Sara Mills **Homework 12** **Due 12-05-2014**

1. (a) Determine if 263971561528920616734719481550558507053587468809734470480776001876408265223219114775084265031990690177815089740164579165619765636958994506 47 is prime or composite. If its composite, 100 bonus points for factoring it

   (b) Determine if 488201074680928332129651732099021391784465757297337421150506388258888112215866559233474392257413785023275573560608778027194572748742242086 3 is prime or composite. If its composite, 100 bonus points for factoring it

2. Suppose you recover the following message fragment: 155569159442807947826197582424583507093562898086527642933713795235986430144004384981475624211595397929616099357910521583383815006609941885705988833341 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key $e = 493936079822226373773078103555479444177653533697495352197964033026997361578980479225887991849380253695762323059130115858095881277207128184458524549 5$ and private keys: $p = 6981435478518721003185534962335067476344995776248575240090608399911435758 69$ and $q = 2663142615475731181143052555613582863367770926370778203335208959586087318 7$.

3. You and I set up a Diffie-Hellman key exchange with prime $p = 77545670293437147188573372878788885643307$, and primative root $a = 2$. You choose as your private key, $x_{\text{you}} = 591290401296005207134891414778418937811 00$. You look up my public key it is: $\alpha_{\text{my}} = 205568793231735423389306348441548796229 48$.

   (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.