

## 18.310 Homework Assignment #6:

1. Choose two primes  $P$  and  $Q$  between 1000 and 2000. (They are chosen this size so that multiplying two numbers less than  $N = PQ$  doesn't overflow your spreadsheet arithmetic. Find them any way you want.) Construct an RSA encoder and decoder based on the number  $N = PQ$  as follows.

1a. Find a suitable number  $c$  so that the encoded message  $r$  is found by taking the message  $m$  and raising it to the power  $c$ , so  $r = m^c \pmod{N}$ .

1b. Now construct a spreadsheet program that uses Euclid's algorithm to find  $d$  so that the decoding is done by taking  $r^d \pmod{N}$ .

1c. Construct an encoder on a spreadsheet that inputs the message, and outputs  $r = m^c \pmod{N}$ .

1d. Construct a decoder on a spreadsheet that takes the output from the encoder, and raises it to the  $d^{\text{th}}$  power  $\pmod{N}$  to decode the message.