv x_1 \mod \bar{p}-1$ und $\bar{e} \equiv x_2 \mod \bar{q}-1$ (Chinesischer Restsatz).
5. Gib $(\bar{n} = \bar{p} \cdot \bar{q}, \bar{e})$ als vk aus.

Dann gilt: $\sigma^{\bar{e}} \equiv h(m) \mod \bar{n}$, d.h. Signatur gilt, weil $\sigma^{\bar{e}} \equiv h(m) \mod \bar{p}$ und $\sigma^{\bar{e}} \equiv h(m) \mod \bar{q}$.

Lösungen

- DSA ist sicher gehen (starke) Key Substitution
- vk immer mitsignieren

VII.8.2. Subliminal Channel

Gut Simmons hat gemerkt, dass Signaturen Nachrichten enthalten können (subliminal channels).

Beispiel:

RSA-PSS signiert eine spezielle Kodierung:

FIXME: Bild RSA-PSS, S. 29