Taylor Coury **Homework 12** **Due 12-05-2014**

1. (a) Determine if 27460035718692096411558971365297242717871414385924823357482924902293370842517142183216195723317883900428954444692187090710733051325369 99119 is prime or composite. If its composite, 100 bonus points for factoring it

   (b) Determine if 436051362275350323960727043078432246545981669131845315325855056655039804751932291948779049216396127293260808053852445159730389812113202106 7 is prime or composite. If its composite, 100 bonus points for factoring it

2. Suppose you recover the following message fragment: 883425372617558967531932867450307541457334742656016701188595617390856536669594575937668204934465606294910037057547425058611615820745193905010298371 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key $e = 7939371389479889170717349792959906116519455506818247362796527823605534388614054992296199290974542899699838734437836474570267251508327178550638829 71$ and private keys: $p = 1550432531417399510705274184362209353682054761093570694950049998478950327 7$ and $q = 7454909298225400841829369242601628068728001976792540823812177436260279891 1$.

3. You and I set up a Diffie-Hellman key exchange with prime $p = 254120312914718509586354174408206406241 47$, and primative root $a = 2$. You choose as your private key, $x_{\text{you}} = 206421641839634748654043365533207928494 74$. You look up my public key it is: $\alpha_{\text{my}} = 270431132656720525236289081528789131915 6$.

   (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.