**USING THE RSA SPREADSHEET**

**WARNING:** DO NOT enter values into boxes which are green or blue - you should ONLY enter values into yellow boxes.

**Encryption**
1. Open the Encryption worksheet.
2. Enter the smallest value for your plaintext in the yellow box next to the X. The spreadsheet will automatically adjust the rest of the plaintext values.
3. Enter values of \( p \) and \( q \) in the yellow boxes. The spreadsheet will automatically calculate the corresponding values of \( N \) and \( M \) for you.
4. Enter a value for \( e \) - the spreadsheet will tell you if it is relatively prime to \( M \). If not, choose another value.
5. The spreadsheet will automatically give you the encrypted values, \( Y \), and you can then use these to encrypt your message.

**Decryption**
1. Open the Decryption worksheet and look at the cells with a green background first.
2. The values of \( p \), \( q \), \( N \), \( M \) and \( e \) are automatically copied from the Encryption worksheet.
3. Calculate the value of \( d \) either by trial and error or by using Euclid's Extended Algorithm (Euclid worksheet, see below) and enter it into the yellow box for \( d \).
4. Enter the values you want to decrypt into the yellow boxes with \( Y \) at their left.
5. If the numbers involved in calculating values of \( X \) from values of \( Y \) aren’t too large, they will appear automatically in the next row, \( X \).
6. If you get #NUM!, this tells you that the spreadsheet can’t handle the calculations.
7. All is not lost! The blue columns on the left of the spreadsheet are set up to calculate large powers by an alternative method which should get round the problem - can you see what the method is? Enter the value of \( Y \) into the yellow ‘Y’ box and then go down the blue ‘Power of Y’ column until you are on the row corresponding to the value of \( d \).
8. The corresponding \( X \) value is the answer you want, and you can copy it into the lower \( X \) row.

**Euclid’s Extended Algorithm**
1. Open the Euclid worksheet.
2. The values of \( p \), \( q \), \( e \) and \( M \) are copied automatically from the Encryption worksheet. The calculation is carried out automatically from these values.
3. The value of \( d \) appears automatically in the final column.
4. This is how it works:
   i. The initial 1\(^\text{st}\) no. is \( M \) and the initial 2\(^\text{nd}\) no. is \( e \).
   ii. The 1\(^\text{st}\) no. is divided by the 2\(^\text{nd}\) no. and the quotient and remainder entered into the ‘Q’ and ‘R’ columns.
   iii. The ‘\( a \)’ and ‘\( b \)’ columns give the remainder as a combination of multiples of \( M \) and \( e \).
      Example:
      
      If \( M = 160 \) and \( e = 7 \), we have
      
      \[
      160 \div 7 = 22 \times 7 + 6, \quad \text{so } Q = 22 \text{ and } R = 6
      \]
      
      \[
      6 = 1 \times 160 - 22 \times 7, \quad \text{so } a = 1 \text{ and } b = -22
      \]
   iv. \( d \) is the final \( b \) before a zero remainder occurs, mod \( M \).
5. This algorithm always works to find a value of \( d \). For small calculations, trial and error may be quicker if you are doing it by hand, however. The main use of this algorithm is to find highest common factors.