Second Computer Assignment

Implement the RSA public-key cryptosystem. You should choose two prime numbers that are at least 2 digits long (greater than 100), and output the product of these primes and the exponent e to encrypt. You should query the user (me) to input a 4 digit message M, and your program should output the encrypted message M^e. You should then demonstrate that you can decrypt M^e by outputting "The original message was $(M^e)^d = M (\text{mod } pq)$" for your private key d (which you will have to compute).

This project should be emailed to me no later than Friday November 2 at 5 PM. Include in your email a description of how you found your private key d.