MCS 425: Codes and Crytography

Homework 4

Due in class, Friday September 28

This assignment is to write your own code to implement the RSA algorithm.

You will need to write the following functions and subroutines:

- Compute the decryption exponent d (write the code for modular inversion by using the extended Euclidean algorithm)
- Encryption algorithm: given the message m, and n and e, compute the ciphertext c.
- Decryption algorithm: given c, n, and d, compute the message m.

In the encryption and decryption algorithms make sure to implement the successive squaring algorithm to do modular exponentiation efficiently. Your algorithms should work quickly for numbers that are 100 or 200 digits long.

You do not need to write functions to test p and q for primality or to come up with large primes.

Send your code in by email.