

ISO/IEC 9979 ALGORITHM REGISTER ENTRY

a.) ISO entry name	{ iso standard 9979 rc2-sbc (8) }
b.) Name of algorithm	RC2 Symmetric Block Cipher™
c.) Intended range of applications	<ol style="list-style-type: none"> 1. Confidentiality 2. Authentication - as detailed in ISO 9798. RC2 may be used as a nonreversible function to support authentication exchange. 3. Data Integrity - as detailed in ISO 9797 4. Hash Function - as detailed in ISO 10118 part 2
d.) Cryptographic Interface Parameters	<p>Input size: 64 bits Output size: 64 bits Key length: 8 to 1024 bits, multiples of 8 An "effective key size" of 1 to 1024 bits is specified independent of the key length</p> <p>Other parameters (e.g., Initialization Vector) as required by mode</p>
e.) Test Words	<p>(For Electronic Code Book Mode)</p> <p>Key: fedc ba98 7654 3210 Effective key size: 64 bits Input data: 0123 4567 89ab cdef Output data: aff6 1f28 adb8 f992</p>
f.) Sponsoring Authority	ANSI
Registration Requested by	RSA Data Security, Inc.
Contact for Information	<p>Burt Kaliski RSA Laboratories 100 Marine Parkway, Suite 500 Redwood City, CA 94065 USA Telephone +1 415 595 7703 Facsimile +1 415 595 4126 E-Mail burt@rsa.com</p>
g.) Date of submission	January 4, 1994
Date of registration	October 31, 1994
h.) Whether the Subject of a National Standard	No.
i.) Patent - License Restrictions	Not patented. Proprietary to RSA Data Security, Inc.
j.) References	None.

k.) Description of Algorithm	The algorithm is a block cipher with 18 rounds of "mixing" and "mashing" operations involving an internal table. The table is set up from a variable size key. An "effective key size" parameter limits the number of possible internal tables, independent of the key length. Exact details will not be generally published.
l.) Modes of Operation	Preferred mode of use: Cipher Block Chaining Secondary modes of use: 1. Electronic Code Book 2. Cipher Feedback 3. Output Feedback
m.) Other Information	Software implementations operate in excess of 200 Kbytes per second.
n.) Date of latest update of record	(to be determined)