CS 174 Homework Assignment 10 (due Monday, May 13)

1. When using the RSA system, Alice sends message M to Bob, whose public key is $(e = 43, n = 77)$. If the cryptogram intercepted is $C = 5$, what is M?

2. In a digital signature system based on RSA, Alice has public key $(e = 11, n = 899)$. How will she sign the message 876?

3. Suppose that a user of RSA chooses by mistake a large prime for his modulus n. Show that in this case decryption is easy.

4. Give a zero-knowledge proof for the presence of a k-clique in an undirected graph.

5. In class we showed how to use the RSA crypto-system for threshold decryption; i.e., we showed how to use the partial decryptions from $m + 1$ users to recover a message. Show how to use El Gamal's crypto-system for threshold decryption.