Homework 17, due October 14

(1) (a) (Page 193, problem 8) In order to increase security, Bob chooses n and two encryption exponents e_1, e_2. He asks Alice to encrypt her message m to him by first computing $c_1 \equiv m^{e_1} \pmod{n}$ and then encrypting c_1 to get $c_2 \equiv c_1^{e_2} \pmod{n}$. Alice then sends c_2 to Bob. Does this double encryption increase security over single encryption? Why or why not?

(b) (Page 193, problem 11) Suppose that there are two users on a network with RSA moduli n_1 and n_2 (not equal to each other). If you are told that n_1 and n_2 are not relatively prime, how would you break their system?

(2) (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.

(3) (Page 194, problem 16) Suppose two users Alice and Bob have the same RSA modulus n and suppose that their encryption exponents e_A and e_B are relatively prime. Charles wants to send the message m to Alice and Bob, so he encrypts to get $c_A \equiv m^{e_A}$ and $c_B \equiv m^{e_B}$. Show how Eve can find m if she intercepts c_A and c_B.