Random Number Generators

CIS-4040 Homework #5

Peter C. Chapin, Vermont Technical College

Due: Monday, July 10, 2017

This homework covers random number generators. Read Chapter 8 in the text.

1. Consider the Blum Blum Shub random number generator described in Section 8.2 (on page 242) of the text. Following the example shown there, compute the first ten random bits produced using a seed value of 127,815 (instead of the seed value used in the example). Note that the security of a BBS generator depends on the difficulty of factoring n (which in this example is only 192649). In real life, much larger primes would be needed, and the computations would be quite time consuming. Thus this generator produces random bits relatively slowly.

2. Search online for a hardware random number generator (there are several commerical products available). Give the URL for the device's web site, the name of the device, the physical principle it uses to generate random numbers, and at least one other interesting specification (bit rate, price, power consumption would all be reasonable possibilities).