

Re: linear congruential pseudorandom number generator question

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2124.html>

From: Korejwa (korejwa_at_tiac.net)

Date: 04/30/05

Date: Sat, 30 Apr 2005 07:31:44 GMT

On Sat, 30 Apr 2005 05:53:27 +0000 (UTC), David Wagner
<daw@taverner.cs.berkeley.edu> wrote:

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

>

> 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.

Yes, I can compute $A^{-1} \text{ MOD } N$. You've changed my X to a Y and algebraically solved one equation. The real problem is solving two equations simultaneously, where each equation has a variable which is not known exactly, but known to be within a range of values.

Given:

$$X1 = (A * X0 + C) \text{ MOD } N$$

$$X2 = (A * X1 + C) \text{ MOD } N$$

$X1$ is known to be an integer in the set $X1(0)$ to $X1(0)+V$

$X2$ is known to be an integer in the set $X2(0)$ to $X2(0)+W$

$A, C, N, X1(0), X2(0), V, W$ are known.

Using A^{-1} , you can algebraically solve the first equation for $X0$. But since $X1$ is not known exactly, and only known to be within a known set of values, $X0$ can only be calculated as being within a known set of values.

But by combining the first equation with the second equation, we can narrow down the possible $X0$ values further.

I haven't solved this problem, so I don't know whether it makes more sense to solve for the $X0$ set, or the set of another instance of X . If you can find a way to combine these two equations to describe the possible values for $X0, X1$, or $X2$, the process can be repeated to narrow down the possible X values until only one remains. Once one instance of X is known exactly, whether it be $X0$ or a later instance, calculating exact value of the

sci.crypt: Re: linear congruential pseudorandom number generator question

others is easy.