Subject: Re: IDL random number generator
Posted by James Kuyper on Fri, 09 May 2003 14:13:26 GMT

krijger@astro.uu.nl wrote:
>
> Hi,
> I know that randomn is pseudo-random, how many numbers can you
> generate before the non-randomness kicks in?
>
> Thijs Krijger

None. The non-randomness is there from the very beginning. You could
make a true random number generator by running it off of the radioactive
decay of atoms, or some similar hardware-based approach. However,
software random number generators are absolutely deterministic, once
you've set up the seed. You can set the seed form a clock setting, which
means that the precise sequence of random numbers generated depends upon
the precise time at which the program reads the clock. But even the very
first number can be absolutely predicted from the seed value.

Every random number generator has a period, after which it starts
repeating the same exact sequence. How long that period is depends upon
the quality of the algorithm used. Commonly used algorithms have periods
in the range of 100,000 numbers or better. Very sophisticated generators
can have periods that are so long that your computer will become
obsolete before the sequence repeats.