

Which Bits to Use From a Linear Congruential Pseudo–Random Number Generator?

Source: <http://sci.tech–archive.net/Archive/sci.math/2008–09/msg02983.html>

- *From:* "David T. Ashley" <dta@xxxxxxxx>
 - *Date:* Wed, 24 Sep 2008 19:05:38 –0400
-

Hi,

I'm developing a small embedded system and plan to implement an LCG as described here:

http://en.wikipedia.org/wiki/Linear_congruential_generator

The function I have in mind is

$$X(n+1) = (1664525 * X(n) + 1013904223) \bmod 2^{32}$$

which naturally lends itself to a 32–bit seed.

The random number function will only return 16 bits of the 32–bit seed ... the question is which 16 bits to choose?

The web page hints that the least significant bits will have a shorter period than 2^{32} ... should I choose bits above those ... but how should I decide which ones?

Thanks.

.