Homework 3

1. (10 + 10 points) Let DDH assumption hold over the multiplicative group $G = \{g^0, g, \ldots, g^{\lvert G \rvert - 1}\}$, where $g$ is a generator for the group.

   (a) Prove that the distributions $(g, g^x, g^y, g^{xy}) \approx_{(c)} (g, g^x, g^y, g^z)$, where $x, y, z \leftarrow \{1, \ldots, \lvert G \rvert - 1\}$.

   (b) Prove that the distributions $(g, g^x, g^y, g^{x/y}) \approx_{(c)} (g, g^x, g^y, g^z)$, where $x, y, z \leftarrow \{1, \ldots, \lvert G \rvert - 1\}$. (Here $x/y$ is computed over $\mathbb{Z}_{\lvert G \rvert}^*$)

2. (10 + 15 points) Let $H = \{h^{(i)} : i \in I\}$ be a CRHF family, where $I$ is the set of indices for the functions and $h^{(i)} : \{0, 1\}^{2n} \rightarrow \{0, 1\}^n$.

   (a) Define $h^{(2,i)} : \{0, 1\}^{4n} \rightarrow \{0, 1\}^n$, for $i \in I$, as follows. For an input $x \in \{0, 1\}^{4n}$, interpret it as a concatenation of 4 blocks of $n$-bit strings $(x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)})$. The output $y = h^{(2,i)}(x)$ is defined by

   \[
   \begin{array}{c}
   y \\
   \hline
   h^{(i)} \\
   \hline
   h^{(i)} \\
   \hline
   h^{(i)} \\
   \hline
   x^{(1)} \\
   x^{(2)} \\
   x^{(3)} \\
   x^{(4)}
   \end{array}
   \]

   Prove that $H^{(2)} = \{h^{(2,i)} : i \in I\}$ is a CRHF family.

   (b) Intuitively, the construction above interprets the input as blocks of length $n$. Then it embeds a balanced binary tree such that the leaves correspond to these input-blocks. At each interior node of the balanced binary tree, the construction applies $h^{(i)}$ to compresses the two incoming inputs. The output of the function is the output of the hash function at the root.

   Extend the above intuition to construct $h^{(t,i)} : \{0, 1\}^{2^t \cdot n} \rightarrow \{0, 1\}^n$. Prove that $H^{(t)} = \{h^{(t,i)} : i \in I\}$ is a CRHF family. For this problem interpret $t$ as an constant integer $\geq 2$.  

1
3. (25 points) Let \( H = \{ h^{(i)} : i \in I \} \) is a universal one-way hash function (UOWHF) family if \( h^{(i)} : \{0, 1\}^{2n} \rightarrow \{0, 1\}^n \), for all \( i \in I \), and the following definition holds.

For an arbitrary efficient adversary \( A \) the following is true:

(a) The adversary \( A \) sends \( x \in \{0, 1\}^{2n} \)

(b) The honest challenger \( H \) picks \( i \in I \) and sends \( h^{(i)} \) to the adversary \( A \)

(c) The adversary \( A \) replies with \( x' \in \{0, 1\}^{2n} \)

(d) The honest challenger outputs \( z = 1 \) if \( h^{(i)}(x) = h^{(i)}(x') \)

We have \( \Pr[z = 1] \leq \text{negl}(n) \) in the above experiment.

Define \( h^{(2,i,j)} : \{0, 1\}^{4n} \rightarrow \{0, 1\}^n \), for \( i, j \in I \), as follows. For an input \( x \in \{0, 1\}^{4n} \), interpret it as a concatenation of 4 blocks of \( n \)-bit strings \( (x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}) \). The output \( y = h^{(2,i,j)}(x) \) is defined by

\[
\begin{align*}
\text{y} & \rightarrow \ h^{(j)} \\
\text{h^{(i)}} & \text{h^{(i)}} \\
\text{x^{(1)}} & \text{x^{(2)}} \quad \text{x^{(3)}} \quad \text{x^{(4)}}
\end{align*}
\]

Prove that \( \mathcal{H}^{(2)} = \{ h^{(2,i,j)} : i, j \in I \} \) is a UOWHF family.