Chapter 14 Homework 1, 3

1. Consider the diagram of tunnels in Figure 14.2. Suppose each of the four doors to the central chamber is locked so that a key is needed to enter, but no key is needed to exit. Peggy claims she has the key to one of the doors. Devise a zero-knowledge protocol in which Peggy can prove to Victor that she can enter the central chamber. Victor should obtain no knowledge of which door Peggy can unlock.

   Peggy can enter the path she needs to in order to use her key. Victor can then enter and call out which tunnel he wants Peggy to use to exit. She can then use her key to go through the central chamber (if Victor did not call her corridor out already) and exit by the requested route. With 4 choices, there is only a $\frac{1}{4}$ chance of fooling Victor if Peggy does not have a key.

3. Naive Nelson thinks he understands zero-knowledge protocols. He wants to prove to Victor that he knows the factorization of n (which equals pq for two large primes p and q) without revealing the factorization to Victor or anyone else. Nelson devises the following procedure: Victor chooses a random integer $x \bmod n$, computes $y \equiv x^2 \pmod{n}$, and sends y to Nelson. Nelson computes the square root s of $y \bmod n$ 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. You may assume that p and q are $\equiv 3 \pmod 4$

   Nelson, knowing p and q, can calculate $y \equiv x^2 \pmod{p}$ and $y \equiv x^2 \pmod{q}$. Since we can assume $p, q \equiv 3 \pmod 4$, we have

   $$x_1 \equiv y^{\frac{p+1}{4}} \pmod{p}$$
   $$x_2 \equiv y^{\frac{q+1}{4}} \pmod{q}$$

   Then, using the Chinese Remainder Theorem, he can combine these congruences into one modulo $n = pq$.

   Alternately, he can compute $y_1 \equiv y \pmod{p}$ and $y_2 \equiv y \pmod{q}$. Then he can calculate $a_1 \equiv y_1^{\frac{p+1}{4}} \pmod{p}$ and $a_2 \equiv y_2^{\frac{q+1}{4}} \pmod{q}$. Next, he can calculate $b_1 \equiv q^{-1} \pmod{p}$ and $b_2 \equiv p^{-1} \pmod{q}$. Finally, he can calculate

   $$S \equiv a_1 b_1 q + a_2 b_2 p \pmod{n}$$

   (b) Explain how Victor can use this procedure to have high probability in finding the factorization of n. (Therefore it is not a zero-knowledge protocol.)

   Once Victor confirms $s^2 \equiv y \pmod{n}$, he knows $\pm x$ and $\pm s$. He can then find $(x - s, n) = p$. Once he obtains p, finding q is trivial.

   (c) Suppose Eve is eavesdropping and hears the values of y and s. Is it likely that Eve obtains any useful information? (Assume no value of y repeats.)

   This will not allow Eve to find p or q. This is not enough information to determine $\pm x$, which she would need to find n, p or q.