CSS322 – Pseudo Random Numbers and Stream Ciphers Notes

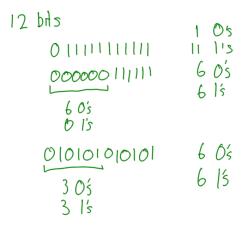


Figure 1: Different checks for randomness; Lecture 08

$$\frac{LCG}{K_{n+1}} = (a X_n + c) \mod m$$

Ex1. $a = 1, c = 1, m = 100$
Seed, $X_0 = 23$
 $X_1 = (1 \times 23 + 1) \mod 100 = 24$
 $X_2 = 25$
 $X_3 = 26$
 $X_4 = 27$
 $X = \{23, 24, 25, 26, 27, ..., 99, 0, 1, ..., 22\}$
Period = 100
Ex2. $a = 7, c = 0, m = 32$
 $X_0 = 1$
 $X_1 = (7 \times 1 + 0) \mod 32 = 7$
 $X_2 = (7 \times 7 + 0) \mod 32 = 17$
 $X_3 = (7 \times 17 + 0) \mod 32 = 23$
 $X_4 = (7 \times 23 + 0) \mod 32 = 1$
 $X = \{1, 7, 17, 23\}$
Period = 4
Ex3 $a = 5, c = 0, m = 32$
 $X = \{1, 5, 25, 29, 17, 21, 9, 13\}$
Period = 8
Ex4 $a = 5, c = 0, m = 32$
 $X = \{3, 15, 11, 23, ..., \}$

Figure 2: Linear Congruential Generator Examples; Lecture 09