

# Re: linear congruential pseudorandom number generator question

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2122.html>

---

*From:* David Wagner ([daw\\_at\\_taverner.cs.berkeley.edu](mailto:daw_at_taverner.cs.berkeley.edu))

*Date:* 04/30/05

Date: Sat, 30 Apr 2005 05:53:27 +0000 (UTC)

Korejwa wrote:

>If I have a sequence of numbers that I know were generated by a linear  
>congruential pseudorandom number generator, how can I calculate the  
>internal state of the generator?

>The pseudorandom number generator performs this function:

>

> $Y = (A * X + C) \text{ MOD } N$

>return a value which reduces  $X$  to the range of a specified Min–Max value.

>

> $A$ ,  $C$ , and  $N$  are known constants.  $X$  is modified each time the function is  
>called.

Given  $Y$ , it is trivial to learn  $X$ , since  $X = A^{-1} * (Y - C) \text{ mod } N$ ,  
and inverses can be computed using the extended Euclidean algorithm.