RC4 Encryption Algorithm

http://www.vocal.com

ADI - AMD
ARM - DSP Group
LSI Logic ZSP
MIPS - TI

VOCAL Technologies, Ltd. software libraries include a complete range of ETSI / ITU / IEEE compliant algorithms, optimized for execution on ANSI C and leading DSP architectures (ADI, AMD-Alchemy, ARM, DSP Group, LSI Logic ZSP, MIPS and TI).

The RC4 encryption algorithm was developed by Ronald Rivest of RSA. This is a shared key stream cipher algorithm which requires a secure exchange of a shared key which is outside the specification of the RC4 algorithm. The RC4 algorithm is used identically for encryption and decryption as the data stream is simply XORed with the generated key sequence. The algorithm is serial as it requires successive exchanges of state entries based on the key sequence. Hence implementations can be very computationally intensive. This algorithm has been released to the public and is implemented by many programmers. This encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol) using a 40 and 128-bit keys. Published procedures exist for cracking the security measures as implemented in WEP.

The VOCAL implementation of the RC4 encryption algorithms for the MIPS is available in several forms. The forms include pure optimized software and varying levels of hardware complexity utilizing UDI instructions. The RC4 operations are supported using UDI instructions for improved performance. When special assistance hardware is not available (as is the case on most general purpose processors), the RC4 byte manipulation/exchange operations are implemented via software.

In the algorithm the keystream is completely independent of the plaintext used. An 8 * 8 S-Box (S_0 S_{255}), where each of the entries is a permutation of the numbers 0 to 255, and the permutation is a function of the variable length key. There are two counters i, and j, both initialized to 0 used in the algorithm.

RC4 Features:

- RC4 uses a variable length key from 1 to 256 bytes to initialize a 256-byte state table. The state table is used for subsequent generation of pseudo-random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to give the ciphertext. Each element in the state table is swapped at least once.
- The RC4 key is often limited to 40 bits, because of export restrictions but it is sometimes used as a 128 bit key. It has the capability of using keys between 1 and 2048 bits. RC4 is used in many commercial software packages such as Lotus Notes and Oracle Secure SQL.
- The RC4 algorithm works in two phases, key setup and ciphering. Key setup is the first and most difficult phase of this algorithm. During a N-bit key setup (N being your key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations. These mixing operations consist of swapping bytes, modulo operations, and other formulas. A modulo operation is the process of yielding a remainder from division. For example, 11/4 is 2 remainder 3; therefore eleven mod four would be equal to three.
- Once the encrypting variable is produced from the key setup, it enters the ciphering phase, where it is XORed with the plain text message to create an encrypted message. XOR is the logical operation of comparing two binary bits. If the bits are different, the result is 1. If the bits are the same, the result is 0. Once the receiver gets the encrypted message, he decrypts it by XORing the encrypted message with the same encrypting variable.

Custom Product Design Division
200 John James Audubon Parkway
Buffalo, New York 14228
716-688-4675
http://www.vocal.com/

RC4 Strengths:

- The difficulty of knowing where any value is in the table.
- The difficulty of knowing which location in the table is used to select each value in the sequence.
- A particular RC4 key can be used only once.
- Encryption is about 10 times faster than DES.

RC4 Weakness:

- The RC4 algorithm is vulnerable to analytic attacks of the state table.
- One in every 256 keys can be a weak key. These keys are identified by cryptanalysis that is able to find circumstances under which one of more generated bytes are strongly correlated with a few bytes of the key.
- WEAK KEYS: these are keys identified by cryptanalysis that is able to find circumstances under which one or more generated bytes are strongly correlated with small subset of the key bytes. These keys can happen in one out of 256 keys generated.

RC4 Terminology:

- RC4 = Ron's code # 4 or Rivest
- Cipher = a cryptographic algorithm used for encryption and decryption.
- Symmetric key algorithm = an algorithm that uses the same key to encrypt and decrypt
- Stream cipher = algorithm that encrypts data one byte at a time
- Anonymous remailer = distribution system that strips off all of the sender information and remails the message under an anonymous name.
- Cyperpunk = computer users that believe that privacy from government and large business institutions must be protected. These users generally have expertise in cryptography.
- State table: is a table initialized from 1 to 256 bytes. The bytes in the table are used for subsequent generation of Pseudo-Random bytes. The Pseudo-Random stream generated is XORed with the plaintext to give the ciphertext.

RC4 Performance:

- The following table summarizes the number of MIPS required for RC4 encryption/decryption for 1 million bits per second for each of the three implementations:

	RAM	MIPS
Optimized MIPS Assembly	2.5	none
RC4 Operation Support UDI Primitives	1.75	0 bytes
RC4 Key Byte Generator UDI Accelerator	0.22	256 bytes

- Each of the UDI implementations is a hardware block specifically designed for the implementation. RAM space is required by the key byte generator to locally maintain the state table for key generation. This state would need to be preserved and restored in case of a context switch if other processes would need the same functionality. This overhead is not considered in the above performance projections. Encryption and decryption state data may be stored in separate state memories to allow for independent processes

RC4 Hardware Implementation:

- VOCAL Technologies, Ltd. also offers a RC4 hardware implementation. For more detail contact David Jamieson at (716) 688-4675 or http://www.vocal.com

Custom Product Design Division
200 John James Audubon Parkway
Buffalo, New York 14228
716-688-4675
http://www.vocal.com/