John Slater **Homework 12** **Due 12-05-2014**

1. (a) Determine if 434509339313825594162653364945567248550454626454963235520941147135693176894149976856221026524265321493668208143849077242676400821823304379 7 is prime or composite. If its composite, 100 bonus points for factoring it

   (b) Determine if 677315043441706989159588982780719509530917746251124637220248164294152392843619735497923129168999555932538294371968359128569909971754620217 91 is prime or composite. If its composite, 100 bonus points for factoring it

2. Suppose you recover the following message fragment: 349689943599660268831466651430005874390848612604499603703934545360295445096340049650241262148648781663405389672426586013549214785696404888656216261 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key $e = 260987784362191260737966884448448382639443523358286017483645984020987116477864542534542617673633939659076029948155734551261953198792368958295157717$ and private keys: $p = 3045608048760829281$ and $q = 1453594942360595065206871380409785832635435483856741234675131160383583553$.

3. You and I set up a Diffie-Hellman key exchange with prime $p = 89068631541784244541336489268662727970 03$, and primative root $a = 2$. You choose as your private key, $x_{\text{you}} = 80197380462371524726363726348981053537 22$. You look up my public key it is: $\alpha_{\text{my}} = 68517498125716931466719840883234159276 79$.

   (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.