Problem Set 6

During class on November 11th, we determined that the RSA encryption scheme needs to meet the following three conditions in order to be considered secure and reliable. (The numbered steps referenced below refer to the steps in the RSA process as described on the handout from class that day.)

Condition 1. In Step 4, we should always be able to find a value for *d* regardless of my choices for *p*, *q*, and *e*.

Condition 2. The value for *x* calculated in Step 9 should always equal the value of *x* that Bob selects in Step 6.

Condition 3. The number *m* needs to be very difficult for Eve to factor.

Here are the three relevant theorems I distributed on the second handout in class that day:

Theorem 1. If *a* and *b* are relatively prime, then there exist numbers *s* and *t* such that $as + bt = 1$.

Theorem 2. Let *p* and *q* be distinct primes. For any integer *a*,

$$a^{k(p-1)(q-1)+1} \equiv a \pmod{pq}$$

where k is any positive integer.

Theorem 3. The number of prime numbers less than or equal to *n* is approximately equal to $\frac{n}{\ln n}$ for large values of *n*.

The questions in this week's problem set ask you to connect the dots between these conditions and theorems.

1. Use Theorem 1 to prove that Condition 1 is satisfied.

2. Use Theorem 2 to prove that Condition 2 is satisfied.

3. This is a two-part question.

    a. What does Theorem 3 tell you about the difficulty involved in factoring *m*?

    b. What assumptions did you make in your answer to part (a)?