Secure Computation: Homework 1

Submit in class or by email by **Wednesday March April 2, 2014**.
Prove the correctness of all your answers.

1. Following is a description of a sigma protocol for proving knowledge of an RSA decryption. The public information is n, an RSA modulus, e an RSA exponent, and a value y in Z^*_n. The prover knows x such that $x^e=y$ mod n. The protocol is the following
   1. P chooses a random r in Z^*_n and sends $a=r^e$ mod n to V.
   2. V chooses a random bit b and sends it to P.
   3. P computes $c=rx^b$ mod n and sends it to V.
   4. V accepts iff $c^e=ac^b$.

   a. Prove that this protocol satisfies the completeness property of sigma protocols.
   b. Prove that this protocol satisfies the special soundness property of sigma protocols.
   c. Prove that this protocol satisfies the special honest-verifier ZK property of sigma protocols.
   d. What is the probability that a prover that does not know x can successfully finish the protocol. How can we reduce the success probability of such a prover by repeating the protocol?

2. This exercise shows that it is possible to construct a commitment scheme from a Σ protocol.
   Assume we are given a *hard* relation R with generator G (this generator generates pairs (x,w) ∈ R), and an efficient Σ protocol P.
   Assume also that given x, it is easy to decide if there exists w such that (x,w) ∈ R. We denote this easy decision problem as checking if x ∈ L_R. (For example, if R is a relation that contains group elements x and their discrete log to the base g in some group, where g is a generator of the group, this check verifies that x is an element in the group.)
   With this set-up, it is possible to build a perfectly (i.e., unconditionally) hiding commitment scheme, which is efficient and allows commitment to many bits:
   - **Set-up:** V runs (by itself) the generator G on input 1^k to get (x,w) ∈ R. It sends x to P. P then checks that x ∈ L_R.
   - **Commit:** To commit to a t-bit string e, P runs the simulator M on input x,e to get (a,e,z), and sends the value a to V.
   - **Open:** To open the commitment, P sends e,z to V , who checks that (a,e,z) is an accepting conversation (w.r.t. x).

   Prove that this scheme is a perfectly hiding commitment scheme with computational binding. (For the hiding part of the proof, note that by the definition of Σ protocols the simulation is perfect, and therefore the first message a generated by the simulation is uncorrelated to the value e.)