2007 - Exercises X.

1. Let p be a prime and α a primitive element of $\mathbb{Z}_p^*$. Ivan is given $b = \alpha^a \pmod p$ and he claims that he knows the discrete logarithm a of $b \pmod p$. Ivan wants to convince Jan of this fact but without revealing a to him.
   Propose a zero-knowledge protocol for this problem. Show that it satisfies completeness, soundness and zero-knowledge properties.

2. Alice and Bob want to find out whether they like each other.

   - Alice has a bit x_A such that $x_A = 1$ if she likes Bob and $x_A = 0$ otherwise.
   - Similarly, Bob has a bit x_B such that $x_B = 1$ if he likes Alice and $x_B = 0$ otherwise.
   - Alice and Bob want to compute $l = x_A \wedge x_B$.
   - To prevent possible embarrassment, they want to find out l without revealing their true feelings.

   A friend of Alice and Bob, Carol, proposes the following protocol:

   (i) Carol generates two random and distinct primes p, q such that $p \equiv q \equiv 3 \pmod 4$, a random quadratic non-residue y with Jacobi symbol 1 and computes $n = pq$. Then she announces the pair (n, y).
   (ii) Alice chooses a random $u_A \in \mathbb{Z}_n^*$, and sends $w = u_A^2 y^{x_A} \pmod n$ to Bob.
   (iii) If $x_B = 0$, then Bob chooses a random $u_B \in \mathbb{Z}_n^*$ and computes $z = u_B^2 \pmod n$, otherwise he sets $z = w$. Then he sends z to Carol.
   (iv) If z is a quadratic residue modulo n, then Carol announces 0, otherwise she announces 1.

   Answer the following questions.

   (a) Show that the protocol is correct.
   (b) Suppose that Alice knows what Bob sends to Carol. Show that Alice can learn something about Bob's bit x_B even if $x_A = 0$.
   (c) Propose a modification of the protocol so that it is still correct, but neither Alice nor Bob can learn anything about the other's bit, if his or her own bit is 0.

3. Show how to implement standard oblivious transfer using 1-out-of-2 oblivious transfer.

4. How can a group of people calculate their average age without anyone learning the age of anyone else?

5. Alice and Bob want to buy a new car, but they cannot agree on a color of the car. Alice wants peas-green colour, Bob prefers salmon-pink. However, Alice and Bob are not in the same city and are communicating over the Internet only. They have decided to toss a coin. Consider the following 4 ways to do it:

(1) Alice tosses a coin sends the result to Bob.

(2) Alice videotapes herself tossing a coin and sends the result and the video to Bob.

(3) i. Alice generates two random and distinct primes p, q such that $p \equiv q \equiv 3 \pmod 4$, chooses a random bit b and a random quadratic non-residue y modulo $n = pq$.
ii. Alice chooses a random $u \in \mathbb{Z}_n^*$, computes $z = u^2 \pmod n$ and sends $z' = zy^b \pmod n$ and n to Bob.
iii. Bob chooses a random bit b' and sends it to Alice.
iv. Alice reveals p and q and the result is $b \oplus b'$.

(4) i. Alice generates two random and distinct primes p, q such that $p \equiv q \equiv 3 \pmod 4$, chooses a random bit b and a random quadratic non-residue y modulo $n = pq$.
ii. Alice chooses a random $u_A \in \mathbb{Z}_n^*$, computes $z_A = u_A^2 \pmod n$ and sends $z'_A = z_A y^b \pmod n$, y and n to Bob.
iii. Bob chooses a random bit b' and a random $u_B \in \mathbb{Z}_n^*$, computes $z_B = u_B^2 \pmod n$ and sends $z'_B = z_B y^{b'} \pmod n$ to Alice.
iv. Alice reveals p and q and the result is $b \oplus b'$.

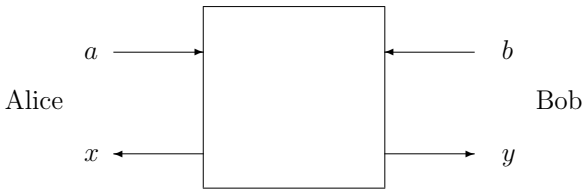
Answer the following questions and explain your reasoning.

(a) Show which of the protocols is resilient against cheating Alice?

(b) Show which of the protocols is resilient against cheating Bob?

6. Suppose that you have supernatural powers and you can control the local weather. More precisely, suppose that you can make it rain or not rain on the following day. How could you prove this to a suspicious scientist without revealing your magical methods so that the scientist would be 99,9% sure about it. How long would it take?

7. **Bonus** Design an unconditionally secure oblivious transfer protocol (standard or 1-out-of-2) which uses the following device. If such a scheme does not exist, explain the reason.



- The device has two inputs a, b and two outputs x, y.
- a, b, x, y are bits, related as follows: $a \cdot b = x \oplus y$.
- Alice (Bob) owns the input a (b) and the output x (y).
- Once Alice (Bob) inputs a (b), she (he) immediately obtains x (y).
- $Pr[x = 0 \,|\, a, b] = Pr[x = 1 \,|\, a, b] = Pr[y = 0 \,|\, a, b] = Pr[y = 1 \,|\, a, b] = \frac{1}{2}$