Hashfunktionen – soviel Mathematik wie nötig, sowenig wie möglich

Wolfgang Dautermann

12. Januar 2010

1 Motivation

Hashfunktionen kennt man zur Verifikation von Downloads. Aber wo und wofür werden Hashfunktionen noch verwendet? Welche Hashfunktionen gibt es und worauf wird beim Entwurf einer Hashfunktion geachtet?

Häufig sind Hashfunktionen auch in IT-Nachrichtenwebseiten zu finden – meistens dann wenn ein Verfahren *geknackt* wurde. Ist es dann komplett unbrauchbar?

2 Geplante Struktur des Vortrags

- Grundlagen von Hashfunktionen.
- Einsatzbeispiele von Hashfunktionen
- Angriffe
- Ausgewählte kryptographische Hashfunktionen
  - MD4
  - MD5
  - SHA1
  - SHA3
- Zusammenfassung

3 Zielgruppe

Linux-User, die wissen wollen, was Hashfunktionen eigentlich sind, und wo Hashfunktionen eingesetzt werden, ev. Entwickler und Programmierer, die Hashfunktionen in eigenen Programmen einsetzen wollen.

4 Praktische Vorführung

Eine praktische Vorführung habe ich nicht geplant.

5 Literatur/Weblinks

- Wikipedia Artikel:`http://en.wikipedia.org/wiki/Hash_function`
- `http://www.nist.gov/hash-competition` (SHA3-Competition)
- MD5 considered harmful today: `http://www.win.tue.nl/hashclash/rogue-ca/`