Redvers Consulting Ltd

Redvers Encryption Module

Die Redvers Datenverschlüsselungsroutine „Redvers Encryption Module" bietet Ihren COBOL-Anwendungen Zugriff auf den Advanced Encryption Standard (AES) Algorithmus, um vertrauliche Daten unter Verwendung eines 128, 192 oder 256-Bit Schlüssels sicher verschlüsseln und entschlüsseln zu können.

Merkmale:

- Vom NIST zertifiziert (Nummer 1141)
- Läuft auf jedem Rechner, der COBOL ausführen kann
- Unterstützt alle Geheimhaltungsgrade
- Wird als COBOL Quellprogramm lizensiert (verschlüsselt)
- Schnell, effizient, professionell und skalierbar
- Kann Ihre Produktionsdaten in sichere Testdaten umwandeln
- Kann im Batch-Modus oder Online aufgerufen werden
- **Kostenlose 30-Tage-Demoversion**

Die zu verschlüsselnden Daten können sich in einem einzelnen Feld, in mehreren Feldern oder in einem ganzen Satz befinden. Diese Verschlüsselung auf Feld-Ebene kann dafür verwendet werden, nur schützenswerte Daten zu bearbeiten, wodurch Anwendungsprogramme auf nicht so sensible Daten zugreifen können, ohne zuvor die gesamte Datei oder Datenbank zu ver- oder entschlüsseln.

Das „**Redvers Encryption Module**" wird von Kunden auf der ganzen Welt genutzt, und läuft auf **iSeries/AS400**, **UNIX**, **HP**, **Linux**, **Fujitsu Siemens BS2000**, **Micro Focus** und **IBM Mainframe-Systemen**. Es wird häufig in Anwendungen genutzt, die dem **PCI**-Sicherheitsstandard der Kreditkartenindustrie entsprechen.

Wie sicher ist die AES-Verschlüsselung?

Wir zitieren hier aus einer Beschreibung der US-amerikanischen Staatlichen Standard- und Technologiebehörde „National Institute of Standards and Technology" (NIST):

Aufgrund seiner verbesserten Sicherheit und Effizienz wird AES letztlich den früheren Datenverschlüsselungsstandard (DES) der NIST ablösen, der seit 1977 verwendet wird, und Triple DES, zertifiziert im Jahr 1999. Wenn man einen Rechner bauen könnte, der einen DES-Schlüssel in einer Sekunde entschlüsselt, dann würde dieser Rechner ungefähr 149 Billionen (1.000 Milliarden) Jahre benötigen, um einen 128-Bit AES-Schlüssel zu brechen; das ist länger, als unser Universum existiert. Im Jahr 1997 versammelte NIST die besten Kryptographen der Welt, um Algorithmen für den neuen Verschlüsselungsstandard zu entwickeln und zu bewerten. Nach vierjähriger Arbeit entstand der neue AES.

Überblick

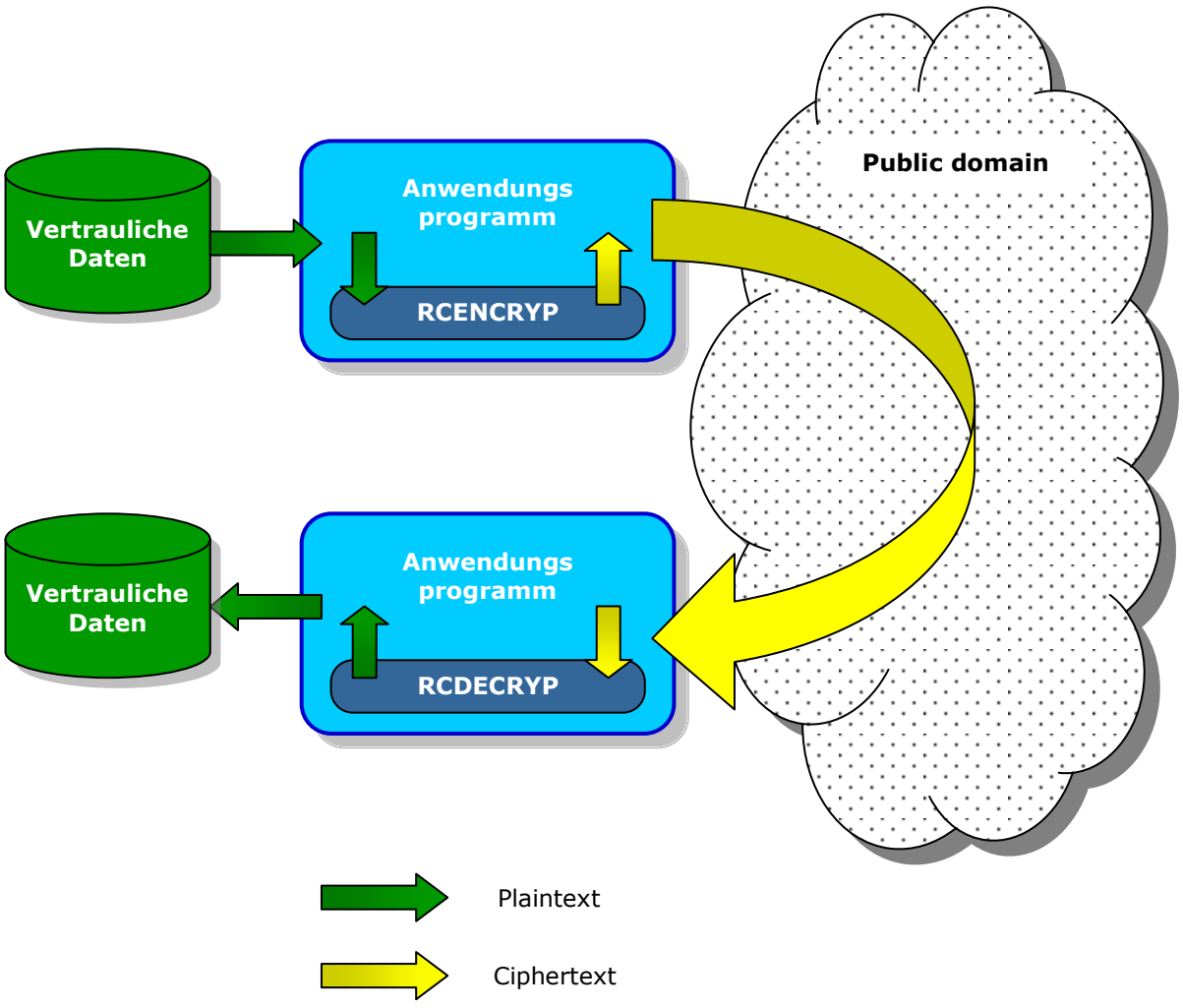
Die Datenverschlüsselungsroutine „**Redvers Encryption Module**“ besteht aus zwei COBOL Unterprogrammen, wobei einer für die Verschlüsselung der Daten (**RCENCRYP**) und das andere für die Entschlüsselung (**RCDECRYP**) zuständig ist. Diese Unterprogramme können von jeder Anwendung aufgerufen werden unabhängig von der verwendeten Plattform, im Batch- oder Onlinemodus.

Zu verschlüsselnde Daten (Plaintext) werden an **RCENCRYP** als Zeichenstring, der im Hauptspeicherbereich der Anwendung gehalten wird, übergeben. **RCENCRYP** liefert dann den entsprechenden, verschlüsselten String zurück (codierter Text). Verschiedene Parameter, wie Länge des Strings, Geheimhaltungsgrad und Schlüssel werden in einem Kommunikationsblock mit festem Format übertragen.

Die Entschlüsselung geschieht, indem der codierte Text-String an **RCDECRYP** übergeben wird, zusammen mit dem Kommunikationsblock. **RCDECRYP** liefert dann den entsprechenden lesbaren Plaintext-String zurück.

Das „**Redvers Encryption Module**“ nutzt die Standard-AES-Verschlüsselungsroutine, was bedeutet, daß es verschlüsselten Text erzeugen kann, der dann von anderen AES-konformen Routinen entschlüsselt werden kann, und daß es seinerseits Text entschlüsseln kann, der von anderen AES-konformen Routinen erstellt wurde.

Die für die Ver-/Entschlüsselung bestimmten Daten können aus einem einfachen Feld, einem Teil eines Datensatzes, einem vollständigen Datensatz oder aus einer vollständigen Datei bestehen, wobei in letzterem Fall die Datensätze nahtlos aneinander angefügt sind.



Technische Informationen

Die Datenverschlüsselungsroutine „**Redvers Encryption Module**" nutzt den „Advanced Encryption Standard" (AES) Algorithmus, manchmal als „Rijndael Algorithmus" bezeichnet, um Daten zu verschlüsseln und entschlüsseln unter Verwendung eines 128, 192 oder 256 Bit-Schlüssels. Der symmetrische Block-Code nach AES wurde im Jahr 2001 vom National Institute of Standards and Technology (NIST) in der US-amerikanischen FIPS Publication 197 vorgestellt.

Der AES-Algorithmus wird in Verbindung mit einem von fünf möglichen Vertraulichkeitsmodi genutzt, wie sie von NIST veröffentlicht wurden in der „Special Publication 800-38A". Diese Modi sind im einzelnen: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feed Back (CFB), Output Feed Back (OFB) und Counter (CTR).

Verschlüsselung mit erhaltenem Format wird erreicht, indem einer von fünf zusätzlichen Vertraulichkeitsmodi verwendet wird, was dazu führt, daß jegliche Auswahl numerischer, kleingeschriebener, großgeschriebener, gemischter Zeichensatz oder alphanumerischer verschlüsselter Texte erzeugt werden kann. In all diesen Fällen hat der erzeugte, verschlüsselte Text die selbe Länge wie der zu verschlüsselnde Text, der als Eingabe dient, was die Tokenisierung vertraulicher Daten vereinfacht. Dabei wird der FF1-Algorithmus verwendet, wie er in der NIST Special Publication 800-38G definiert wurde.

Die Erstellung von **CMAC** (Cipher Message Authentication Code) auf der Grundlage einer Verschlüsselung und die Verschlüsselung mittels **CCM** (Mode for Authentication and Confidentiality) sind die Grundlage für authentifizierte Datenübertragung mit zwei Vertraulichkeitsmodi: MAC & CCM. Diese Modi sind definiert in der NIST Special Publication 800-38B und in der Special Publication 800-38C.

Die **„Redvers Encryption Module"** unterstützt und entspricht allen oben genannten Vertraulichkeitsmodi und wurde vom Cryptographic Algorithm Validation Program (CAVP) mit NIST validiert - Validierungsnummer 1141.

Der Hauptspeicher, der von unserer Routine für die vorübergehende Speicherung des unverschlüsselten Textes und des Verschlüsselungscodes verwendet wird, wird mit einem Aufruf von „**clean storage**" gesäubert, nachdem alle Daten ver- oder entschlüsselt wurden.

Um die Erzeugung von Testdaten und/oder codiertem Text, der einfach verändert und übertragen werden kann, zu erleichtern, kann codierter Text im base64-Format oder als einfache Ganzzahlen erzeugt werden (es kann dabei zu einigen Verkürzungen kommen).

Die Verschlüsselung geschieht mit einer Geschwindigkeit von **125.000 Bytes pro Sekunde**, gemessen im ECB Modus mit einem 256 Bit Schlüssel. Entschlüsselung erfolgt mit **60.000 Bytes pro Sekunde** im ECB Modus mit einem 256 Bit Schlüssel. Diese Benchmarks wurden gemessen auf einem IBM zSeries Mainframe unter z/OS 1.10.

Das Produktangebot

Eine Dauerlizenz für das „**Redvers Encryption Module**" 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.

Alle Lizenzen beinhalten:

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

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: http://www.cobol.de/data_encryption_pricing.php

* Kostenlos in den ersten zwei Jahren mit einer geringen jährlichen Folgegebühr.

Über Redvers Consulting

Redvers Consulting wurde 1988 gegründet. Das Unternehmen bietet Software und Dienstleistungen auf der Grundlage der Programmiersprache COBOL an.

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.

In den Anfangsjahren lag der Schwerpunkt unserer Arbeit auf der Optimierung von Batchläufen, und diese Aufgabe setzt sich bis heute fort. In jüngster Zeit haben wir uns verstärkt mit der Erstellung von Lösungen und Tools auf COBOL-Basis beschäftigt. Die neuen Entwicklungen auf diesem Gebiet sind das „Redvers COBOL XML Interface" und das „Redvers Encryption Module".

Wir sind Businesspartner von IBM, HP und Fujitsu Siemens und Mitglieder unserer Entwicklungsabteilung sind Mitglied in der Professional Contractors Group. Wir haben zahlreiche Business-Awards in London und in Großbritannien erhalten.

Einige unserer Kunden:

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)

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

Deutsches Büro:

Redvers Consulting Ltd
Postfach 30 03 26,
50773 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