

Redvers Consulting Ltd

Redvers Encryption Device



The Redvers Encryption Device 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
- Distributed in COBOL source code ([cloaked](#))
- Fast, efficient, professional and fully scalable
- Operates at field, record or file level
- Can be used to turn production data into safe test data
- Supports calls from batch or online
- [Free 30 day trial available](#)

The Redvers Encryption Device 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.

Data selected for encryption can consist of a single field, part of a record, a complete record or a file of records concatenated end-to-end. 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 decryption.

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

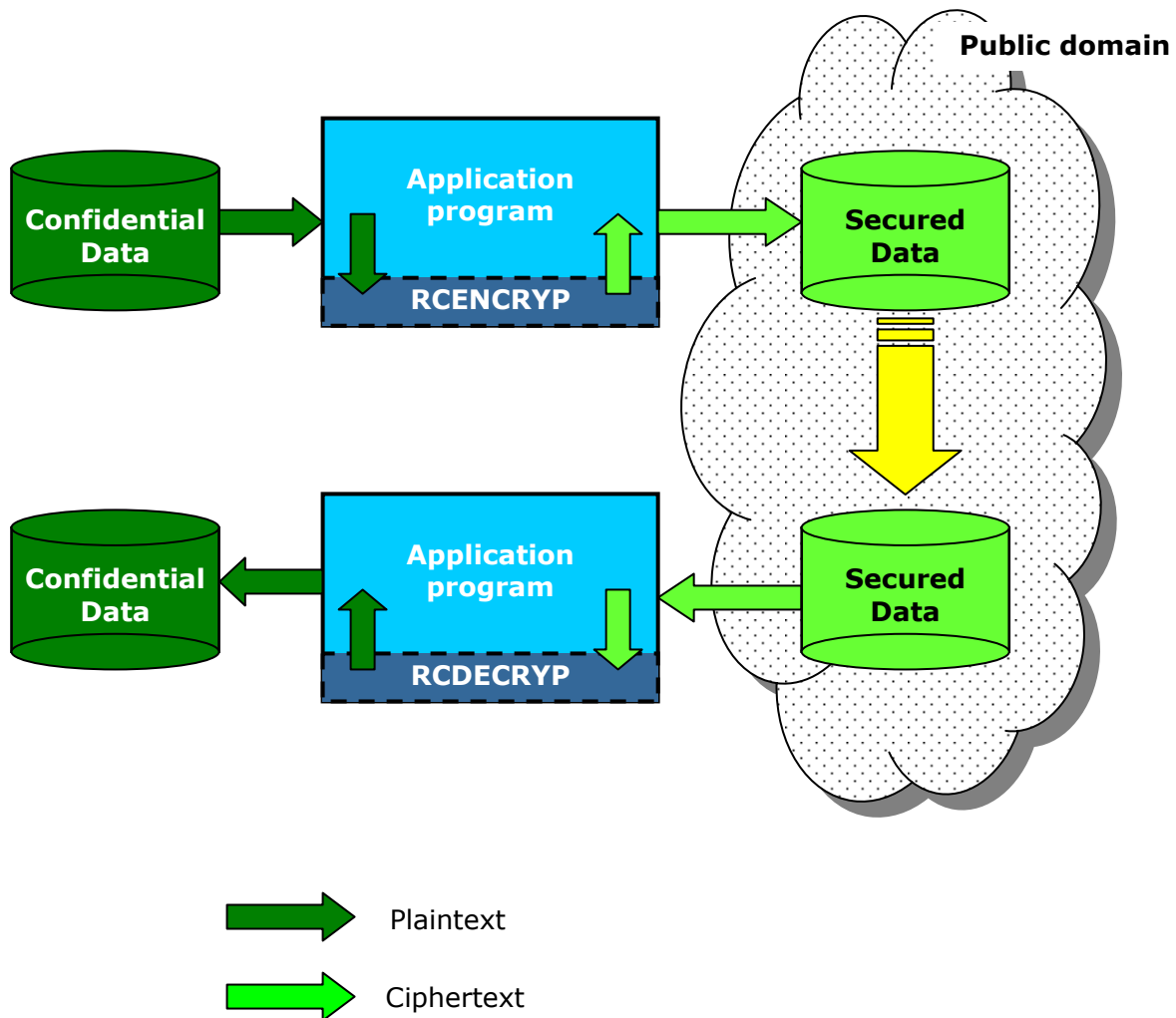
The Redvers Encryption Device consists of a pair of efficient, easy to use, COBOL subroutines (**RCENCRYP** and **RCDECRYP**) that encrypt and decrypt data strings as required. These subroutines may be called in batch or on-line modes.

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 string lengths, 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.

The Redvers Encryption Device runs the standard AES cipher so that it can generate ciphertext for decryption by other AES ciphers and decrypt ciphertext, generated by other AES ciphers.

Secure test data can also be generated by **RCENCRYP**. Alphanumeric data is returned in the form of a base64 character string and numeric values are returned as an integer.



Technical Information

The Redvers Encryption Device 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](http://www.nist.gov) (NIST) in U.S. [FIPS PUB 197](http://www.fips.gov) [<http://www.csrc.nist.gov/publications/PubsFIPS.html>]. Its worldwide use is encouraged by the U. S. Government and many specialist security organizations.

The AES algorithm is used in conjunction with one of five **confidentiality modes**, defined in NIST [Special Publication 800-38A](http://www.nist.gov) [http://www.csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html]. These modes are: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feed Back (CFB), Output Feed Back (OFB) and Counter (CTR). The Redvers Encryption Device supports all these confidentiality modes.

The Redvers Encryption Device fully conforms to [FIPS PUB 197](http://www.fips.gov) and [Special Publication 800-38A](http://www.nist.gov) specifications and has been validated by the [Cryptographic Algorithm Validation Program \(CAVP\)](http://www.nist.gov) at the NIST – [number 1141](http://www.nist.gov): [http://csrc.nist.gov/groups/STM/cavp/documents/aes/ae_sval.html]

Redvers Encryption Device 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 device to temporarily store plaintext and encryption keys, is wiped clean with a “**clean storage**” call, once all data has been encrypted or decrypted.

Due to the fact that COBOL data can terminate with a binary field, the Redvers Encryption Device uses the [Public-Key Cryptography Standards \(PKCS#5\)](http://www.rsa.com) [<http://www.rsa.com/rsalabs/node.asp?id=2127>] **padding** method (*ECB, CBC and CFB confidentiality modes only*).

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 Device costs **6,000 US dollars** or equivalent currency. Alternatively, the software can be leased on an annual basis for just **1,200 US dollars** per year.

Your purchase includes:

- Product source code (*cloaked*)
- Sample COBOL calling program
- User Guide
- Corporate level software license
- Two year warranty
- 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.

Further information can be found at: www.redversconsulting.com/data_encryption.php

* Free for the first two years followed by an annual fee of 1,200 US dollars.

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, WRQ** 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:

Affiliated Computer Services (USA)
Bank One / JP Morgan (USA)
Barclays Life Assurance (UK)
Canada Life Assurance (UK)
Citibank NA (USA & UK)
CUNA Mutual Life Insurance (USA)
Deutsche Bank (USA)
Deutsche Rentenversicherung Bund (DE)
Dun & Bradstreet (UK)
FirstBank (USA)
Fegro Selgros (DE)
GMAC Insurance (USA)
John Deere (USA)
Lehman Brothers (USA & UK)
Oppenheimer (USA)
Railtrack / Network Rail (UK)
Sasktel (Canada)
Standard Life Assurance (UK)
Suncorp (AUS)
WorldCom / MCI (USA)
Zurich Insurance (UK & SUI)

Contact Information

www.redversconsulting.com/contact.php

Development Office:

Redvers Consulting Ltd
Channelsea House,
Canning Road,
London E15 3ND, UK

Tel: +44 (0)208 503 1211

Fax: +44 (0)700 603 8655

Head Office:

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

Tel: +44 (0)870 922 0633

Fax: +44 (0)700 603 8655

German Office:

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

Tel: +49 (0)221 1704 9000

Fax: +49 (0)221 271 1016