CS174 Sp2001 **Homework 10** **Due: April 19, 2001**

This homework is due by 5pm on Thursday April 19th. Please hand it to the CS174 homework box on the second floor of Soda Hall.

1. Suppose a sender re-uses a one-time El-Gamal key. That is, they send an encrypted message $(g^s, M_1 h^s)$ and then another $(g^s, M_2 h^s)$ using the same g, h and s. What could someone who sees both messages learn about M_1 and M_2?
2. In the RSA digital signature scheme, is it acceptable for the hash function to be (a) one-way (b) weakly collision-free or (c) strongly collision-free? Dont pick a condition which is stronger than needed. Explain your choice.
3. Give a zero-knowledge proof for the presence of a k-clique in a graph. How could you make this protocol non-interactive?