15-859(D) Randomized Algorithms

Homework # 5 **due: November 19, 1998**

Exercises:

1. Problem 11.3 in the book (show that given an oracle for estimating the number of matchings in a bipartite graph, one can produce a near-uniform generator of matchings in a bipartite graph).

2. Describe a decision (yes/no) problem that is poly-time equivalent to factoring (given an oracle for solving the decision problem one can factor and vice-versa) and show that your decision problem is in NP $\cap$ co-NP.

Problems:

3. Exercise 14.4 (p. 397) in the book: prove for $n = p_1^{k_1} \cdots p_t^{k_t}$ that

$$\phi(n) = \prod_{i=1}^{t} p_i^{k_i - 1}(p_i - 1).$$

   Thus, given a factorization of n we can compute $\phi(n)$.

4. Problem 14.3 in the book: show that given n and $\phi(n)$ we can compute the factorization of n (note: we did this in class just for the special case $n = pq$).

5. (Due to M. Blum). Consider an instantiation of RSA with encryption exponent equal to 3. That is, a plaintext message x is encrypted into cyphertext message m by computing $m = x^3 \bmod n$, where n is the recipient's public key. (Assume $x < n$.)

   Suppose someone uses this method to send the same message x to three different people, Show how an eavesdropper, listening on all three lines, can recover the plaintext.