Math 290 Number Theory for Teachers
Homework 5
Due: Friday, February 21, 2014

This homework will be a collaboration between you and two other group members, but each group member must turn in his or her own problem set. If you have problems with your group members, please let Li-Mei know. You are not expected to do these computations by hand. Just explain what computations you are doing and show your work for full credit.

1. Each person in the group should choose primes p and q larger than 100 and a power k relatively prime to $\varphi(pq)$. Share the numbers $m = pq$ and k with your group members, but not p and q. For this problem set, record p, q, k and what information you shared (made public) and what information you kept private.

Each person in the group should encode one message, decode one message, and play evil eavesdropper for one message.

2. For the **encoding**: Use one of the other group member's public information to encode a message of at least 15 characters for them. Make sure that each group member will get a message. Show your work for this problem set–how you went from the original message to the encoded message.

3. For the **decoding**: Take the message that your groupmate encoded for you and decode it using your secret information. Make sure that you show your work for this problem set.

4. For the **eavesdropping**: Intercept a message not meant for you (and that you didn't encode). Explain what you would need to know in order to decode it. (You don't have to decode it; just explain how you would.) Explain why this seems difficult.