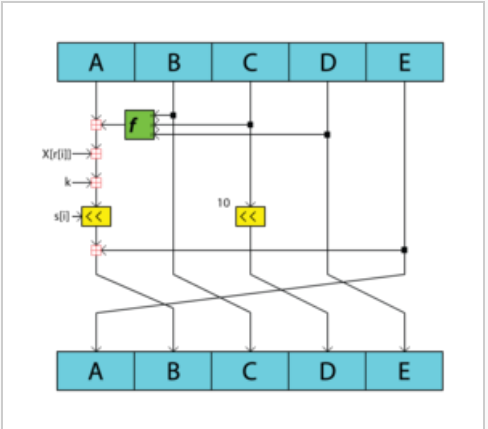
RIPEMD

From Wikipedia, the free encyclopedia
(Redirected from RIPEMD-160)

RIPEMD (**RACE Integrity Primitives Evaluation Message Digest**) is a family of cryptographic hash functions developed in Leuven, Belgium, by Hans Dobbertin, Antoon Bosselaers and Bart Preneel at the COSIC research group at the Katholieke Universiteit Leuven, and first published in 1996. RIPEMD was based upon the design principles used in MD4, and is similar in performance to the more popular SHA-1.

RIPEMD	
General	
Designers	Hans Dobbertin, Antoon Bosselaers and Bart Preneel
First published	1996
Certification	RIPEMD-160: CRYPTREC (Monitored)
Detail	
Digest sizes	128, 160, 256, 320 bits



A sub block from the compression function of the RIPEMD 160 hash algorithm.

RIPEMD-160 is an improved, 160-bit version of the original RIPEMD, and the most common version in the family. RIPEMD-160 was designed in the open academic community, in contrast to the NSA designed SHA-1 and SHA-2 algorithms. On the other hand, RIPEMD-160 appears to be used somewhat less frequently than SHA-1, which may have caused it to be less scrutinized than SHA. RIPEMD-160 is not known to be constrained by any patents.

As well as 160-bit, there also exist 128, 256 and 320-bit versions of this algorithm, called RIPEMD-128, RIPEMD-256, and RIPEMD-320, respectively. The 128-bit version was intended only as a drop-in replacement for the original RIPEMD, which was also 128-bit, and which had been found to have questionable security. The 256 and 320-bit versions diminish only the chance of accidental collision, and don't have higher levels of security (against preimage attacks) as compared to, respectively, RIPEMD-128 and RIPEMD-160.

In August 2004, a collision was reported for the original RIPEMD.[1] This does not apply to RIPEMD-160.[2]

Contents [hide]

RIPEMD-160 hashes [edit]

The 160-bit RIPEMD-160 hashes (also termed RIPE *message digests*) are typically represented as 40-digit hexadecimal numbers. The following demonstrates a 43-byte ASCII input and the corresponding RIPEMD-160 hash:

```
RIPEMD-160("The quick brown fox jumps over the lazy dog") =
37f332f68db77bd9d7edd4969571ad671cf9dd3b
```

RIPEMD-160 behaves with the desired avalanche effect of cryptographic hash functions (small changes, e.g. changing `d` to `c`, result in a completely different hash):

```
RIPEMD-160("The quick brown fox jumps over the lazy cog") =
132072df690933835eb8b6ad0b77e7b6f14acad7
```

Wikipedia
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
Français
Italiano
日本語
Polski
Српски / srpski
Edit links

The hash of a zero-length string is:

```
RIPEMD-160("") =
9c1185a5c5e9fc54612808977ee8f548b2258d31
```

See also [edit]

- Comparison of cryptographic hash functions
- Topics in cryptography

References [edit]

1. ^ Xiaoyun Wang; Dengguo Feng; Xuejia Lai; Hongbo Yu (2004-08-17). "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD" (PDF). Retrieved 2011-06-03.
2. ^ Florian Mendel; Norbert Pramstaller; Christian Rechberger; Vincent Rijmen (2006). "On the Collision Resistance of RIPEMD-160". Retrieved 2014-11-06.

External links [edit]

- RIPEMD-160: A Strengthened Version of RIPEMD (RIPEMD-160 specification and reference implementation)
- RIPEMD-160 Ecrypt page

v · t · e	**Hash functions & message authentication codes**
	Security summary
Common functions	MD5 · SHA-1 · SHA-2 · SHA-3/Keccak
SHA-3 finalists	BLAKE · Grøstl · JH · Skein · Keccak (winner)
Other functions	FSB · ECOH · GOST · HAS-160 · HAVAL · LM hash · MDC-2 · MD2 · MD4 · MD6 · N-Hash · RadioGatún · **RIPEMD** · SipHash · Snefru · Streebog · SWIFFT · Tiger · VSH · WHIRLPOOL · crypt(3) (DES)
MAC algorithms	DAA · CBC-MAC · HMAC · OMAC/CMAC · PMAC · VMAC · UMAC · Poly1305-AES
Authenticated encryption modes	CCM · CWC · EAX · GCM · IAPM · OCB
Attacks	Collision attack · Preimage attack · Birthday attack · Brute force attack · Rainbow table · Distinguishing attack · Side-channel attack · Length extension attack
Design	Avalanche effect · Hash collision · Merkle–Damgård construction
Standardization	CRYPTREC · NESSIE · NIST hash function competition
Utilization	Salt · Key stretching · Message authentication

v · t · e	**Cryptography**
	History of cryptography · Cryptanalysis · Cryptography portal · Outline of cryptography
	Symmetric-key algorithm · Block cipher · Stream cipher · Public-key cryptography · Cryptographic hash function · Message authentication code · Random numbers · Steganography

Categories: Cryptographic hash functions