Math 4450/6450 Cryptography Test #1 – February 29, 2010

1. What is the size of the keyspace of a Hill cipher over $\mathbf{Z}/p\mathbf{Z}$ where we encode blocks of four numbers together and p is prime? How do we prove this?

2. Please explain an attack to find the key length of the Vigenere cipher, and why it works.

3. Please find the shared secret that Alice and Bob share if they are working with $(p, g) = (17, 3)$, Alice sends 8 to Bob, and Bob sends 4 to Alice. About how long should this attack take if p is replaced by a very large prime?

4. Please give an efficient algorithm for computing the order of a unit in $(\mathbf{Z}/n\mathbf{Z})^\times$ when n is very large, and use it to find the order of 7 in $(\mathbf{Z}/31\mathbf{Z})^\times$.

5. Please describe an efficient algorithm to generate a secure El Gamal keypair, being careful to label the entries in your public and private keys.