

sci.crypt: Re: Idea for algo.

Re: Idea for algo.

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-12/1890.html>

From: Tom St Denis (tomstdenis_at_iahu.ca)

Date: 12/31/03

Date: Wed, 31 Dec 2003 02:57:05 GMT

"Peter" <peter_rabbit@shaw.ca> wrote in message
news:MQqIb.872695\$pl3.250677@pd7tw3no...
> *Any serious thoughts? Has something like this been done before?*

No and here's why. You have to shuffle after every byte you process. And how do you shuffle? You need some random bits [or pseudo]. So you might as well make better use of your PRNG.

I'd say study some cryptanalysis... don't make your own designs...

Tom