NAME

snobol4random − SNOBOL4 random number functions

SYNOPSIS

-INCLUDE 'random.sno'

NUMBER = RANDOM()

SRANDOM(NUMBER)

SRANDOMDEV()

DESCRIPTION

The **RANDOM()** function uses a non-linear additive feedback random number generator employing a default table of size 31 long integers to return successive pseudo-random numbers in the range from 0 to (2**31)-1. The period of this random number generator is very large, approximately 16*((2**31)-1).

The **SRANDOM()** function sets its **INTEGER** argument seed as the seed for a new sequence of pseudo-random numbers to be returned by **RANDOM()**. These sequences are repeatable by calling **SRANDOM()** with the same seed value. **RANDOM()** will by default produce a sequence of numbers that can be duplicated by calling **SRANDOM()** with 1 as the seed.

The **SRANDOMDEV()** routine initializes a state array using the **random**(4) random number device (if available) which returns good random numbers, suitable for cryptographic use. Note that this particular seeding procedure can generate states which are impossible to reproduce by calling **SRANDOM()** with any value, since the succeeding terms in the state buffer are no longer derived from the LC algorithm applied to a fixed seed. Data from the **random**(4) device may be precious, and repeated calls to **SRANDOMDEV()** should be avoided. When the **random**(4) device is not available, a 32-bit seed will be generated using time, process id, and an element of the process stack.

SEE ALSO

snobol4(1), **random**(3), **random**(4)

AUTHOR

Philip L. Budne