ISO 9979/0007

ISO/IEC 9979 ALGORITHM REGISTER ENTRY

a.) ISO entry name	{iso standard 9979 rc4-ssc (7)}
b.) Name of algorithm	RC4 Symmetric Stream Cipher™
c.) Intended range of applications	Confidentiality
d.) Cryptographic Interface Parameters	Input size: 8 bits Output size: 8 bits Key length: 8 to 2048 bits, multiples of 8
e.) Test Words	Key: fedc ba98 7654 3210 Input data: 0123 4567 89ab cdef Output data: dae1 0fb4 e886 c667
f.) Sponsoring Authority	ANSI
Registration Requested by	RSA Data Security, Inc.
Contact for Information	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
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 generates a pseudorandom byte stream from an internal table and adds the stream to the input data with a bitwise exclusive-or operation. The table is set up from a variable size key. Exact details will not be generally published.
l.) Modes of Operation	Additive Stream Cipher
m.) Other Information	RC4 takes 8–16 machine instructions per byte. Software implementations operate in excess of 900 Kbytes per second.
n.) Date of latest update of record	(to be determined)