Pseudo Random Number Generator Computer Security IV1013

Axel Månson Lokrantz

2023-04-07

A pseudo random number generator, or PRNG, is a computer algorithm used to generate random numbers. Unlike truly random numbers, which are generated by physical processes like radioactive decay or atmospheric noise, PRNG use an algorithm that generates a number sequence that appears to be random.

There are several types of PRNGs, each with its own algorithm to generate a sequence of numbers. Some of the commonly used PRNG algorithms are lagged Fibonacci generators, linear feedback shift registers, Blum Blum Shub, Fortuna, and linear congruential generators.

Linear congruential generators, or LGCs, are simple types of PRNG and used widely. An LCG generates a sequence of numbers using a mathematical formula based on a linear congruence, which is an equation of the form:

$$X_{n+1} = (a * X_n + b) mod_m$$

Where X_n is the current random number, X_{n+1} is the next random number, a and b are constants, and m is the modulo. The value of m, often chosen as a prime, determines the length of the sequence.

One of the simplest LGCs is the Lehmer random number generator, which operates in the multiplicative group of integers modulo m. To use Lehmers generator, m is chosen as a large prime number, and a as a primitive root of m. X_0, or the seed, is chosen to be co prime with m. Since m is a prime, the maximum period becomes $\phi(m) = m - 1$. b is often chosen as 0 to avoid $X_i = 0$.

Suppose we choose a prime number $m = 2^3 1 - 1$ and $a = 16807$, which is the primitive root of m. The maximum period is then $\phi(m) = m - 1 = 2147483646$, meaning the sequence is 2147483646 $n_u$mbers long before it starts to repeat itself. To generate a sequence of random numbers, we choose an initial seed X_0 and repeat the LGC formula as many times as we want the sequence to be long.