Introduction to Cryptology ENEE459E/CMSC498R: Homework 2

Due by beginning of class on 3/4/2014.

1. Write a program that increments a counter $2^{24}, 2^{25}, 2^{26}, \ldots, 2^{33}$ times, and measure how many seconds your program takes to run in each case. Estimate how many years your program would take to increment a counter 2^{64} or 2^{128} times.

2. Exercise 3.2

3. Exercise 3.5

4. Exercise 3.6

5. Let G be a pseudorandom generator where $|G(s)| \geq 2 \cdot |s|$.
   (a) Define $G'(s) = G(G(s))$. Is G' necessarily a pseudorandom generator?

   (b) Define $G'(s) = G(s||\overline{s}$, where $\overline{s}$ is the bit-wise negation of s. Is G' necessarily a pseudorandom generator?

   (c) Define $G'(s) = s_1, \ldots, s_{n/2}||G(s_{n/2+1}, \ldots, s_n)$. Is G' necessarily a pseudorandom generator?

   (d) Define $G'(s) = G(s)||G(\overline{s})$, where $\overline{s}$ is the bit-wise negation of s. Is G' necessarily a pseudorandom generator?