Advanced Topics in Cryptography

Homework 1

Due by April 2, 2006 (before class).

Prove the correctness of all your answers.

1. Let OT^m denote 1-out-of-2 oblivious transfer of m bit inputs. Let ROT^m denote the following primitive:
   - The sender's input consists of two m-bit strings, x_0, x_1.
   - The receiver has no input.
   - At the end of the protocol the receiver learns (b,x_b), for a randomly chosen $b \in \{0,1\}$, and learns nothing about x_{1-b}. The sender learns nothing.

   Prove the following two reductions:
   a. It is possible to construct ROT^1 from OT^2.
   b. It is possible to construct OT^1 from ROT^1.

2. Consider an adversary to a secure multi-party protocol (MPC) which is semi-honest, but in addition can, at any point in the protocol, stop any of the parties which it controls from sending any additional messages. (For example, if it controls parties 1,2 and 10, it can make party 1 stop sending messages after step 3, and make party 10 stop sending messages after step 7.)
   Show how to adapt the protocol we showed in class to be secure against this type of adversary.