Problem 1 [5*5=25pts]

In this problem, your task is to understand and compare the privacy policies of the three most famous world wide email services, namely, hotmail, yahoo, and gmail. Go to the following links for the respective policies and read through them carefully.

http://privacy.yahoo.com/privacy/us/mail/
http://mail.google.com/mail/help/privacy.html

Now, answer the following questions:

1. Identify the common features/properties in these privacy policies, and compare hotmail, yahoo and gmail based on these features. For example, one feature is concerning “spam”; so compare the policies of hotmail, yahoo and gmail with respect to “spam”.
2. Are there some features unique to a particular service (e.g. yahoo has it, but hotmail and gmail does not)? If so, are these features good? Should other services also include those features in their privacy policies?
3. Are there any features which you think should be included in the privacy policies, but are currently excluded? Explain these features and mention why they are important.
4. What are the mechanisms each email service employs to implement the above features? (You might have to search around to figure this out!) Mechanisms could be technical or non-technical or legislative.
5. Based on the features and based on the corresponding mechanisms, and based on your experience with these services (I assume you have accounts on at least two of them), which email service provides you the best “assurance” in terms of your individual privacy? Explain your answer.

Problem 2 [25pts]

Prove the Biba Security theorem for the Low-Water Mark Policy
[Hint: use mathematical induction]
Problem 3 [20+15+15pts]

1. We studied in the class how to send an anonymous email using mix networks. We studied two types of mix networks: decryption-based (involving layered encryptions) and re-encryption-based. Explain how to modify the explained decryption-based technique so that the receiver of an anonymous email can reply to the sender of the email, without learning the identity of the sender.

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.

3. Download the MixMaster anonymous remailer (unix-based) software from http://mixmaster.sourceforge.net/, build it, learn about it and use it to send me an anonymous email with the “Subject: CS 392_YourName”.