# Introduction to Cryptology ENEE459E/CMSC498R: Homework 3

Due by beginning of class on 2/21/2017.

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. Based on your findings, what do you think would be a reasonably setting for the security parameter $k$ of a cryptosystem which is assumed to be secure against attackers running in time $2^{\sqrt{k}}$?

2. The best algorithm known today for finding the prime factors of an $n$-bit number runs in time $2^{c \cdot n^{\frac{1}{3}} (\log n)^{\frac{2}{3}}}$. Assuming 4Ghz computers and $c = 1$ (and that the units of the given expression are clock cycles), estimate the size of numbers that cannot be factored for the next 100 years.

3. Prove the equivalence of Definition 3.8 and Definition 3.9.

4. Let $G$ be a pseudorandom generator that on security paramter $n > 1$, takes as input bitstrings of length $n$ and has expansion factor $\ell(n) > 2n$. In each of the following cases, say whether $G'$ is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.
   (a) Define $G'(s) = G(s_1, \ldots, s_{\lceil n/2 \rceil})$, where $s = s_1, \ldots, s_n$.
   (b) Define $G'(s) = G(0^{|s|} || s)$.
   (c) Define $G'(s) = G(\mathsf{rotate}(s, 1))$, where $\mathsf{rotate}(s, 1)$ rotates the bits of $s$ to the right by one position.

5. There are two files on the course webpage rand_1.txt and rand_2.txt. One of these files contains the output (in hexadecimal) of a pseudorandom generator and the other file is not random or pseudorandom. Can you distinguish which file is which? Use the statistical tests provided by NIST here `http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html`