Document Number: WG14 N415/X3J11 95-016

C9X Revision Proposal

Title: Improved random number guidleines
Author: Derek Jones
Author Affiliation: Knowledge Software Ltd
Postal Address: 62 Fernhill road, Farnborough, Hants GU14 9RZ
England
E-mail Address: derek@knosof.co.uk
Telephone Number: +44 1252 520667
Fax Number: +44 1252 377226
Sponsor:
Date: 18 Feb 95
Proposal Category:
X_ Editorial change/non-normative contribution
__ Correction
__ New feature
__ Addition to obsolescent feature list
__ Addition to Future Directions
__ Other (please specify)
Area of Standard Affected:
__ Environment
__ Language
__ Preprocessor
X_ Library
__ Macro/typedef/tag name
__ Function
__ Header
__ Other (please specify)
Prior Art:
Target Audience: Developers who rely on calls to rand delivering a sequences of numbers that are random

Related Documents (if any): Algorithm 183, Applied Statictics 1982, Vol 31, No 2

Proposal Attached: X_ Yes __ No, but what's your interest?
Abstract: Making the world a better place to write software in.

Proposal: Clause 7.10.2.2 contains example code for the rand function. The random quality of the number sequences generated by this code is poor. Replacing the example by an alternative algorithm may lead to higher quality of implementations.

The proposed algorithm is:

```
x = (171 * x) % 30269
y = (172 * y) % 30307
z = (170 * z) % 30323
rand_num = fmod(x/30269.0 + y/30307.0 + z/30323.0, 1.0)
```

The cycle length of this generator exceeds 2.78 * 10^13. At 1,000 calls per second the sequence would repeat after 880 years.

As well as a long sequence length this generator delivers numbers uniformly distributed between 0 and 1.

Actual implementation has to rewrite the first three assignment expressions to prevent overflow on the multiplication.