

Re: Another Dumb Idea for Debunking...

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-10/msg00978.html>

- *From:* "TC" <aatcbtccctc@xxxxxxxxxx>
 - *Date:* 31 Oct 2006 03:47:09 -0800
-

Bill Cox wrote:
(snip)

PS. One more thing. Be aware that RC4 is deprecated. The experts here (of which I am –not– one) would say to use a modern cipher like AES. AES is a block cipher, but there are modes of operation that make a block cipher work like a stream cipher (if that's what you really want).

In other words, probably not many people will jump in to help, if you plan to use RC4 in a new project.

Gotta go,
TC (MVP MSAccess)
<http://tc2.atspace.com>