Peter Lucas **Homework 12** **Due 12-05-2014**

1. (a) Determine if 230500773032553159239082184178422447943774513596756901225505608689232557178987095173813272270943132374998889401195193210636802682222824143 23 is prime or composite. If its composite, 100 bonus points for factoring it

   (b) Determine if 203936500922974923931805580293155658060037368921845276504787352727027699983903326009298686592273674541057388239607292391986318571000074330 71 is prime or composite. If its composite, 100 bonus points for factoring it

2. Suppose you recover the following message fragment: 176757602902901284738979982515020754163604858690937049968379257051590333206293128736380949160940781753688985426626258302144782206259146065961203456 0 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key $e = 53782949105379431948143851378445355740932918830737392485320509783524636921694648841310861620617798828384702125554055028571249623069006017072162673305$ and private keys: $p = 11834970536431037746207050064104106706789624775107305154644543985605581563$ and $q = 80061995291638998435502364745021675640100322159686640652542299080290455343 7$.

3. You and I set up a Diffie-Hellman key exchange with prime $p = 14877079290264587697322117715331945093803$, and primative root $a = 2$. You choose as your private key, $x_{\text{you}} = 72845785481647461296214785980431197953 28$. You look up my public key it is: $\alpha_{\text{my}} = 18305481763018530404439404135878361328 54$.

   (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.