Math 1350 RSA Exercises - August 2, 2010

You may use a calculator or computer for exercises 3 and 4. However, you MUST show your work on paper for successive squaring of the numbers and the product you calculate to get the exponent you need.

1. Suppose Boris picks primes 11 and 23.
   (a) What are m and n?
   (b) If Boris picks $e = 63$, what should his decryption exponent d be?
   (c) Which of the following e would be possible as encryption keys: 22, 37, 64, 229? Why?
2. Now Boris publishes m and e for Clarissa to send him a message, along with the guideline that A should be represented by 5, B by 6, C by 7, etc. through Z by 30. Clarissa wants to send him the message `TALK NOON`.
   (a) What numbers will Clarissa calculate, including the exponent and modulus?
   (b) What message will Boris receive?
3. You wanted to be able to receive messages encrypted by RSA, and you choose the following values: $p = 7, q = 13, m = 91, n = 72, e = 47$.

   You posted that each letter should be encrypted individually, numbered by A being 0, ..., Z is 25.

   Find your decryption key d and decrypt `4 57 13 42`.
4. Encrypt the name `ADAM` using 2 letter blocks, numbering the letters A=00, B=01, C=02, ..., Z=25. Let $m = 2599, n = 2^3 \cdot 3^3 \cdot 11$, and $e = 17$.