**PROBLEM SET 9 – Week 12**

1. Resilience (50pts)

For this task, you can use your own (or shared) data for full credit or the gnutella network gnutella2.gdf for 80% credit. The Guess toolbars, downloadable as 'resiliencedegree.py' and 'resiliencebetweenness.py' from cTools will work on modestly sized networks (~1000 nodes) that are undirected. If your network is directed, you will need to either make an undirected version of it for these scripts to work (or modify the scripts). The resilience toolbars will let you specify the % of nodes to be removed and whether it is random failure (nodes are selected at random) or targeted attack (the highest degree nodes or nodes with highest betweenness are removed). It will also compute the size of the largest component and display the network after the nodes are removed. You may also do this assignment in igraph or any other software.

Please answer the following about the network (turn in 1 image of the original network, and 1 image of the network at less than 1/2 of its original size according to one of the attack strategies).

A. First tell me what network you are using (what are the nodes and edges). Then tell me what percentage of the nodes need to be removed to shrink the giant component to 1/2 of its size in degree targeted vs. betweenness targeted vs. random failure? Comment on this result with respect to the degree distribution and community structure (or lack thereof) in your network.

B. Now construct a random network with the same number of nodes and edges (you can do this by selecting 'Empty' when starting up Guess and then typing

```
>>> makeSimpleRandom(numberofnodes,numberofedges)
```

How do the percentages of nodes removed compare in the intentional attack and random failure in order to reduce the size of the largest component in this network by 1/2? Compare this with the answer to 2A: how does the resilience of your network (observed in A) compare to that of this equivalent random graph?