This problem set is due by the start of lecture on Tuesday, Feb. 17. The problem set should be typed up in Latex and compiled into pdf. Please both bring in a physical copy and email to rashid@cs.utexas.edu (for backup purposes). Please clearly indicate your collaborators for each problem.

1. Recall, that a collision resistant hash function is a function $H(x)$ where
   1) The domain is smaller than the range
   2) It is hard for an attacker to find $M \neq M'$ such that $H(M) = H(M')$.

   Consider the hash function $H : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow G$, that takes two elements of $\mathbb{Z}_p$ and hashes it to one group element of order $p$. Assume the hash function is defined by $u^{x_1} \cdot v^{x_2}$, where $u, v$ are chosen by a trusted setup authority. Show that if there exists an attacker that can find a collision then the attacker (algorithm) can be used to break the discrete log problem in the same group.

2. In class we saw that the decisional Diffie-Hellman (DDH) assumption implies that El Gamal encryption is semantically secure under Chosen Plaintext Attack (CPA). Prove that the security of El Gamal encryption is equivalent to the DDH assumption by showing that an attacker on DDH can break El Gamal. What does this say about the security of ElGamal in groups where there exists efficiently computable bilinear maps?

3. We would like to be able to build a secure encryption system even in the circumstance where the decisional Diffie-Hellman assumption is false. One possible tool is to use a potentially weaker assumption called the decisional linear assumption. The decisional linear problem is that given a group $G$ of prime order $p$ and elements $g, u, v, g^a, u^b$ distinguish whether $T = v^a \cdot u^b$ or is random. (A uniformly random bit $\gamma \in \{0, 1\}$ is flipped to determine $T$) The assumption is that no (poly-time) attacker should be able to guess $\gamma$ will more than $1/2 + \text{negligible}$ advantage.

   Create a public key encryption system that is CPA secure under this assumption. First, describe three algorithms: Setup, Encrypt, and Decrypt. Then show that if the decisional linear assumption holds your system is semantically secure under CPA attacks (the game we defined in class). Note: You are not allowed to assume this is a bilinear group.

4. Sometimes different models of security are equivalent. Consider the following security game for an encryption system with a (finite) message space $\mathcal{M}$. The game is the similar to CPA security except the attacker only gets to submit one message $M^*$. The challenge flips a bit $\gamma$ and encrypts $M^*$ if $\gamma = 0$ and a uniformly random message $M_R \in \mathcal{M}$ if $\gamma = 1$. Show that this new game is equivalent to the traditional CPA game by arguing that an encryption system secure under this new game must also secure
under the traditional CPA encryption game. (You only need to show this direction since the other one is trivial.)

5. We would like to show that a selectively secure Identity-Based Encryption (IBE) system is not necessarily fully secure. Assume there exist a IBE system secure under the standard (full) definition of security with algorithms: Setup, KeyGen, Encrypt, Decrypt. Moreover, assume identities in the system are in the space \( \{0, 1\}^\lambda \), where \( \lambda \) is the security parameter.

Create a new IBE system that is selectively secure, but not fully secure. First describe your system with algorithms: Setup', KeyGen', Encrypt', Decrypt'. Your new algorithms can build upon the existing ones (some might even be the same). Then prove that the system is selectively secure. Finally, show an attack in the full security game. \textit{Hint: Your system might look “unnatural” to allow such an attack.}