Homework 1

(Due Date: Sep 21, 2015)

1. (5 points) Prove that if $\mu_1(\cdot)$ is a non-negligible function and $\mu_2(\cdot)$ is a negligible function, then $\mu(\cdot)$ is also a non-negligible function, where $\mu(n) = \mu_1(n) - \mu_2(n)$ for any $n \in \mathbb{N}$.

2. (10 points) Consider a function $f : \{0,1\}^n \to \{0,1\}$. Let $\mathcal{A}$ be a randomized algorithm that computes f with probability $\frac{3}{4}$. Given $\mathcal{A}$, construct a randomized algorithm $\mathcal{B}$ that computes f with probability at least $1 - \frac{1}{2^n}$.

3. (15 points) Let $f : \{0,1\}^n \to \{0,1\}^m$ be a strong one-way function. Consider the following function $g : \{0,1\}^n \to \{0,1\}^m$:

$$g(x) \quad = \quad \left\{ \begin{array}{ccc} 0^m & : & x = 0^n \\ f(x) & : & \text{otherwise} \end{array} \right\}$$

   Prove that g is a strong one-way function.

4. (5+15 points) Given a weak one-way function f, construct a strong one-way function g. Give the construction of g and security proof.

5. (Extra Credit Problem) Construct f such that f is a strong one-way function but $f(f(\cdot))$ is not one way.

6. (Extra Credit Problem) Define a function f such that, if there exists a one-way function, then f is a one-way function.