Homework 19, due October 19

(1) (a) Does 48382 have a square root modulo 83987? Explain.
  (b) Let $n = 213523 \cdot 304687$. Find x and y with $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$.

(2) Suppose you know that

$$2716102579495508531 20^2 \equiv 6895623477363257591127495777410796786162454893304 98^2$$

$$\pmod{6465410235775891941079948367093647049851252987191349}.$$

Use this information to factor 6465410235775891941079948367093647049851252987191349.

(3) (Page 108, problem 27) Alice designs a cryptosystem (following Rabin) as follows. She chooses two distinct primes p and q congruent to 3 (mod 4) and keeps them secret. She makes $n = pq$ public. When Bob wants to send Alice a message m, he computes $x = m^2 \pmod{n}$ and sends x to Alice. She makes a decryption machine that does the following: When the machine is given a number x, it computes the square roots of $x \pmod{n}$ since it knows p and q. There is usually more than one square root. It chooses one at random and gives it to Alice. When Alice receives x from Bob, she puts it into her machine. If the output from the machine is a meaningful message, she assumes it is the correct message. If it is not meaningful, she puts x into the machine again. She continues until she gets a meaningful message.
  (a) Why should Alice expect to get a meaningful message fairly soon?
  (b) If Eve intercepts x (she already knows n), why should it be hard for her to determine m?
  (c) If Eve breaks into Alice's office and can try a few chosen ciphertext attacks on Alice's decryption machine, how can she determine the factorization of n?