CS174 Sp2001 **Homework 11** **out: Apr 19, 2001**
J. Canny **due: Apr 26, 2001**

This homework is due by 5pm on Thursday April 26th. Please hand it to the CS174 homework box on the second floor of Soda Hall.

1. Consider the discrete log zero-knowledge proof from class where the conversation consists of the messages $v = g^r$, b, and w, and the challenge b is chosen randomly from $\mathbb{Z}_p$. Show that from two conversations (v, b_1, w_1) and (v, b_2, w_2) an observer can recover the secret key.

2. Complete the derivation started in class for threshold encryption using El-Gamal.