Kerry Ojakian's CSI 30 Class
Class Assignment #13

1. Consider RSA encryption. Suppose your private key is $(65, 3)$. Someone sends you the encrypted message "6". Decode it.

---

2. Consider RSA encryption. Now you are an eavesdropper. Bob's public key is $(51, 13)$. Someone sent Bob the encrypted message "12". Decode the message. You can do this without even knowing Bob's private key.

---

3. Consider RSA encryption. Use the primes 3 and 11, and $e = 13$.

   (a) Find your public key.

   (b) Find your private key.

   (c) If someone wants to send you the message "2", what is the encrypted message they would actually send.

   (d) If you receive the encrypted message "10", what is the person's message?

4. We will partition the class into 4 groups, named for the elements of Z_4. Each group will get space on the blackboard.

   - Part 1: Each group creates a public and private key (keep it small!). Write your public key in your group's board space.
   - Part 2: If you are group x, send a single secret letter to group $x + 1 \pmod 4$, using their public key. Write your encoded message in their board space.
   - Part 3: Decode the secret message passed to you, using your private key.