

linear congruential pseudorandom number generator question

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2119.html>

From: Korejwa (korejwa_at_tiac.net)

Date: 04/30/05

Date: Sat, 30 Apr 2005 05:49:15 GMT

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:

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

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.

Using algebra, I can calculate a range of possible values that X could be for any given output. Each consecutive output reduces the set of possible X values exponentially, until only one possibility remains. But how do you calculate the reduced set of possible X values for each known consecutive output?

I hope my poor description of this problem is clear enough. I'm sure it has a solution and many people have examined it before.