RSA Public-Key Encryption Lab

1. If necessary, click on the tab for the **Key Selection** worksheet. Use a random process to choose two different prime numbers **p** and **q** between 137 and 311 (displayed in a list in cells **g5:l15)**. Enter these primes in cells B6 and B7. Be sure that cells C6 and C7 both display the message "OK". The spreadsheet automatically computes the *modulus* (the product **p*q**) in cell B8 and the *Euler totient* (the product **(p-1)*(q-1)**) in cell B9. Note that the Euler totient would be difficult to determine from the modulus by itself; one needs to know the two primes. Write your two primes, your modulus, and your Euler totient below:

   p: _____ q: _____ modulus: _____

   Euler totient: _____

2. Choose a small number (no more that two digits) that has no factors (except 1) in common with the Euler totient. Enter this number as your public key and enter it in cell B15. If cell C15 displays the message **Invalid Public Key**, you need to select a different public key. When you have chosen a valid public key, the message **OK** will appear in cell C15. The spreadsheet will automatically compute your private key in cell B20. The private key is chosen so that **(Public Key)*(Private Key)** leaves a remainder of one when divided by the Euler totient. (This would not be possible if the private had a factor other than 1 in common with the Euler totient.) Write your public and private keys below:

   Public key: _____

   Private key: _____

3. Once both you and your partner have each created a modulus and pair of keys, you are ready to exchange encrypted messages. Give your **modulus** and **public key** to your partner. Do ***not*** give your partner your private key or Euler totient. In return, your partner will give you her/his public key and modulus.

4. Click on the tab for the **Encoding** worksheet. Enter your partner's modulus and public key in cells B6 and B7. Write these values below:

   Partner's modulus: _____

   Partner's public key: _____

5. Enter a message in cell B11. This message should consist of a string of fifteen or more CAPITAL LETTERS with no spaces or punctuation marks. The spreadsheet will encipher only the first fifteen letters of your message. Your message could be a

short phrase or sentence, your mother's name or your pet iguana's name. For example, I used **PLEASEHELPMENOW** to test this spreadsheet. Note that a message to be enciphered is usually called *plaintext*. The enciphered form of the message is called the *ciphertext*.

6. The enciphered form of the message (the ciphertext) should appear in cell B13. (This may take a few seconds.) The spreadsheet determines the ciphertext as follows:

   - Split the plaintext up into blocks of three letters (called *trigraphs*).
   - Obtain a numeric representation for each letter based on its position in the alphabet (A→0, B→1, etc.).
   - Compute a numeric code for each trigraph using the formula

     (First Letter Code) * 26^2 + (Second Letter Code) * 26 + (Third Letter code).

     For the mathematically inclined, this is interpreting each trigraph as a number in base twenty-six.

   - Encipher each plaintext trigraph code by computing (**Plaintext trigraph code)$^{\text{Public Key}}$**, dividing the result by the **Modulus** and taking the remainder.
   - Convert each enciphered trigraph code into a *quadragraph* – a block of four letters – as follows:

     - Divide the code by 26^3. The *quotient* is the code for the first letter of the quadragraph. The spreadsheet uses the *remainder* to get codes for the other three letters.
     - Divide the *remainder* from the first step by 26^2. The quotient is the code for the second letter. The spreadsheet uses the remainder to get the codes for the other two letters.
     - Divide the remainder from the second step by 26. The quotient is the code for the third letter and the remainder is the code for the fourth letter.

       For the mathematically inclined, this quadragraph calculation determines the representation of the enciphered message as a four-digit number in base twenty-six (using the letters of the alphabet as our digits).

Some of the details of this calculation appear in cells A16:K38 of the Encoding worksheet. Enter the plaintext and ciphertext below. Show the steps of the conversion process in the table.

Plaintext: _____

Plaintext		Ciphertext	
Trigraph	**Trigraph Code**	**Enciphered Code**	**Quadragraph**

Ciphertext: _____

7. Give the ciphertext (*but not the plaintext*) to your partner. In return, your partner will give you a ciphertext message. Record the ciphertext message from your partner below. In the rest of this exercise, you will be deciphering this message.

   Ciphertext from partner: _____

8. Click on the tab for the **Decoding** worksheet. Enter your modulus and your *private* key in cells B6 and B7 of this worksheet. Enter the ciphertext you received from your partner as the "Encrypted Message" in cell B13. The deciphering process is similar to the enciphering process:

   - Split the ciphertext up into quadragraphs (instead of *trigraphs*).
   - Obtain the numeric representation for each letter and compute a numeric code for each trigraph using the formula

     (First Letter Code) * 26^3 + (Second Letter Code) * 26^2 + (Third Letter Code) * 26 + (Fourth Letter Code).

     Encipher each ciphertext quadragraph code by computing

     (**Ciphertext quadragraph code**)$^{\text{Private Key}}$,

dividing the result by the **Modulus** and taking the remainder

- Convert each deciphered quadragraph code into a trigraph.
  - Divide the code by 26^2. The quotient is the code for the first letter.
  - Divide the remainder from the first step by 26. The quotient will be the code for the second letter and the remainder the code for the third.

Note that deciphering uses the *private* key in place of the public key. Some of the details of this calculation appear in cells A19:D23 of the Decoding Worksheet. The deciphered message should appear in cell B13. Record the results of each deciphering step in the table below.

Ciphertext		**Plaintext**	
Quadragraph	**Quadragraph Code**	**Deciphered Code**	**Deciphered Trigraph**

Now, write the deciphered message (plaintext) below.

Deciphered message: _____