William Graf **Homework 12** **Due 12-05-2014**

1. (a) Determine if 606569164077864874518588414841413446607652176924984336995613984952992907447475027613937403849941704666576913370745903006519304958947642217 89 is prime or composite. If its composite, 100 bonus points for factoring it

   (b) Determine if 224178259488991931700981007028965871369168422146983073607496713558119004684769184887510566741439513940537077619139651208615052957503807991 31 is prime or composite. If its composite, 100 bonus points for factoring it

2. Suppose you recover the following message fragment: 87415581744223671646124280297023535991431480011984840136452974750532742474417057269184035466144083777751133749535883792723985712141607810152906162253 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key $e = 480590457894161571799451751775206761304190787812356118724007711420348105587214340123017182025699801777227437966164297496589842792840377178563362272 37$ and private keys: $p = 600240205395180100025353918303007729488569913698639834023990766188028292889$ and $q = 21913968673995383933484913172964216184822552886649679341538658056523114594 9$.

3. You and I set up a Diffie-Hellman key exchange with prime $p = 135555886108689616799030228732786954906 27$, and primative root $a = 2$. You choose as your private key, $x_{\text{you}} = 948892405836560413737047214784624745862 3$. You look up my public key it is: $\alpha_{\text{my}} = 213573561003477851594654882645732330871 5$.

   (a) What is your public key?

   (b) What is our common key?

   (c) (100 Bonus Points) What is my private key?

   (d) If you were unable to answer the previous question, what difficult problem were you unable to solve?

4. (a) Make a table of powers of 10 (mod 19).

   (b) Use that table (you must show you are using the table to get full credit) to find 7^{12} (mod 19).

   (c) Use that table (you must show you are using the table to get full credit) to find, x such that $12^x \equiv 8 \pmod{19}$.

   (d) Use the table to find all primiative roots of 19.