Verteilte Systeme

...für C++ Programmierer

Kryptographische Hashfunktionen

by

Dr. Günter Kolousek

Hashfunktionen

- Hashfunktion h
  $h : K \to \{0, \ldots, m-1\}$
  ordnet jedem Schlüssel $k \in K$ einen Index $h(k)$ mit
  $0 \leq h(k) \leq m-1$ zu.
- Anforderungen
  - gleichmäßige Verteilung, um (Adress)Kollisionen zu vermeiden
  - Surjektivität, d.h. alle möglichen Hashwerte sollen auch durch Hashfunktion auch errechnet werden können
  - effizient berechenbar

Kryptographische Hashfunktion

- kollisionsresistente Einweghashfunktion
  - Einwegfunktion: kann in die eine Richtung leicht berechnet werden, die andere Richtung ist nicht berechenbar (oder nur mit extrem viel Aufwand).
  - Hashfunktion
  - kollisionsresistent
    - schwache Kollisionsresistenz: praktisch unmöglich zu gegebenen x einen unterschiedlichen Wert x' zu finden, der gleichen Hashwert aufweist
    - starke Kollisionsresistenz: praktisch unmöglich zwei verschiedene Werte x und x' zu finden, die gleiche Hashwerte aufweisen
- Einteilung
  - schlüssellose Hashfunktionen
  - schlüsselabhängige Hashfunktionen

Hashfunktionen

- MD5 (Message Digest 5): 128 Bits, unsicher
- SHA
  - SHA (auch SHA-1): 128 Bits, unsicher
  - SHA-2: Weiterentwicklung von SHA
    - SHA-224
    - SHA-256
    - SHA-384
    - SHA-512
- SHA-3: wird meist in Kombination zu SHA-2 eingesetzt
  - Neuentwicklung, Gewinner internationaler Ausschreibung
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
  - SHAKE128 und SHAKE256: beliebige Länge des Hashwertes