Math 3207 Assignment 5, April 2016

Please show all working and reasoning to get full marks for any question. Hand in your rough working as well so I can see how you investigated and reached your final results. You can use Maple at any point and can email me any worksheets you created.

You are reminded that plagiarism is a serious offense and when it is detected you will be punished. Feel free to discuss the questions in general with myself and your colleagues but the work attempted must be yours alone.

1. (a) Show that your number n is composite by showing that 3^n is not congruent to 1 mod n using repeated squaring of 3 mod n. [2]

   (b) Determine the continued fraction of $\sqrt{n}$ by using surds until they repeat and calculate the convergents $\frac{\alpha_j}{\beta_j}$ of the first 6 terms and check to what percentage each is an approximation of $\sqrt{n}$. Verify that the values of the denominators of the surds appear as expected when you calculate $\alpha_j^2 - n\beta_j^2$. [5]

   (c) Use the continued fraction method to factorise n. [2]

   (d) How many iterations would Fermat factorisation with $k = 1$ take to find the factorisation? What odd number k would find the factorisation the fastest? How many steps would it usually take for Pollard $p - 1$? Explain your answers fully with evidence. [3]

2. (a) Verify that for your continued fraction for $\sqrt{n}$ the remainders are all of the form $r = \frac{\sqrt{n}-p}{q}$ and explain why this is true in general for any given n and how it implies that the continued fraction eventually repeats by showing that $p < \sqrt{n}$ and $q < 2\sqrt{n}$. What is the longest possible period for such a continued fraction? [3]

   (b) By considering the irrational numbers of the form $\frac{\sqrt{n}+p}{q}$ show that the continued fraction for $\lfloor\sqrt{m}\rfloor + \sqrt{m}$ is purely periodic and palindromic for any m which is not a perfect square. [3]

3. Suppose that my public key is n and my public key is 3163, create the message "OK" using the 26 letter alphabet to send to me. Using your knowledge of the factorisation of n, determine what my private key would be. [2]