Digitale Signaturen

Analogie

alle können für einen verschlüsseln (↗ public)

nur der eine kann entschlüsseln (↳ private)

Signatur

nur einer kann die richtige Unterschrift erzeugen (↗ private)

aber alle können verifizieren, dass die Unterschrift gültig (↳ public)

RSA Signaturen

m zu signierende Nachricht

Parameter: n, e öffentlich

p, q, d geheim

Signatur erzeugen (Konzept)

$s \equiv m^d \bmod n \rightarrow (m, s)$ ist signierte Nachricht

Signatur verifizieren

berechne $s^e \equiv (m^d)^e \equiv m \bmod n$

falls m als Ergebnis, dann akzeptiere die Signatur

Problem:

m wird nur mod n betrachtet, d.h. Nachrichtenlänge auf 2048 Bits beschränkt bzw.

$m+n$, $m+2n$, $m+3n$, ...

haben alle die gleiche Signatur

Abhilfe: statt m wird ein Wert $h(m)$ signiert, wobei $h()$ eine sichere Hashfunktion ist.

h = SHA-2 oder h = SHA-3

meist SHA-256

Grundsatz:

für Verschlüsselung und Signatur unterschiedliche Parameter benutzen, d.h. (n, e) und (n', e')

Signaturen nach ElGamal-Modell

DSA, ECDSA (Digital Signature Algorithm)

ECDSA → elliptic curves

FIPS 186-4 Standard

- Rechnen mod p, p hat L Bits, z.B. 2048
- Problem für Angreifer: Diskrete Logarithmen (wie Diffie-Hellman)
- Primfaktor q von $p-1$ wird von Größe her vorgegeben, q hat N Bits, z.B. 224

Parametererzeugung:

p, g, q hierbei q Teiler von $p-1$ und Primzahl

↳ speziell: $g^q \equiv 1 \bmod p$

$y \equiv g^x \bmod p$

↳ siehe B.1.1 (x per Zufallsgenerator /dev/random)

x geheim (private key)

Signaturerzeugung

Abschnitt 4.6 in FIPS-186

k Zufallszahl

$$r \equiv (g^k \bmod p) \bmod q$$

Hashwert von m ist z

$$s \equiv \frac{1}{k} \cdot (z + x \cdot r) \bmod q$$

wiederhole falls $r=0 \vee s=0$

(m, r, s) ist signierte Nachricht

Verifikation einer Nachricht (m, r, s)

Abschnitt 4.7

checke $0 < r < q$, $0 < s < q$

$$w = \frac{1}{s} \bmod q$$

z Hashwert von m

$$u_1 \equiv z \cdot w \bmod q$$

$$u_2 \equiv r \cdot w \bmod q$$

$$v = \left[\left(g^{u_1} \cdot y^{u_2}\right) \bmod p\right] \bmod q$$

Akzeptiere Signatur, wenn $v = r$

Signaturtest:

$$g^{u_1} \cdot y^{u_2} \equiv g^{z \cdot w} \cdot g^{x \cdot r \cdot w} \equiv g^{w \cdot (z + x \cdot r)}$$

$$\equiv g^{\frac{1}{s} \cdot (z + x \cdot r)} \equiv g^k \equiv r \bmod p$$

zusätzlich $(\ldots) \bmod q$ bei v und r ✓

Mittwoch

DSA Implementierung

PoC, proof-of-concept