

Re: 8 Bit Random Numbers

Source: <http://sci.tech-archive.net/Archive/sci.electronics.basics/2009-02/msg00141.html>

- *From:* nospam@xxxxxxxxxxx
 - *Date:* Fri, 06 Feb 2009 21:57:59 +0000
-

Nobody wrote:

If you want highly-random bytes, and can spare 258 bytes of RAM, I would echo nospam's suggestion to use RC4 (aka ArcFour, as RC4 is a trademark):

A description of ARCFOUR (Alleged RC4), written by Neil Bawd in 1997 and updated in 2000:

In 1987 Ron Rivest developed the RC4 cipher-system for RSA Data Security, Inc. It used a well-guarded proprietary trade secret. The system was popular and is used in several hundred commercial cryptography products, including Lotus Notes, Apple Computer's AOCE, and Oracle Secure SQL. It is part of the Cellular Digital Packet Data Specification, and is used by Internet Explorer, Netscape, and Adobe Acrobat.

Seven years later, source code alleged to be equivalent to RC4 was published anonymously on the Cypherpunks mailing list. Users with legal copies of RC4 confirmed compatibility.

The code is extremely simple and can be written by most programmers from the description.

We have an array of 256 bytes, all different.

Every time the array is used it changes – by swapping two bytes.

The swaps are controlled by counters *i* and *j*, each initially 0.

To get a new *i*, add 1.

To get a new *j*, add the array byte at the new *i*.

Re: 8 Bit Random Numbers

Exchange the array bytes at i and j.

The code is the array byte at the sum of the array bytes at i and j.

This is XORed with a byte of the plaintext to encrypt, or the ciphertext to decrypt.

The array is initialized by first setting it to 0 through 255.

Then step through it using i and j, getting the new j by adding to it the array byte at i and a key byte, and swapping the array bytes at i and j. Finally, i and j are set to 0.

All additions are modulo 256.

The cipher key to be used when initializing can be up to 256 bytes, i.e., 2048 bits. It works best when it's shorter so the randomizing done at initialization can thoroughly shuffle the array. At most 64 bytes are recommended for the key.

The name "RC4" is trademarked by RSA Data Security, Inc. So anyone who writes his own code has to call it something else. In 1997 I called it ARCIPHER. ARCFOUR has been since widely accepted as the name of the alleged RC4.

It is popular because it is small, fast, and believed to be secure.

It's a rare ex