

IV. Hashfunktionen

(hier immer kryptographische)

IV.1. Anwendungen

- Passwortdateien
- Time Stamping
- Digitale Signaturen (s. VII)
- RSA-ES-OAEP (s. VI.4.3)

IV.2. Eigenschaften

einer Hashfunktion $h: \{0, 1\}^* \rightarrow \{0, 1\}^k$:

- Einwegfunktion¹
- preimage resistant: gegeben $x \in \{0, 1\}^k$ ist es schwierig, ein m zu finden mit $h(m) = x$
- collision resistant: es ist schwierig, m und m' , $m \neq m'$, zu finden mit $h(m) = h(m')$
- die Ausgabelänge von Hashfunktionen sollte mindestens 160 bit sein (wg. Meet-in-the-Middle-Angriff)

IV.3. Merkle-Damgård-Konstruktion

gegeben: eine Kompressionsfunktion $f: \{0, 1\}^{2k} \rightarrow \{0, 1\}^k$ (Kandidat: Blockchiffre)

FIXME: Bild Merkle-Damgard-Konstruktion, S. 10

Die Sicherheit der so entstandenen Hashfunktion hängt nur von der Sicherheit von f ab. Aber: eine gegebene Kollision lässt sich verlängern.

IV.4. Das Random Oracle Model

Manchmal stellt man sich Hashfunktionen vor wie echt zufällige „Orakel“. Beweise im Random Oracle Model sind trotzdem nur Heuristiken, da ein Angriff die innere Struktur der Hashfunktion ausnutzen kann.

¹die Annahme der Existenz von Einwegfunktionen ist eine stärkere Annahme als $P \neq NP!$ → Hashfunktionen sind eine noch stärkere Annahme

IV.5. Der Angriff von Wang

Der Angriff von Wang findet Kollisionen von MD5 zu gegebenem Initialisierungsvektor. Diese wirken wie zufällig.

Problem (Beispiel Postscript):

- gegeben: Dokumente P und Q und eine Kollision $h(S) = h(R)$
- hashe „if“
- nimm dies als Initialisierungsvektor: Kollision $h(\text{if } S) = h(\text{if } R)$
- MD5 ist eine Merkle-Damgård-Konstruktion \rightarrow Erweitern der Kollision zu
 - if $S = S$ then display P else Q
 - if $R = S$ then display P else Q
- Ergebnis: zwei Dokumente mit gleichem Hash, aber unterschiedlicher Inhalt wird angezeigt (P oder Q)

Daher gibt es zur Zeit einen neuen Wettbewerb SHA3.

IV.6. Symmetrische Authentifikation (MAC - Message Authentication Code)

Ein MAC ist eine Abbildung $MAC: \{0,1\}^* \times \{0,1\}^k \rightarrow \{0,1\}^k$.

Sicherheitsbegriff: ein Angreifer \mathcal{A} mit Zugriff auf ein Orakel, das gültige MACs ausrechnet, darf keinen gültigen MAC mit zugehöriger Nachricht finden können, ohne das Orakel nach dieser Nachricht gefragt zu haben.

- Vorschlag 1: $h(key||m) \rightarrow$ funktioniert nicht **FIXME:** warum?
- Vorschlag 2: $h(m||key) \rightarrow$ funktioniert nicht **FIXME:** warum?
- HMAC: $h((key \oplus o_pad)||h((key \oplus i_pad)||m))$

FIXME: Bild HMAC, S. 12