From Bob to Alice – Part 1

Pair up with one person playing the role of Alice and the other the role of Bob. Go through the RSA encryption and decryption steps below.

Alice

1. Select two prime numbers p and q.
2. Calculate $m = pq$ and $n = (p - 1)(q - 1)$.
3. Select a number e that is relatively prime to n.
4. Find a number d such that $e \cdot d \equiv 1 \pmod{n}$.
5. Publish (that is, tell Bob) the values of e and m.

Bob

6. Let x be the numeric value of your message. (Note that x must be a number between 0 and $m - 1$).
7. Calculate the ciphertext $y = x^e$ MOD m.
8. Send the ciphertext y to Alice.

Alice

9. Calculate the plaintext $x = y^d$ MOD m.

Once you finish Step 9, "Alice" should compare the value of x *s/he found with the value of* x *that "Bob" chose. If those values are the same, you did everything correct. If so, swap roles and run through the steps again so that each member of the pair gets a chance to be "Alice."*

Then discuss the following questions in your pairs:

1. Which steps were the hardest ones to carry out? Would they be difficult for a computer to carry out?

2. What characteristics of this algorithm would you have to believe to be true in order to consider it a secure and reliable encryption scheme?

3. Which of those characteristics can you mathematically prove to be true? What additional information would you need to prove all of those characteristics?