Homework #5: Protocol design  
(Optional extra credit assignment)
ECT 582, Prof. Robin Burke
Fall 2003
Due: 10/30/2003

Objective:
Design a protocol to solve an e-commerce problem.

What to do:
Radio 4 U is a subscription-based streaming radio service. Users buy subscriptions to different streams of music being continuously broadcast over the Internet. Users can take their music subscriptions to different locations (home, car, health club, office computer) by the use of a USB-compatible hardware token unlocked with a PIN. The Radio 4 U device itself has a place to plug in the token, a numeric keypad and a small 2 line LCD display.

Devise a protocol for the subscription-based streaming radio service so that subscriptions to different parts of the service are transferable between users, but the original user can no longer use his access credentials after the transaction. For example, Alice has paid to have access to the "Contemporary Jazz" and "Baroque" section of a streaming music service, and Bob has a subscription to the "Latin Jazz" and "Speed Metal" streams. Bob agrees to sell Alice his "Latin Jazz" service for some consideration. At the end of the protocol, Alice should have access to all three subscriptions and Bob would no longer have access to "Latin Jazz" even if he had somehow managed to make a copy of the contents of his hardware token before the transfer.

You may make any necessary assumptions about how the Radio 4 U subscription model works. It may be useful, for example, to assume that Radio 4 U makes use of PKI and public key certificates. You may not assume any extra interactive components beyond the radio itself, such as a separate web site for performing this subscription transfer. Your protocol should be secure in that Eve cannot transfer Bob's subscriptions to herself or generate fake transfers on Bob's behalf without breaking the cryptography.

Note that we not concerned so much with how the music data is actually streamed by Radio 4 U. You may make assumptions about this as necessary, but your protocol need only address subscription transfer.

Bonus points if your protocol is anonymous – that is, if Radio 4 U doesn't know who has transferred which subscriptions to whom.

What to turn in:
Post a description of your protocol on your web site. Your description should include an informal description of the Alice/Bob variety and also a more formal description that indicates what kinds of messages are exchanged and their contents. You should indicate what cryptographic operations you are using, and the locations where information is stored.