Linear congruential generators

LCG fixed parameters a, b, m
from seed x_0 generate

$$x_{n+1} \equiv a x_n + b \pmod{m}$$

$$PRG(x_0) = x_1 x_2 x_3 \ldots$$

real world glibc uses $a = 1103515245$, $b = 12345$, $m = 2^{31}$

comments

- LCGs are easy to predict ($\Rightarrow$ unsuitable for crypto)
- pros: easy to implement, decent statistical properties

EG stream cipher using LCG $x_{n+1} \equiv 5x_n + 3 \pmod{8}$, $8 = 2^3$

$k = (100)_2$ (4) $\quad m = (101\ 111\ 001)_2$

$x_0 = 4$
$x_1 = 5x_0 + 3 \equiv 7 \pmod 8$
$x_2 = 5x_1 + 3 \equiv 6$
$x_3 = 5x_2 + 3 \equiv 1$

$PRG(x_0) = x_1 x_2 x_3 \ldots$
$= 7, 6, 1, \ldots$
$= 111, 110, 001, \ldots$

$c = m \oplus PRG$

m	101	111 001
$\oplus$ PRG	111	110 001
$= c$	010	001 000

EG $c = (111\ 111\ 111)_2$

Eve knows: stream cipher with $x_{n+1} \equiv 5x_n + 3 \pmod{8}$, $8 = 2^3$
$m = (110\ 1\ldots)_2$

$c = m \oplus PRG$
$PRG = c \oplus m$
$= 001\ 000\ 011$ (1111.. 1101..)
$x_1 = 1 \pmod 8$

$x_2 = 5x_1 + 3 \equiv 0 \pmod 8$
$x_3 = 5x_2 + 3 \equiv 3$

c	111	111 111
$\oplus$ PRG	001	000 011
$= m$	110	111 100