# CS-690C: Homework 5

**Problem 1.** (30 points.) Suppose a colleague who needs to implement some cryptography asks you, "what is the random oracle model?" How would you answer? Be succinct and precise.

**Problem 1.** (70 points.) Let $G$ be a finite cyclic group of order $p$, generated by $g$. We write all groups multiplicatively. We call $G$ *pairing friendly* if there is another finite cyclic group $G_T$ (called the target group), of order $p$ and generated by $g_T$, such that: there is an efficiently computable bilinear, non-degenerate map $e\colon G \times G \to G_T$. Bilinear means that $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in \mathbb{Z}_p$. Non-degeneracy means $e(g, g) = g_T$.

Explain succinctly and precisely why ElGamal KEM is *tightly secure* in pairing friendly groups where the computational Diffie-Hellman (CDH) problem holds in $G$. This means that we can avoid the factor $q_H$ loss when reducing security of the ElGamal KEM to the CDH problem. Here $q_H$ is an upper-bound on the number of hash queries the KEM adversary can make.