The Procedure

1. Bob chooses prime numbers p, q so that $pq = n > c$, where c is the size of the largest message they expect to encrypt. n is called the key length.

2. Bob chooses e, d by first computing $\varphi(n) = (p-1)(q-1)$, then choosing e so that $\gcd(e, \varphi(n)) = 1$. Bob can then release the keypair (e, n), and now each Alice, Bob, and Eve have their own step to perform.

   Bob: computes the multiplicative inverse of $e \pmod{\varphi(n)}$, using Wolfram-Alpha, in order to find his private key d.

   Alice: chooses a message which is converted to a large natural number M. We have many ways of doing this, however for the purpose of this exercise we will use $a = 1, b = 2, \ldots, z = 26$, and a space is 00. For messages longer than a single character, simply combine the letters. For example, a message "abc" will be encoded with $M = 010203$. Alice encrypts her message text with Wolfram-Alpha using $M^e \pmod{n}$, and reveals it to both Bob and Eve.

   Eve: uses Wolfram-Alpha to attempt to factor n, and if successful, uses the p, q she finds in order to find d (see Bob's instructions above).

3. Now Bob and Eve (if successful) should reveal the decrypted messages; and confirm whether they recieved it.

Exercise 1

For the first exercise, delegate who will be Bob, Alice, and Eve, and perform the procedure with $p = 2$ and $q = 13$. This is exactly enough to encrypt a message of one character. Fill out the following:

1. What was the message sent by Alice?

2. What was Bob able to decrypt?

3. What was Eve able to encrypt?

4. How private was the message?

5. For what purposes would you use this level of encryption?

Exercise 2

For the second exercise, use `bigprimes.org` or some other random site to choose some primes p, q with more digits. Try to ensure that the primes are small enough that Eve has a chance at breaking the message. All participants will need Wolfram-Alpha.

1. What was the message sent by Alice?

2. What was Bob able to decrypt?

3. What was Eve able to encrypt?

4. How private was the message?

5. For what purposes would you use this level of encryption?

Exercise 3

For the final exercise, use `bigprimes.org` or some other random site to choose some primes p, q with enough digits that Bob and Alice can agree that Eve will not be able to factor n using Wolfram (How can they check this!).

1. What was the message sent by Alice?

2. What was Bob able to decrypt?

3. What was Eve able to encrypt?

4. How private was the message?

5. For what purposes would you use this level of encryption?