Problem 1 [15+25pts]

1. We studied in the class how to send an anonymous email using (decryption-based) mix networks. We modified the explained decryption-based technique so that the receiver of an anonymous email can reply to the sender of the email (i.e., achieve two-way communication), without learning the identity of the sender. Can this technique be deployed in the real-world by simply installing only a new client software compatible with the given mix network? Explain why or why not. If your answer is negative, describe another mechanism that supports two-way communication (from client to a server and vice versa), without any loss of privacy.

2. The property of anonymity that we studied is as follows: the recipient knows that the message was sent by someone belonging to a group (of size $k$) but does not learn the identity of the sender (with a probability better than $1/k$). Another related property is called *unlinkability*, which can be described as follows: if a sender sends two (say different) messages to the same recipient, it is hard for the recipient to tell if the two messages were sent by the same sender; in other words, it is hard to link the two messages to the same sender. Does the mix networks technique provide unlinkability? Explain your answer. You can assume that the same group of senders (of size $k$) is being used by the mix network over the transmission of both messages.

Problem 2 [60pts]

We discussed web search privacy problem in the wake of the accidental release of AOL search data in 2006. In this exercise, your task is to evaluate the following mechanisms that are being deployed in practice to achieve web search privacy:

- Tor: [http://www.torproject.org/](http://www.torproject.org/)
TrackMeNot: http://mrl.nyu.edu/~dhowe/trackmenot/ (related documentation is here: http://www.nyu.edu/projects/nissenbaum/papers/HoweNissTMN.2.8d.pdf)

1. [10pts] Briefly describe the above mechanisms (since Tor was already discussed in class, you do not need to describe it) and how they try to achieve web search privacy

2. [50pts] Perform web (google) search using all three mechanisms (one-by-one) (whenever necessary, you would need to install the client software; a windows machine will suffice for the same). Now, critically compare the three mechanisms in terms of (1) the level of privacy provided, (2) performance at the client side as well as at the web search engine, and (3) the usability and level of convenience of web searching