Homework 2

1. (5 points) Let $G_n \colon \{0,1\}^n \to \{0,1\}^m$ be a PRG, where $m > n$. Consider the new function $G'_n \colon \{0,1\}^n \to \{0,1\}^m$ defined as follows.

$$G'_n(s) = \begin{cases} 0^m, & \text{if } s = 0^n \\ G(s), & \text{otherwise.} \end{cases}$$

   Is G'_n a PRG?

2. (5 points) Consider a construction which reverses the role of the key s and the input x in the GGM construction. Is the new construction a PRF? (Hint: Use G'_n.)

3. (5 points) Let $H_n = \{h_i\}_{i \in I}$ be a CRHF with domain $\{0,1\}^n$ and range $\{0,1\}^m$, where $m < n$. Let $H'_n = \{h'_i\}_{i \in I}$ be a function family with domain $\{0,1\}^*$ and range $\{0,1\}^m$. The function h'_i is defined as follows.

   (a) Suppose x has length N, where $N = n + (a-1)(n-m) + b$, where $0 < b \leqslant (n-m)$

   (b) Concatenate x with $(n-m) - b$ 0s. Let x' be the resulting string.

   (c) Interpret $x' \equiv (x_0, x_1, \ldots, x_a)$ such that $|x_0| = n$ and $|x_1| = \cdots = |x_a| = (n-m)$.

   (d) Output: $\overbrace{h_i(h_i \cdots (h_i}^{(a+1)\text{-times}}(h_i)(x_0) \circ x_1) \cdots) \circ x_a)$

   Here $\circ$ is the concatenation operator, i.e. $a \circ b$ represents the concatenation of the strings a and b. Is H' a CRHF?

4. (7.5 + 7.5 points) Show that DDH $\implies$ CDH $\implies$ DL.

5. (5 points) Show that existence of a PKE protocol implies existence of a 2-round key-agreement protocol.

6. (Extra Credit) Show that DL $\implies$ OWF.