WORKSHEET #4 – MATH 5405
SPRING 2016

DUE: TUESDAY, 2/9/2016

We will play around with Diffie-Hellman key exchange. You may work in groups (as long as those groups have a primitive element).

1. Consider the prime 29. Verify that 10 is a primitive root mod 29.

2. Alice and Bob want to find a common key to communicate securely. Alice choose the prime 29 and the primitive root 10. She choose her own *secret* key s and shared $15 = 10^s \bmod 29$. Suppose Bob choose his secret to be $t = 11$. Find Alice and Bob's shared key.

3. Now take on the role of Eve. Figure out what Alice's secret key s was.

That was too easy. Alice and Bob need to choose a new prime that's not so easy to brute force. They chose $p = 3847$ and for their generator they chose $x = 5$.

4. Use a computer to help verify that 5 is a generator mod 33703. You can use the code from the homework due Thursday if you'd like (or better yet, write your own faster code).

5. Alice chose a private key s and computed $5^s \bmod 33703 = 7108$. Take the role of Eve and write a computer program in python that will find s.