IV054 Coding, Cryptography and Cryptographic Protocols
2014 - Exercises X.

1. Assume you have zero-knowledge proofs for quadratic residues and nonresidues, that means you can prove with zero knowledge whether $x \in \mathrm{QR}(n)$ or $x \in \mathrm{QNR}(n)$. Consider the *Bit commitment scheme I* from the lecture slides. Let Peggy send to Victor two commitments $f(b_0, x_0)$ and $f(b_1, x_1)$ for bits b_0 and b_1. Find a zero-knowledge proof for Peggy to show that either $b_0 = b_1$ or $b_0 \neq b_1$.

2. Given multiple instances of the 1-out-2 Oblivious Transfer Box, construct a protocol for 1-out-k Oblivious Transfer.

3. Suppose that G is a finite group containing N elements, b is a fixed element of G, and y is an element of G for which Peggy has found a discrete logarithm to the base b, *ie.* she has solved the equation $b^x = y$ for a positive integer x. She wants to demonstrate to Victor that she knows x without giving him a clue as to what x is. We first suppose that Victor knows the order N of the group. Here is the sequence of steps performed:

   (1) Peggy generates a random positive integer $e < N$ and sends $b' = b^e$ to Victor.

   (2) Victor flips a coin. If it comes up heads, Peggy must reveal e and Victor checks that in fact $b' = b^e$.

   (3) If the coin comes up tails, then Peggy must reveal the least positive residue of $x + e$ modulo N, Victor checks that $yb' = b^{x+e}$.

   (4) Steps (1)-(3) are repeated until Victor is convinced that Peggy must know the value x of the discrete logarithm.

   Find answers for the following questions:

   (a) If Peggy does not really know the discrete log, then what are the odds against her successfully fooling Victor for T repetitions of steps (1)-(3)?

   (b) Suppose that Victor does not know the value of N.

      (i) Explain how the protocol described above is not really zero knowledge.

      (ii) How could Peggy decrease the amount of information Victor obtains about N?

   (c) Suppose that Peggy does not know N, and so in step (1) she chooses a random e in some other range (*eg.* $e < B$, where B is an upper bound for the possible value of N), and in step (3) she sends simply $x + e$ rather than the least positive residue of $x + e$ modulo N. Explain why this is not a zero-knowledge proof.

4. Suppose Alice and Bob are separated and cannot communicate. Let them play the following game. Both of them receive a single bit input x and y respectively (Alice does not know Bob's input and Bob does not know Alice's input). Their goal is to produce single bit answers a and b respectively. They win the game if $a \oplus b = x \cdot y$. Show that if they use deterministic strategies (*ie.* Alice chooses a based only on x and Bob chooses b based only on y), they cannot win the game with probability 1.

5. Random Access Code is the following protocol. Alice owns a random binary string $(a_1, a_2, \ldots, a_n)$, $a_i \in \{0, 1\}$ of length n. She is allowed to send to Bob a *single bit* message m. Bob randomly generates a number $j \in \{1, \ldots n\}$. Then he applies a corresponding decoding function D_j to the received bit a. The protocol is successful, if $D_j(m) = a_j$ for every $j \in \{1, \ldots, n\}$. Show that if Alice and Bob own a hypothetical device that allows them to win the game introduced in the previous exercise with probability 1, they can construct Random Access Code for $n = 2$.