RACE Integrity Primitives Evaluation Message Digest

RIPEMD-160

- eine kryptographische Hashfunktion
- Ausgabe von 160 Bit
- in Europa entwickelt
- 1996 erstmals publiziert
- Designprinzipien von MD4
- gleicht SHA-1
- arbeitet auf 512-Bit-Blöcken
- führt zwei parallele Funktionen (*left line* und *right line*) mit jeweils fünf Runden aus
- Teil des ISO/IEC Standard
- bis 2006 keine erfolgreichen Kryptoanalysen bekannt
  - August 2004, a collision was reported for the original RIPEMD not apply to RIPEMD-160
- verwendet in Bitcoin

- ist nicht patentiert

- Kleine Änderungen bei der Eingabe ergeben komplett anderen hash z.B.
  - „Thomas Wenzlaff“ = 9f0b99c682957da56df8103fea8435e5f842db40
  - „Tomas Wenzlaff“ = bf081a62d6a683763740cc34df504ddfd7d79373
  - „Thomas Wenzlaf“ = d70a59ea96c9fc226a6bf3a891b1f7558f1109f5
  - „Thomas wenzlaff“ = f5d3668b51dd6f9021cbc85f686f78d3627cbb9a
- Prof. Dr. Hans Dobbertin
  - Kryptologe 1952 - 2006
  - Uni Hannover
  - BSI
  - Lehrstuhl Ruhr-Uni Bochum
- "160-Bit RIPEMD-160 Hashes werden typisch mit 40-HEX-Zeichen dargestellt." = 309fdc3478ebcfe7b26911cdfadf60ade73a5e1c
  - Leerstring = 9c1185a5c5e9fc54612808977ee8f548b2258d31
  - Ein Leerzeichen = ac53a3aea6835b5ec12054e12d41d392e9d57b72
  - 1 Millionen mal ein a = 52783243c1697bdbe16d37f97f68f08325dc1528

www.wenzlaff.info

The RIPEMD-160 page