Alessandra Cole **Homework 12** **Due 12-05-2014**

1. (a) Determine if 714404589173372506772256436645727130169909529407063297068042388377457360232586640393210900158597414569370017864414634645942797699949939493 949321 is prime or composite. If its composite, 100 bonus points for factoring it

   (b) Determine if 344677791201869908590343404335916551519921594316296236490228462004460244037036177940834744996168808660126176880194144232988814052984090804481 is prime or composite. If its composite, 100 bonus points for factoring it

2. Suppose you recover the following message fragment: 361141475338558110172144626076124766769596307086335949450886970101120490350660601425243774279450957161378959128620594536035291797564477945793011826248 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key $e = 158658679045941052677288055602573212774902787214401772573933652490514442849627919152215434327786972430738527630155186559085362236853854478870043573757$ and private keys: $p = 6328635651462778609919639373919500342391821802117523217797490394057012277 83$ and $q = 756881041913589651125703940637319416975428340785507556406650485160726407937$.

3. You and I set up a Diffie-Hellman key exchange with prime $p = 709514697884457481605289599271768502461 19$, and primative root $a = 13$. You choose as your private key, $x_{\text{you}} = 640352363171254147017699802784398091000 22$. You look up my public key it is: $\alpha_{\text{my}} = 581558359364761444790051354523713556644 38$.

   (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.