Homework 5 **ICS 247 Security Algorithms**

Due: Friday, March 12, 2004, in class

Please answer the following questions, each of which is worth 10 points.

1. Describe a protocol for electronic poker that is resistant to collusions between pairs of players.

2. Is there a way to modify the (Shamir) secret sharing scheme described in class so that we distribute shares to four individuals, x_1, x_2, x_3, and x_4, such that the secret is revealed only if the subgroup contains x_1 and x_2? Why or why not?

3. Is there a way to modify the (Shamir) secret sharing scheme described in class so that we distribute shares to four individuals, x_1, x_2, x_3, and x_4, such that the secret is revealed only if the subgroup contains the subset $\{x_1, x_2\}$ or $\{x_3, x_4\}$? Why or why not?

4. Peggy claims to have a fast algorithm for graph isomorphism, and for two given graphs G_1 and G_2, Peggy says these two are definitely not isomorphic. Describe a zero-knowledge proof for Peggy to show Victor that she is right, with very high probability.

5. Formulate an encryption scheme and operator $*$ so that

$$E(M_1) * E(M_2) = E(M_1 + M_2),$$

   where $+$ denotes modular addition.