Exercise 1. (100 points.) Let $G = \langle g \rangle$ be a finite cyclic group of prime order $p$ generated by $g$. Let $H: G \to \{0, 1\}^k$ be a hash function. Recall the Hashed El Gamal key-encapsulation mechanism (KEM) $\text{HEG} = (\text{K}_{\text{HEG}}, \text{E}_{\text{HEG}}, \text{D}_{\text{HEG}})$ associated to $G$, defined as follows:

<table>
<thead>
<tr>
<th>Alg $\text{K}_{\text{HEG}}$ :</th>
<th>Alg $\text{E}_{\text{HEG}}(X)$ :</th>
<th>Alg $\text{D}_{\text{HEG}}(x, Y)$ :</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x \leftarrow \mathbb{Z}_p$</td>
<td>$r \leftarrow \mathbb{Z}_p$</td>
<td>$Z' \leftarrow Y^x$</td>
</tr>
<tr>
<td>$X \leftarrow g^x$</td>
<td>$Y \leftarrow g^r$ ; $Z \leftarrow X^r$</td>
<td>$K' \leftarrow H(Z')$</td>
</tr>
<tr>
<td>Return $(X, x)$</td>
<td>$K \leftarrow H(Z)$</td>
<td>Return $K'$</td>
</tr>
</tbody>
</table>

Prove the following theorem about its security.

**Theorem 1.** Suppose $A$ is an adversary against the IND-KEM security of $\text{HEG}$ in the random oracle model, making at most $q_h$ hash queries. Then there is an algorithm $B$ for solving the computational Diffie-Hellman (CDH) problem in $G$ such that

$$\text{Adv}_{\text{HEG}}^{\text{ind-kem}}(A) \leq 2q_h \cdot \text{Adv}_{G}^{\text{cdh}}(B).$$

Furthermore, the running-time of $B$ is that of $A$.

How does the above theorem compare to what we proved about Hashed El Gamal in class? Is it better, worse, incomparable? Discuss the pros and cons to both results.

For **50 extra points**, formalize a stronger security model for KEMs (call it IND-KEM-M for IND-KEM with Multiple challenge encapsulations) that gives the adversary access to many challenge encapsulations and their candidate decapsulations (instead of just one as in the IND-KEM notion formalized in class and used for the above theorem). Then prove:

**Theorem 2.** Suppose $A$ is an adversary against the IND-KEM security of $\text{HEG}$ in the random oracle model, making at most $q_h$ hash queries and $q_e$ encapsulation queries (or receiving at most $q_e$ challenge encapsulations). Then there is an algorithm $B$ for solving the computational Diffie-Hellman (CDH) problem in $G$ such that

$$\text{Adv}_{\text{HEG}}^{\text{ind-kem-m}}(A) \leq 2q_h q_e \cdot \text{Adv}_{G}^{\text{cdh}}(B).$$

Furthermore, the running-time of $B$ is that of $A$.

Explain why this result is not very interesting.

For **100 extra points**, study the chosen-ciphertext attack (CCA) security of $\text{HEG}$: First, explain clearly why its CCA security cannot be proven under CDH (or even DDH), no matter what one
assumes about $H$. Then formulate a reasonable strengthening of CDH and prove the CCA security of HEG under your strengthened assumption in the random oracle model. Does your strengthened assumption appear to hold in the prime order groups discussed in class? (Hint: Consider giving the CDH adversary access to a decision oracle.)

For **150 extra points**, propose a relatively simple modification to the Hashed El Gamal scheme whose CCA security can be proven under the standard CDH assumption in the random oracle model. As usual, you have to give a formal security theorem and proof for your modification.