Homework 2 **ICS 247 Security Algorithms**

Due: Friday, January 30, 2004, in class

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

1. Let π be a permutation of the integers $0, 1, 2, \ldots, 2^n - 1$ such that $\pi(m)$ gives the permuted value of m, $0 \leq m < 2^n$. That is, π maps the set of n-bit integers into itself in a one-to-one fashion (that is, it is a *bijection*). The encryption scheme DES is one such permutation for 64-bit integers. We say that such a permutation π has a *fixed point* if there is an m such that $\pi(m) = m$. In other words, for any π that is a permutation encryption scheme, if π has a fixed point, then there is an input m such that the encryption of m is m itself (which is clearly not desirable). Show the somewhat surprising fact that if π is chosen at random, then it has a 60% chance of having a fixed point.

2. Describe an efficient way for a computer to generate a 1,000-bit random number to be used in El Gamal encryption or Diffie-Hellman key generation. This number must be 100% random, unlike the random-number generator built into most programming languages. Also, your approach must not depend on input from the human user(s) wishing to do the encryption or key exchange. (Hint: Think outside the box.)

3. The El Gamal cryptosystem works under the assumption that the sender, Bob, always chooses a different random number, k, which he uses to generate the first term, $a = g^k \bmod p$, in the ciphertext, (a, b), that he sends to Alice. Show how the security of El Gamal encryption is compromised if Bob uses the same random number, k, to encrypt two (different) messages, M_1 and M_2, for Alice. For example, show how you can compute $M_1/M_2 \bmod p$ in this case.

4. Suppose a hash function f randomly maps n integers into the range $[0, 2n - 1]$.
   (a) Give a good bound on the probability that two integers collide.
   (b) Show that with probability at least $1 - 1/n$, the number of integers colliding for any given output value is $O(\log n)$.

5. Use Fermat's little theorem to compute $3^{201} \bmod 11$. Show your work.