Redvers Consulting Ltd

Redvers Encryption Module

The Redvers Encryption Module is an AES (Advanced Encryption Standard) 128, 192 or 256 bit encryption and decryption algorithm, specifically designed for COBOL applications.

Main features:

- Validated by NIST (number 1141)
- Runs on any COBOL platform
- Supports all confidentiality modes
- Creates Format-Preserved (Fixed Format) ciphertexts
- Distributed in COBOL source code ("cloaked")
- Fast, efficient, professional and fully scalable
- Can be used to turn production data into safe test data
- Supports calls from batch or online
- **Free 30 day trial available**

Data selected for encryption can consist of a single field, a group of fields or a complete record. This field level encryption can be used to target sensitive data only, giving applications access to non-sensitive data without the need for unnecessary file/volume encryption and decryption.

The **Redvers Encryption Module** 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. It is frequently used in **PCI** compliant applications and is suitable for securing personal data under **GDPR**.

How strong is AES encryption? Here's an excerpt from a National Institute of Standards and Technology (NIST) Fact Sheet:

"Because of its greater strength and efficiency, AES eventually will replace NIST's earlier Data Encryption Standard (DES), in use since 1977, and Triple DES, approved in 1999. Assuming that one could build a machine that could recover a DES key in a second, then it would take that machine approximately 149 trillion (thousand-billion) years to crack a 128-bit AES key; this is longer than our universe has existed. In 1997, NIST invited the world's best cryptographers to submit and help evaluate algorithms for the new encryption standard. This four-year effort resulted in the new AES."

How it Works

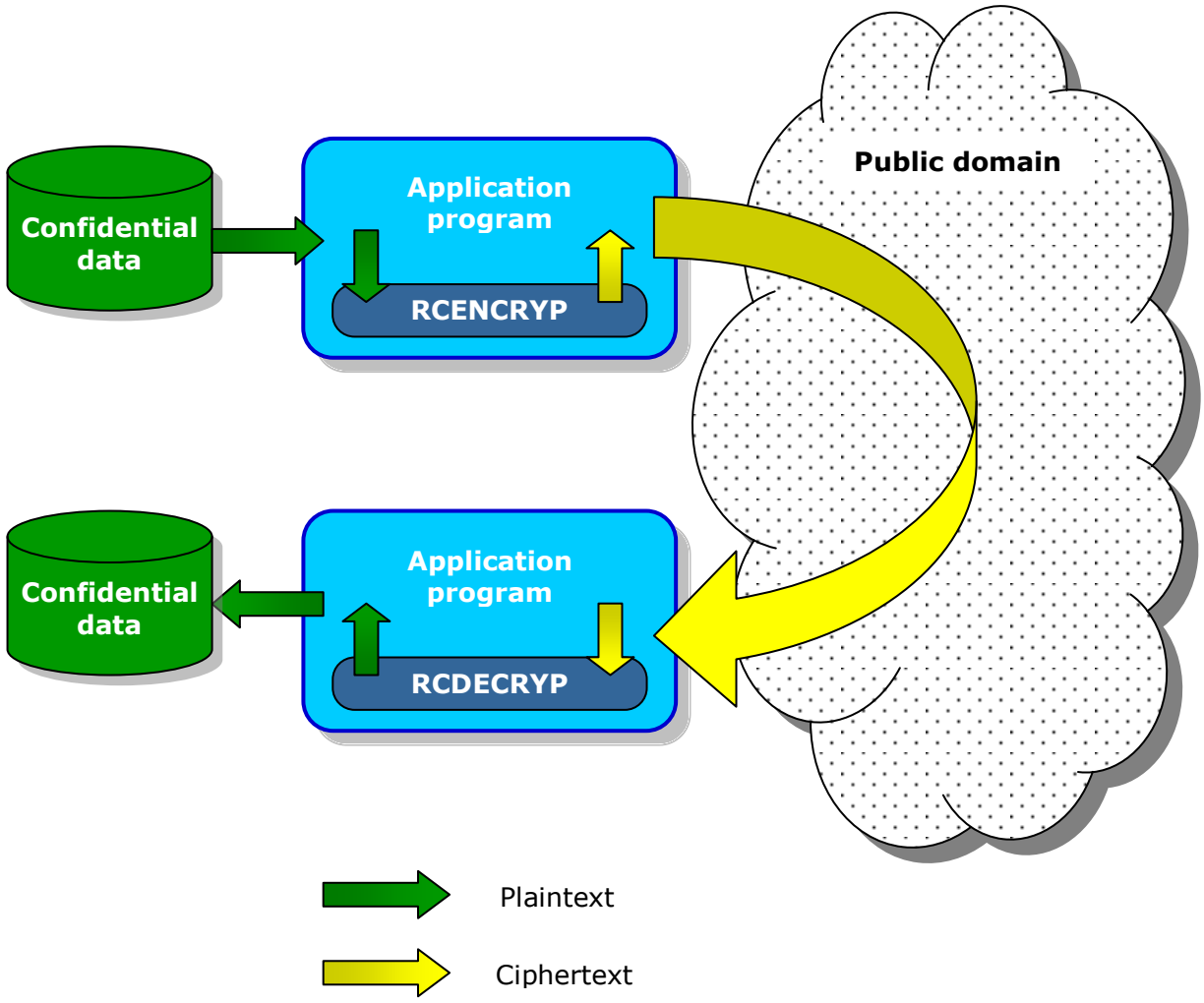
The **Redvers Encryption Module** consists of a pair of efficient, easy to use, COBOL subroutines (**RCENCRYP** and **RCDECRYP**) that encrypt and decrypt data strings as required. These subroutines may be called in batch or on-line modes.

Data to be encrypted (plaintext) is passed to **RCENCRYP** in the form of a character string held in application storage. **RCENCRYP** then returns the equivalent encrypted string (ciphertext). Parameter information, including the string length, confidentiality mode and encryption key are transferred in a fixed format communication block.

Decryption is performed by passing the ciphertext string to **RCDECRYP** along with the communication block. **RCDECRYP** then returns the equivalent readable plaintext.

Secure test data can also be generated by **RCENCRYP** based on the encrypted ciphertext. Alphanumeric values are returned in the form of a Base64 character string and numeric values are returned as an integer.

The diagram below shows how the encryption / decryption routines might be used to transfer confidential data from one secure environment to another:



The Redvers Encryption Module runs the standard AES cipher, which means it can generate cipher-text for decryption by other AES ciphers and decrypt ciphertext, generated by other AES ciphers.

Technical Information

The **Redvers Encryption Module** (2.1) uses the Advanced Encryption Standard (**AES**) algorithm, sometimes known as the **Rijndael** algorithm, to encrypt and decrypt data using **128**, **192** or **256** bit keys. The AES symmetric block cipher was announced in 2001 by the National Institute of Standards and Technology (NIST) in U.S. FIPS PUB 197.

The AES algorithm is used in conjunction with one of five **confidentiality modes**, defined in NIST Special Publication 800-38A.

Format-Preserving Encryption is achieved using one of five additional confidentiality modes, to produce any selection of numeric, upper case, lower case, mixed case or alphanumeric ciphertexts. The precise algorithm used is the FF1 algorithm, defined in NIST Special Publication 800-38G. In each case, the generated ciphertext is the same length as the input plaintext.

Encryption based **CMAC** (Cipher Message Authentication Code) generation and **CCM** (Mode for Authentication and Confidentiality) encryption, provide for authenticated data transfer using two more confidentiality modes: MAC & CCM respectively. These modes are defined in NIST Special Publication 800-38B and Special Publication 800-38C.

The **Redvers Encryption Module** fully supports and conforms to all confidentiality modes and has been validated by the Cryptographic Algorithm Validation Program (CAVP) at NIST - validation number 1141.

Redvers Encryption Module programs do not contain information that can be used to derive encryption keys or plaintext values. These programs are simply computer instructions that result in the publicly known, AES cipher logic process. They can therefore be used in production and development environments.

Machine memory used by the programs to temporarily store plaintext and encryption keys, is wiped clean with a "**clean storage**" call, once all data has been encrypted or decrypted.

Encryption rates are **125,000 bytes per second**, decryption rates are **60,000 bytes per second** (running ECB mode with a 256 bit key). Faster decryption rates can be achieved if CFB, OFB or CTR confidentiality modes are used, as these modes use the forward cipher for decryption. All benchmark timings were performed on an IBM zSeries mainframe running z/OS 1.10.

The Product Package

A perpetual license for the **Redvers Encryption Module** 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:
https://www.redversconsulting.com/data_encryption_pricing.php

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

About Redvers Consulting

Redvers Consulting provide niche software products for the integration, modernization and security of COBOL applications. 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*.

Redvers Consulting have received many business awards over the years, including winning the **Best use of Technology** category in the Thames Gateway Business Awards. We are also business partners with **IBM**, **Micro Focus** and **Fujitsu**.

Our client list includes:

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)
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)

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

Development Office:

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

Tel: +44 (0)208 522 7404

Accounts Office:

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

Tel: +44 (0)870 922 0633

German Office:

Redvers Consulting Ltd
Scharfeneckweg 2,
50739 Köln,
Deutschland

Tel: +49 (0)221 1704 9000