MATH 4282 – Cryptography Assignment #8
Winter 2012

Instructions

- Answer each question completely; justify your answers.

1. Suppose that Alice prepares to use RSA by selecting primes p and q and computing $n = pq$, etc. Without loss of generality, assume that $q > p$ and let $d = \frac{q-p}{2}$.
   (a) Prove that $n + d^2$ is a perfect square.
   (b) If given an integer n that is the product of two primes, and given a small positive integer d such that $n + d^2$ is a perfect square, show how to use this information to factor n.
   (c) Use your answer above to factor $n = 2189284635403183$.

2. Use the Pollard ρ algorithm to factor n:
   (a) $n = 3131$
   (b) $n = 482431$
   (c) $n = 1002468832301$