15-503/859: An Introduction to Theoretical Cryptography — Spring 2016
Problem Set #3 — M. Blum & V. Guruswami
Due before class on Tuesday February 9, 2016.

1. (a) Show that the existence of pseudorandom generator (PRG's) implies the existence of one-way functions (OWF's).[1] More specifically, assume G is a PRG such that G maps $\{0,1\}^n$ to $\{0,1\}^{2n}$ for every n. Argue (with a proof) that G *by itself* is a OWF.
   Can you also prove this if we take a generator that maps n bits to the "minimal" $n+1$ bits?
   (b) *(Required for graduate section of course only; those signed up for 15-503 may attempt for fun)* Prove that the existence of a secure private-key encryption scheme that encrypts messages *twice as long as its key* implies the existence of one-way functions. (Warning: Part (a) by itself doesn't imply that OWF's are required for constructing secure private-key encryption schemes, as it may be possible to construct the latter without relying on a PRG.)
   (HINT: Consider defining $f(m,k,r) = m \circ \mathsf{Enc}_k(m;r)$ where r is the randomness used by the encoder.)

2. Assume G_1 and G_2 are two length-doubling PRG's, and let $\circ$ denote string concatenation and $\overline{a}$ denote the bit-wise negation of a string a.
   (a) Consider $H_1(s) = G_2(\overline{s})$. Show that H_1 is a PRG.
   (b) Consider $H_2(s) = G_1(s) \circ G_2(\overline{s})$. Argue that H is not necessarily a PRG by showing that one can choose G_1 and G_2 which make H_2 very "non-random". The moral of this problem is to see that it is dangerous to apply PRG's to *"computationally correlated"* inputs (e.g., s and $\overline{s}$).
   (c) Show that the conclusion of part (b) holds even if we restrict $G_1 = G_2$ (i.e., for some PRG G, $G(s) \circ G(\overline{s})$ is not a PRG). (HINT: Using any auxiliary PRG G', construct $G = G_1 = G_2$ such that $G(s) = G(\overline{s})$ for any s.)
   (d) Let $G_1(s) = s_1 \circ s_2$ be the output of G_1, where both s_1 and s_2 are of length k. Show that $H_3(s) = G_2(s_1) \circ G_2(s_2)$ is a PRG. The moral is that it is okay to apply PRG's to *"computationally uncorrelated"* inputs such as s_1 and s_2. (HINT: Use the hybrid argument.)

3. A hardcore predicate for a one-way function $f : \{0,1\}^* \to \{0,1\}^*$ is a function $h : \{0,1\}^* \to \{0,1\}$ such that the bit $h(x)$ is easy to compute given x but is hard to compute with better than negligible advantage over random guessing given only $f(x)$; see Defintion 78.3 in Section 3.3.3 of the notes.
   (a) Let $f(x)$ be a polynomial-time computable *permutation*, and let h be a hardcore predicate for f. Show that f must be one-way (i.e., f is a one-way permutation).
   (b) Show that the conclusion above is not necessarily true if f is not a permutation: construct a function f having a hardcore predicate such that f is not a one-way function.

4. (a) Define a notion of indistinguishability for the encryption of multiple *distinct* messages, in which a scheme need *not* hide whether the same message is encrypted twice.
   (b) Give a construction of a *deterministic* encryption scheme that provably satisfies your definition. (You may assume the existence of pseudorandom functions as per Definition 96.2 in Section 3.8 of the Pass-Shelat notes.)

[1] We have already informally seen OWF's as those which are easy to compute but hard to invert with non-negligible success probability; for the precise definition of (strong) OWF's consult Definition 27.3 in Section 2.2 of the Pass-Shelat notes.