6.897 Spring 2004
Homework 3
Handed out: 4/16/2004
Due: 4/29/2004

The homework is to write a "referee's report" on the paper "Verifiable Mixing (Shuffling) of El-Gamal Pairs" by Andrew Neff, written four months ago (dated 12/31/2004). This paper more-or-less includes by reference his earlier paper (reference [23], "A verifiable secret shuffle and its applications to e-voting", from ACM-CCS 2001), so please consider the assignment to include portions of that paper as needed.

Pretend that I am the editor of a journal that has a broad but technical readership. Your report should offer constructive criticism of the paper. Try to understand the proposed method, and point out where the exposition is unclear, unmotivated, poorly organized, etc. If you get stuck, explain exactly where and why. If you think it should be organized differently, explain why and how.

There are many refereeing guidelines on the web, here are a couple that I found using google:
http://www.computer.org/tpds/taskofreferee.html?SMSESSION=NO
http://www.may.ie/nirsa/geo-pub/geo-refereeing.html

Do NOT include an answer to the question "Should this paper be published?" (possibly with revisions). Merely give constructive feedback to the author, noting strengths, weaknesses, errors, improvements, etc.

Your report WILL be sent to Andy Neff. Please indicate in a cover letter whether you wish it to be sent anonymously or not.

If you feel that your report might be useful to others attempting to read Neff's paper, and so you wish to have it posted on our server, please also let me know.

Feel free to collaborate and discuss the paper between yourselves, but the write-up should be your own. Please submit your report by email as a text file or as a pdf file.