Tadeusz Dlugolecki **Homework 12** **Due 12-05-2014**

1. (a) Determine if 74526894945352346837642438049775398664699793346230495109897681109164385467516712140741123837008288747782344688846529336658125182083859167629 is prime or composite. If its composite, 100 bonus points for factoring it

   (b) Determine if 59654367631981952607013560677194929877703949690065656672095432582029012828947738079281398849015415411025803912396759300613363538009425050637 is prime or composite. If its composite, 100 bonus points for factoring it

2. Suppose you recover the following message fragment: 285553222491450184162649708581336058555484033763448547304867745056312997247168344413771639142949480428394159810877986140766504462025584148218085739387 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key $e = 366691874648428105647275854078019031225602913079543503556375270587104320691749328405806879954834484291068869704566985011912272976076595417903460807741$ and private keys: $p = 936123909525785741291844257678293925994701428953258755787580243521295318721$ and $q = 682425810183091754472376382863104993864240131234120017582731174390332347031$.

3. You and I set up a Diffie-Hellman key exchange with prime $p = 3673293158364942958009613645421058129943$, and primative root $a = 5$. You choose as your private key, $x_{\text{you}} = 1228948834959609662098006989996633546995$. You look up my public key it is: $\alpha_{\text{my}} = 2466036811256744177465548468693045825540$.

   (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.