Homework 18, due October 18

(1) (Page 193, problem 7) Nelson uses RSA to receive a single ciphertext c, corresponding to the message m. His public modulus is n and his public encryption exponent is e. Since he feels guilty that his system was used only once, he agrees to decrypt any ciphertext that someone sends him, as long as it is not c, and return the answer to that person. Eve sends him the ciphertext $2^e c \pmod{n}$. Show how this allows her to find m.

(2) (a) Use the Legendre symbol to determine whether 123 is a square (mod 401). Note that 401 is prime.
(b) Evaluate the Jacobi symbol $\left(\frac{24601}{365235}\right)$ showing each step, and explain what the answer means.

(3) (a) Test 118901521 for primality using the Fermat test for several values of a. Is 118901521 prime?
(b) Test 104173 for primality using the Solovay-Strassen test. Use enough values of a to be 99 percent sure that it is prime. (Recall from class that if a number is composite, the test will tell you so for at least half of the possible a.)