15-852 Randomized Algorithms

Homework # 4 **due: March 19, 1997**

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).

Problems:

2. Problem 11.6 in the book. In part (a) you should also show that the stationary distribution is uniform.

3. Suppose we sped up the random walk in Problem 2 as follows: after picking edge e, we find the cycle caused by adding e into the current tree, and select f at random *just from those edges in the cycle.* Does your algorithm still work correctly? If not, can you find a way to modify your algorithm to allow for this slightly different random walk?

4. (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.

   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.