

Re: Another Dumb Idea for Debunking...

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-10/msg00936.html>

- *From:* Ben Rudiak-Gould <br276deleteme@xxxxxxxxxx>
 - *Date:* Mon, 30 Oct 2006 15:54:41 +0000
-

Bill Cox wrote:

I've gone ahead and written a new encryption program. I can't help it
– it was FUN. It's at tinycrypt.sourceforge.net.

I have no objection to this except for the last sentence. You seem to understand that there's little chance that your code is secure; under the circumstances it seems irresponsible to release it on sourceforge.

Looking at your algorithm, the most obvious problem I can see is that `randVal` will always be even at the end of each loop, meaning that the least significant bits of the output are only slightly obscured. I'm sure that someone else here could come up with a complete break if they took the time, but you might find it a good exercise to try this yourself.

The famous cipher RC4 is about as simple as your algorithm and probably about equally fast. It has known flaws, but they can be worked around if you're careful. AES is pretty darn fast too.

— Ben

.