Nickolas Martinez **Homework 12** **Due 12-05-2014**

1. (a) Determine if 419174457742565437735410085087874563767609764469695385927902804431217001433708491547752788272329083069692370380737691088281629269537224679 03 is prime or composite. If its composite, 100 bonus points for factoring it
   (b) Determine if 838028789363463934749874479539091476148843134723379059386034323258737572765857247004166744062821421514974889839248507174958172822249744511 39 is prime or composite. If its composite, 100 bonus points for factoring it

2. Suppose you recover the following message fragment: 492859123202207939203721576767426173155867931363755910274315471245529891722536483955425526259756565457743296998569503602420962114493842762261037351429 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key $e = 403284564071905297799579235981169671197474825020594138958487568853352271267628286786380136123916915606638332413828717301455232873623301724291209261981$ and private keys: $p = 690942844250646778384389229295948519210529904762924747707252690502942538593$ and $q = 8496164724703368134193012618247462610530294500249736176095478306152387174 99$.

3. You and I set up a Diffie-Hellman key exchange with prime $p = 401384257295161733133984765039156149966 39$, and primative root $a = 13$. You choose as your private key, $x_{\text{you}} = 166628526800789463006604946493421825123 73$. You look up my public key it is: $\alpha_{\text{my}} = 181193116494904833174443502401058844371 3$.
   (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.