Homework 2

1. (10 + 10 points) Let $G_{n,\ell}\colon \{0,1\}^n \to \{0,1\}^\ell$ and $H_{n,\ell}\colon \{0,1\}^n \to \{0,1\}^\ell$ be efficient functions.

   (a) Consider the construction $J_{n,\ell}\colon \{0,1\}^{2n} \to \{0,1\}^\ell$ defined by $J_{n,\ell}(s^{(1)}, s^{(2)}) = G_{n,\ell}(s^{(1)}) \oplus H_{n,\ell}(s^{(2)})$. Prove or disprove that $J_{n,\ell}$ is also a PRG, if $G_{n,\ell}$ or $H_{n,\ell}$ are PRGs and $\ell > 2n$.

   (b) Consider the construction $K_{n,\ell}\colon \{0,1\}^n \to \{0,1\}^\ell$ defined by $K_{n,\ell}(s) = G_{n,\ell}(s) \oplus H_{n,\ell}(s)$. Prove or disprove that $K_{n,\ell}$ a PRG, if $G_{n,\ell}$ and $H_{n,\ell}$ are both PRGs.

2. (10 + 10 points) Suppose $f\colon \{0,1\}^n \to \{0,1\}^n$ is a one-way function. Prove or disprove whether the following functions are also one-way functions.

   (a) Let $g\colon \{0,1\}^n \to \{0,1\}^{2n}$ be defined as follows: $g(x) = (f(x), f(x))$.

   (b) Let $h\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$ be defined as follows: $h(x^{(1)}, x^{(2)}) = (f(x^{(1)}), f(x^{(2)}))$.

3. (10 points + Extra Credit) In this problem we will define "slightly" one-way functions. Let $g\colon \{0,1\}^{n'} \to \{0,1\}^{n'}$ be a function that is easy to compute but any arbitrary efficient adversary can invert the function for at most an ε-fraction of the inputs. Such a function g is called ε-easy. Define slightly one-way functions that captures this intuition.

   - (Extra Credit) Given an ε-easy function, for a constant $\varepsilon > 0$, provide a construction for one-way functions.