Redvers Consulting Ltd

Redvers Hashing Algorithm

The Redvers Hashing Algorithm can be used to produce SHA-1, SHA-2 or SHA-3 message digests of 224, 256, 384 or 512 bit lengths, ensuring safe, authenticated data transfer to/from any location.

Main features:

- Runs on any COBOL platform
- Distributed in COBOL source code ("cloaked")
- Calculates SHA-1, SHA-2 and SHA-3 series hash totals, in standard, truncated or Extendable-Output forms
- MAC generation
- Hash produced in binary, hexadecimal and Base64 formats
- Fast, efficient, professional and fully scalable
- Supports calls from batch or online
- **Free 30 day trial available**

Data selected for hashing/MAC generation can consist of a single data string or a series of multiple strings resulting in a single hash total (message digest) or MAC.

Message digests can be used within many security reliant applications for encryption key derivation, pseudorandom number generation and to generate or verify digital signatures.

The **Redvers Hashing Algorithm** is used by customers all over the world, running on **iSeries/AS400, UNIX, HP, CA-Realia, Fujitsu Siemens BS2000, Micro Focus** and **IBM mainframe** platforms.

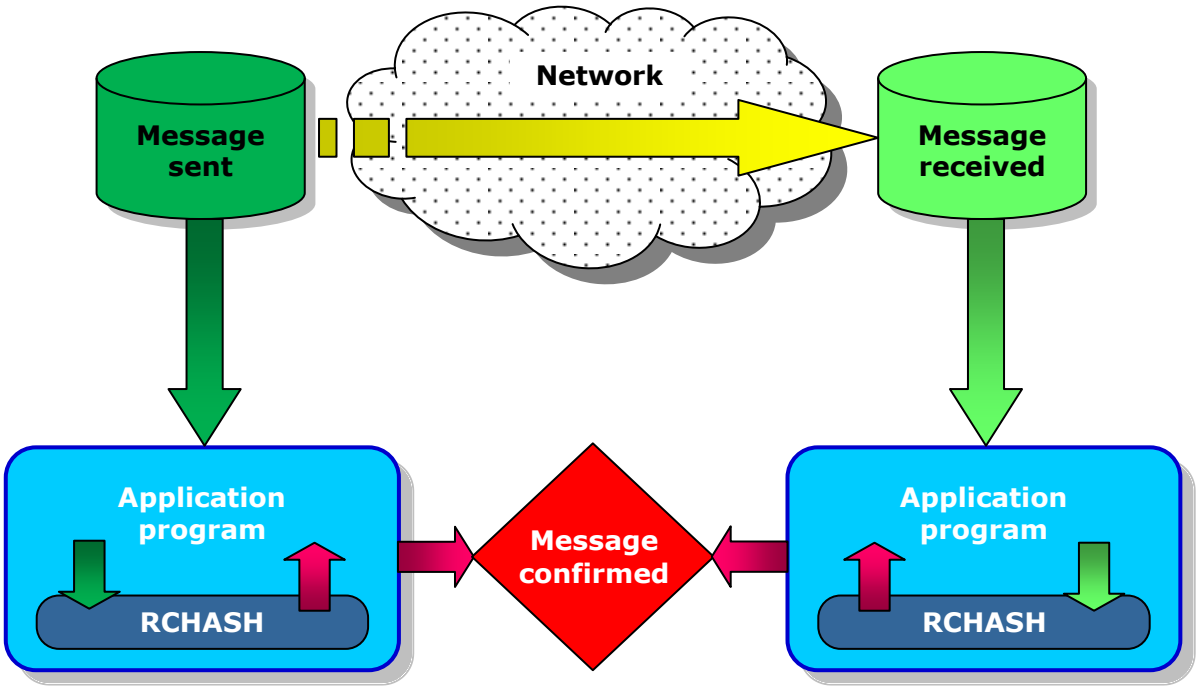
How it Works

The **Redvers Hashing Algorithm** consists of an easy to use, COBOL subroutine (**RCHASH**) that is called from an application to hash any single data string or series of strings.

Selecting the SHA-1 algorithm will produce a hash total of 160 bits (20 bytes). SHA-2 and SHA-3 algorithms can produce hash totals of 224 bits (28 bytes), 256 bits (32 bytes), 384 bits (48 bytes) or 512 bits (64 bytes). Truncated SHA-2 totals (SHA-512/224 and SHA-512/256) and Extendable-Output SHA-3 totals (SHAKE128 and SHAKE256) can also be generated.

The choice of algorithm (SHA-1, SHA-2 or SHA-3) and hash total length is decided by setting an 88 level flag in the calling parameters. The subroutine requires no external files and may be called in batch or on-line modes.

The diagram below shows how hashing might be used to verify the transfer of confidential data from one environment to another:



The Redvers Hashing Algorithm creates standard NIST SHA message digests so that the generated hash values will match values generated by other standard SHA hashing algorithms.

Technical Information

The **Redvers Hashing Algorithm** 2.4 supports thirteen functions within the three SHA (Secure Hash Algorithm) family types:

- SHA-1 (160 bits)
- SHA-2 (224, 256, 384 & 512 bits) plus two truncated 512 versions (SHA-512/224 and SHA-512/256)
- SHA-3 (224, 256, 384 & 512 bits) plus two Extendable-Output versions (SHAKE128 and SHAKE256)

Specifications for the SHA-1 and SHA-2 algorithms can be found in the National Institute of Standards and Technology (NIST) publication **FIPS Publication 180-4**: [http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf]. Specification for the SHA-3 algorithm can be found in **FIPS Publication 202** [http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf]. SHA-3 is based on the Keccak algorithm, defined in **Keccak Reference**: [http://keccak.noekeon.org/Keccak-reference-3.0.pdf].

The Redvers Hashing Algorithm can also be used to generate keyed-hash based Message Authentication Codes (MACs). Specification for MAC generation can be found in **FIPS 198-1:** [http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf].

Information passed to **RCHASH** can consist of a single data string or a series of strings from an input file or database row. The resulting hash/MACs are returned in binary, hexadecimal and Base64 formats for easy application processing.

Although SHA hashing can be used to safely represent confidential information, it cannot be used as a substitute for data encryption if the original data string needs to be recovered. This is because data information is destroyed in the hashing process, making it impossible to recover the original data string from a message digest. If decryption is required, an NIST validated encryption/decryption algorithm like the **Redvers Encryption Module** is recommended.

The Product Package

A perpetual license for the **Redvers Hashing Algorithm** can be provided for a one-off fee. Alternatively, the software can be leased on an annual basis for 20% of the perpetual license cost (minimum two years).

All licenses include:

- Product source code ("cloaked")
- Sample COBOL calling program
- User Guide
- Corporate level software license
- Money back guarantee
- Product upgrades and support via email*

Additional options:

- 24 x 7 telephone hotline support
- Software escrow agreement with Software Escrow Solutions

Software and documents are shipped in the form of email attachments unless otherwise requested. Installation is performed by copying the source code text into your COBOL source code library and running your standard site compiler.

Full pricing details can be found at:
http://www.redversconsulting.com/hashing_algorithm_pricing.php

* Free for the first two years followed by a minimal annual fee.

About Redvers Consulting

Redvers Consulting have been providing top quality products and services for COBOL applications since 1988. Our clients are primarily large financial institutions in Europe and North America, although we also have customers in many other business and geographical areas.

Our ability to deliver software in COBOL source code form, gives customers reliable, efficient and perfectly integrated solutions to business needs. Source code distribution also means our software will run on all hardware platforms and operating systems: *EBCDIC, ASCII, big endian or little endian*.

We are business partners with **IBM**, **HP** and **Fujitsu Siemens**, and our development team are members of the **Professional Contractors Group**. In 2009 we won the Thames Gateway **Best use of Technology Award**.

Our client list includes:

Agora (FR)
ANZ (AUS)
Barclays Life Assurance (UK)
Canada Life Assurance (UK)
Deutsche Bank (USA)
Deutsche Rentenversicherung Bund (DE)
FirstBank (USA)
Fiserv (USA)
GMAC Insurance (USA)
Hanesbrands (USA)
John Deere (USA)
LBS / Finanz Informatik (DE)
J P Morgan (USA)
Oppenheimer (USA)
Pacific Gas (USA)
Network Rail (UK)
R+V Allgemeine Versicherung (DE)
Sasktel (CAN)
SEB (DE)
Standard Life Assurance (UK)
Suncorp (AUS)
SunGard / FIS (USA)
WorkSafeBC (CAN)
Zurich Insurance (UK & SUI)

Contact: https://www.redversconsulting.com/contact.php

Development Office:

Redvers Consulting Ltd
44 Broadway,
London E15 1XH,
UK

Tel: +44 (0)203 130 0773
Fax: +44 (0)700 603 8655

Accounts Office:

Redvers Consulting Ltd
1st Floor, 48 Dangan Rd,
London E11 2RF,
UK

Tel: +44 (0)870 922 0633
Fax: +44 (0)707 505 5472

German Office:

Redvers Consulting Ltd
Postfach 30 03 26,
50773 Köln,
Deutschland

Tel: +49 (0)221 1704 9000
Fax: +49 (0)221 271 1016