Cryptography: Homework 5
(Deadline: Nov 1, 2018)

1. (30 points) Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a polynomial-time computable function, where $l(n) > n$. Consider the following experiment $\mathsf{PRG}_{\mathcal{A},G}(n)$:

   (a) The challenger chooses a bit $b \in \{0,1\}$ uniformly. If $b = 0$, it chooses $r \in \{0,1\}^{l(n)}$ uniformly; if $b = 1$, it chooses $s \in \{0,1\}^n$ uniformly and set $r = G(s)$. The challenger gives r to the adversary $\mathcal{A}$.

   (b) Given $r \in \{0,1\}^{l(n)}$, the adversary $\mathcal{A}$ will guess the value of b and outputs a bit $b' \in \{0,1\}$.

   (c) The output of the experiment, denoted by $\mathsf{PRG}_{\mathcal{A},G}(n)$, is 1 if $b' = b$, and 0 otherwise.

   Show that if G is a PRG, then for any PPT algorithm $\mathcal{A}$, there is a negligible function negl such that $|\Pr[\mathsf{PRG}_{\mathcal{A},G}(n) = 1] - \frac{1}{2}| \le \mathrm{negl}(n)$.

2. (20 points) Prove that if f is a one-way function, then the function g defined by $g(x_1, x_2) = (f(x_1), x_2)$, where $|x_1| = |x_2|$, is also a one-way function.