Simple Linear Congruential Generator

A Linear Congruential Generator (LCG) is a method to generate pseudo-random numbers using the recursion:

$$X_{i+1} = (aX_i + c) \times \mod m$$

where X_i is the i^{th} number of the sequence, a is a multiplier, c is the increment and m is the modulus of the generator. Also, we have tha $0 \leq X_i \leq m$.

The pseudo-random numbers U_i are computed as:

$$U_i = X_i / m$$

The generated sequence if a and m are properly chosen will appear uniformly distributed in the interval $[0, 1]$

Advantages:
- easy to implement
- fast, $O(1)$ time complexity

See: Lehmer, 1951
Lawrance, 1992
Knuth, 1998