Homework 31, due November 18

(1) (Page 321, problem 2) Suppose p is a large prime, α is a primitive root, and $\beta \equiv \alpha^a \pmod{p}$. The numbers p, α, β are public. Peggy wants to prove to Victor that she knows a without revealing it. They do the following.
  (a) Peggy chooses a random number $r \pmod{p-1}$.
  (b) Peggy computes $h_1 \equiv \alpha^r \pmod{p}$ and $h_2 \equiv \alpha^{a-r} \pmod{p}$ and sends h_1, h_2 to Victor.
  (c) Victor chooses $i = 1$ or $i = 2$ and asks Peggy to send either $r_1 = r$ or $r_2 = a - r \pmod{p-1}$.
  (d) Victor checks that $h_1 h_2 \equiv \beta \pmod{p}$ and that $h_i \equiv \alpha^{r_i} \pmod{p}$.

They repeat this procedure t times, for some specified t.
  (a) Suppose Peggy does not know a. Why will she usually be unable to produce numbers that convince Victor?
  (b) If Peggy does not know a, what is the probability that Peggy can convince Victor that she knows a?
  (c) Suppose Nelson tries a variant. He wants to convince Victor that he knows a, so he chooses a random r as before, but does not send h_1, h_2. Victor asks for r_i and Nelson sends it. They do this several times. Why is Victor not convinced of anything? What is the essential difference between Nelson's scheme and Peggy's scheme that causes this?

(2) (Page 322, problem 3) Nelson thinks he understands zero-knowledge protocols. He wants to prove to Victor that he knows that factorization of n (which equals pq for two large primes p and q) without revealing this factorization to Victor or anyone else. Nelson devises the following procedure: Victor chooses a random $x \pmod{n}$, computes $y \equiv x^2 \pmod{n}$, and sends y to Nelson. Nelson computes a square root s of $y \pmod{n}$ and sends s to Victor. Victor checks that $s^2 \equiv y \pmod{n}$. Victor repeats this 20 times.
  (a) Describe how Nelson computes s, assuming $p \equiv q \equiv 3 \pmod{4}$.
  (b) Explain how Victor can use this procedure to have a high probability of factoring n. (Therefore, this is not a zero-knowledge protocol.)
  (c) Suppose Eve is eavesdropping and hears the values of each y and s. Is it likely that she obtains any useful information, if no value of y repeats?

(3) (Page 323, problem 5) Peggy claims to know an RSA plaintext; n, e, c are public and she claims to know m with $m^e \equiv c \pmod{n}$. She wants to prove this to Victor using a zero knowledge protocol. They perform the following steps.
  (a) Peggy chooses a random integer r_1 and computes $r_2 \equiv m \cdot r_1^{-1} \pmod{n}$.
  (b) Peggy computes $x_1 \equiv r_1^e \pmod{n}$ and $x_2 \equiv r_2^e \pmod{n}$ and sends x_1, x_2 to Victor.
  (c) Victor checks that $x_1 x_2 \equiv c \pmod{n}$.

Give the remaining steps of the protocol. Victor should be at least 99% convinced that Peggy is not lying.