Redvers Consulting Ltd

Redvers Hashing Algorithm

Der „Redvers Hashing Algorithm" dient dazu, SHA-1, SHA-2 oder SHA-3 Nachrichtenzusammenfassungen mit 224, 256, 384 oder 512 Bit Länge erstellen, was einen sicheren, authentifizierten Datentransfer zu und von jedem Ort ermöglicht.

Merkmale:

- Läuft auf jedem Rechner, der COBOL ausführen kann
- Wird als COBOL Quellprogramm lizensiert (verschlüsselt)
- Errechnet Hashsummen nach SHA-1, SHA-2 oder SHA-3, im Standard-, abgekürzten oder Extendable-Output Format
- Hash MAC (HMAC) Generierung
- Hash wird erzeugt im Binär-, Hexadezimal und Base64-Format
- Schnell, effizient, professionell und skalierbar
- Kann im Batch-Modus oder Online (z.B. CICS) aufgerufen werden
- **Kostenlose 30-Tage-Demoversion**

Daten, die zum Hashen oder MAC-Generierung vorgesehen sind, können aus einzelnen Datenfeldern oder einer Reihe aufeinanderfolgender Strings bestehen, was zu einer einzigen Hashsumme (Message Digest) oder MAC führt.

Message Digests können innerhalb vieler sicherheitsrelevanter Anwendungen verwendet werden: zur Erzeugung eines Keys zur Verschlüsselung, Erzeugung pseudozufälliger Zahlen, und um digitale Signaturen zu erzeugen oder zu überprüfen.

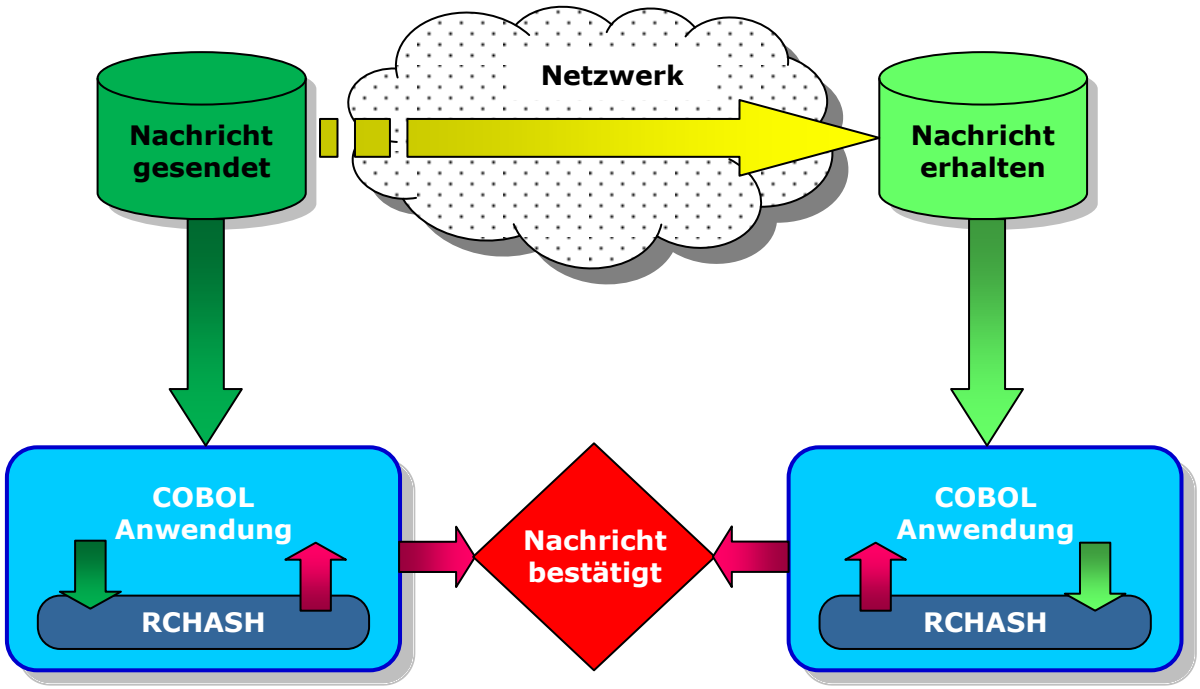
Überblick über die Funktionsweise

Der „**Redvers Hashing Algorithm**" besteht aus einem einfach anzuwendenden COBOL-Unterprogramm (RCHASH), das vom Anwendungsprogramm aufgerufen wird, um einen einzelnen Datenstring oder eine Gruppe von Strings zu hashen.

Die Auswahl des SHA-1 Algorithmus führt zu einer Hashsumme von 160 Bit (20 Bytes) Länge. Die SHA-2 und SHA-3 Algorithmen können Hashsummen von 224 Bit (28 Bytes), 256 Bit (32 Bytes), 384 Bit (48 Bytes) oder 512 Bit (64 Bytes) erzeugen. Abgekürzte SHA-2-Summen (SHA-512/224 und SHA-512/256) und Extendable-Output SHA-3-Summen (SHAKE128 und SHAKE256) können ebenfalls erzeugt werden, ebenso wie Message Authentication Codes (MACs).

Die Auswahl des gewünschten Algorithmus (SHA-1, SHA-2 oder SHA-3) und die Hashlänge erfolgt über die entsprechende Belegung eines Schalters auf 88er-Stufe in den aufrufenden Parametern. Das Unterprogramm benötigt keinen externen Dateizugriff und kann sowohl im Batch- als auch im Onlinemodus aufgerufen werden.

Das Schaubild zeigt, wie Hashing verwendet werden kann, um die Übertragung vertraulicher Daten aus einer Umgebung in eine andere zu verifizieren:



Der „Redvers Hashing Algorithm" erzeugt die standardisierten NIST SHA Nachrichtenzusammenfassungen, so daß die erzeugten Hashwerte den mit anderen üblichen SHA Hashing-Algorithmen erzeugten Werten entsprechen.

Technische Informationen

Der „**Redvers Hashing Algorithm**" 2.4 unterstützt 13 Hashfunktionen innerhalb der drei SHA (Secure Hashing Algorithm) Familien:

- SHA-1 (160 bit)
- SHA-2 (224, 256, 384 und 512 Bit) sowie zwei abgekürzte 512-Funktionen (SHA-512/224 und SHA-512/256)
- SHA-3 (224, 256, 384 und 512 Bit) sowie zwei Extendable-Output Funktionen (SHAKE128 und SHAKE256)

Die Spezifikationen für die SHA-1 und SHA-2 Algorithmen finden sich in der NIST (National Institute of Standards and Technology) FIPS Publication 180-4. Die Spezifikation für den SHA-3 Algorithmus finden sich in der NIST FIPS Publication 202. SHA-3 basiert auf dem Keccak-Algorithmus, wie er im Keccak Reference definiert wurde.

Der „**Redvers Hashing Algorithm**" kann auch dazu verwendet werden, um keyed-hash basierte Message Authentication Codes (HMACs) zu erzeugen. Spezifikationen zur HMAC-Erzeugung finden sich in der NIST FIPS 198-1.

Daten, die an **RCHASH** übergeben werden, können aus einem einzelnen Datenstring oder einer Reihe von Strings bestehen, aus einer Eingabedatei oder einer Zeile in einer Datenbank. Der erzeugte Hash/MAC wird im Binär-, Hexadezimal und Base64-Format zurückgegeben, damit das Anwendungsprogramm in jedem Fall damit weiterarbeiten kann.

SHA Hashing kann zwar dafür vewendet werden, um vertrauliche Informationen sicher zu verifizieren, es ist jedoch kein Ersatz für eine Datenverschlüsselung, wenn die Notwendigkeit besteht, die ursprünglichen Datenstrings wiederherzustellen. Wenn Sie eine Entschlüsselung benötigen, empfehlen wir einen vom NIST validierten Ver- und Entschlüsselungsalgorithmus wie etwa das „**Redvers Encryption Module**" is recommended.

Das Produktangebot

Eine Dauerlizenz für der „**Redvers Hashing Algorithm**" kann für eine einmalige Gebühr erworben werden. Alternativ kann die Software auch gemietet werden für eine jährliche Gebühr, die 20% des Betrags der Dauerlizenz beträgt.

Für diesen Betrag erhalten Sie:

- den Quellcode (verschlüsselt)
- Beispiel für rufende Programme
- Handbücher
- eine unternehmensweit gültige Softwarelizenz
- Geld-zurück-Garantie
- Softwareupgrades und Support per E-Mail*

*Kostenlos für das erste Jahrmit einer geringen jährlichen Folgegebühr.

Zusätzliche Optionen:

- telefonischer Support rund um die Uhr
- Software Escrow / Quellcodehinterlegung bei Software Escrow Solutions.

Die aufgeführte Software und Handbücher werden als Textdateien und PDF E-Mail-Anhänge geliefert, wenn keine abweichenden Vereinbarungen getroffen wurden. Sie werden installiert, indem Sie den Quelltext manuell in Ihre COBOL Quelltextbibliothek kopieren, und dann mit Ihrem üblichen Compiler kompilieren und linken.

Ausführliche Informationen zu den Preisen finden Sie auf:
https://www.cobol.de/hashing_algorithm_pricing.php

Über Redvers Consulting

Redvers Consulting bietet seit 1988 erstklassige Produkte und Dienstleistungen für COBOL-Anwendungen. Unser Ansatz, die Software als Quellcode auszuliefern, ermöglicht unseren Kunden die Erfüllung ihrer geschäftlichen Anforderungen mit einer zuverlässigen, effizienten und perfekt integrierten Lösung.

Unsere Kunden sind überwiegend große Finanzdienstleister in Großbritannien und den USA. In zunehmendem Maße sind wir im deutschsprachigen Raum und auch in anderen Branchen tätig.

Da unsere Software als verschlüsselter Quellcode ausgeliefert wird, bieten wir Unterstützung für alle Hardwareplattformen und Betriebssysteme, für die ein COBOL-Compiler existiert - EBCDIC, ASCII, big endian und little endian.

Einige unserer Kunden:

Agora (FR)
ANZ (AUS)
BAE Systems (USA)
Canada Life Assurance (UK)
Deutsche Bank (USA)
Deutsche Rentenversicherung Bund (DE)
FirstBank (USA)
Fiserv (USA)
GMAC Insurance (USA)
Hanesbrands (USA)
John Deere (USA)
Landesbank Hessen Thüringen (DE)
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 & CHE)

Kontakt: https://www.cobol.de/contact.php

Deutsches Büro:

Redvers Consulting Ltd
Scharfeneckweg 2,
50739 Köln,
Deutschland

Tel: +49 (0)221 1704 9000

Hauptbüro:

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

Tel: +44 (0)870 922 0633

Entwicklungsbüro:

Redvers Consulting Ltd
16-18 Woodford Road,
London E7 0HA,
UK

Tel: +44 (0)208 522 7404