

Re: VBA Random numbers

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-12/1853.html>

From: David Eather (*eather_at_tpg.com.au*)

Date: 12/29/04

Date: Thu, 30 Dec 2004 05:50:03 +1000

Mack wrote:

> *On Wed, 29 Dec 2004 22:07:45 +1000, "David Eather" <eather@tpg.com.au>*

> *wrote:*

>

>> *Guy Macon wrote:*

>>> *During a work-related conversation today the subject of someone*

>>> *using the random function in Windows XP / Microsoft Office Visual*

>>> *Basic for Applications for weak crypto came up. The threat model*

>>> *is a coworker with no special skills other than what can be found*

>>> *on a Google search being able to predict the next number. How*

>>> *good/bad is the VBA PRNG?*

>>>

>>> *(Yes, I know about the dangers of not having the source and of the*

>>> *dangers of someone compromising the OS. Right now I am just curious*

>>> *as to whether anyone has analysed the VBA PRNG.)*

>>

>> *I have some old notes on Microsoft's RNG – it had no serious faults*

>> *so it is probably unchanged. It is a maximum period LCG working*

>> *with a maximum of 31 bits resolution. The output is divided to*

>> *scale the output to a range of 0 to 1 and returned as a single*

>> *precision floating point number. It won't test well with diehard*

>> *but that is because of having only 31 bits rather than some fault*

>> *like RANDU.*

>

> *The reason that generate does poorly isn't so much the 31 bits but the*

> *very bad output. For example every odd number will be followed by*

> *an even number and vice versa. This is NOT good random behavior.*

> *You can't get two even or two odd numbers in a row.*

That is a property of all LCG's (except the bad ones like RANDU) – but they still have properties making them useful for simulations and will probably be suitable for this required task.

>

>>

>> *seed = (214013 x seed + 2531001) mod 2**31*

>>

> *The newer generator described at*

sci.crypt: Re: VBA Random numbers

> <http://support.microsoft.com/kb/q231847/>
>
> *is*
> $seed = (1140671485 * seed + 12820163) \bmod 2^{24}$
>
> *This is an even worse generator.*
>
>> *There is also a trick to making it restart a sequence – from the VB*
>> *help:*
>>
>> *Note To repeat sequences of random numbers, call Rnd with a*
>> *negative argument immediately before using Randomize with a numeric*
>> *argument. Using Randomize with the same value for number does not*
>> *repeat the previous sequence.*
>>
>> *David Eather*
>>
>>
>
> *Leslie 'Mack' McBride*
> *remove text between _ marks to respond via e-mail*