

Re: Unique number generation

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2083.html>

paul_at_atom.sbrk.co.uk

Date: 04/29/05

Date: Fri, 29 Apr 2005 14:41:18 GMT

In article <d4tf8j\$8si\$1@nntp.itservices.ubc.ca>, Unruh wrote:

> *paul@atom.sbrk.co.uk* writes:

>

>> *I'd like to be able to generate some secure unique numbers. A simple
>> implementation might be $val = \text{encrypt}(\text{secret}, \text{seq_no})$, however that
>> doesn't ensure that the numbers will be unique. Ok, I could remove*

> *Yes, it does. If secret is the same for all numbers then val is unique if
> seq_no is. Encryption is a one-one and onto map.*

Very true. I started with the pain of managing millions of existing outputs that I needed to sort and weed duplicates from and was thinking of a more manageable solution. Then I completely missed how simple it was...

Cheers,

Paul