Homework #4

Due: May 24, 2013 **Points:** 100

Questions

1. (*30 points*) Consider a scheme that allows a recipient to reply to a message from a chain of Cypherpunk remailers. Assume that encipherment is used throughout the chain.

   (a) Bob selects a chain of remailers for the return path. He creates a set of keys and enciphers them so that only the key for the current remailer is visible to that remailer. Design a technique by which he could accomplish this. Describe how he would include this data in his message.

   (b) How should Alice's mailer handle the processing of the return address information?

   (c) When Bob receives the reply, what does it contain? How can he obtain the cleartext reply?

   (*text*, problem 14.3)

2. (*30 points*) Revisit the example for $x := y + z$ in Section 16.1.1. Assume that x does not exist in state s. Confirm that information flows from y and z to x by computing $H(y_s | x_t)$, $H(y_s)$, $H(z_s | x_t)$, and $H(z_s)$ and showing that $H(y_s | x_t) < H(y_s)$ and $H(z_s | x_t) < H(z_s)$ (*text*, problem 16.1)

3. (*20 points*) Let $L = (S_L, \leq_L)$ be a lattice. Prove that the structure $IL = (S_{IL}, \leq_{IL})$ is a lattice, given the following definitions:

   (a) $S_{IL} = \{[a, b] | a, b \in S \wedge a \leq_L b\}$
   (b) $\leq_{IL} = \{([a_1, b_1], [a_2, b_2]) | a_1 \leq_L a_2 \wedge b_1 \leq_L b_2\}$
   (c) $lub_{IL}([a_1, b_1], [a_2, b_2]) = (lub_L(a_1, a_2), lub_L(b_1, b_2))$
   (d) $glb_{IL}([a_1, b_1], [a_2, b_2]) = (glb_L(a_1, a_2), glb_L(b_1, b_2))$

   (*text*, problem 16.2, modified)

4. (*20 points*) Why can we omit the requirement $lub(\underline{i}, \underline{b[i]}) \leq \underline{a[i]}$ from the requirements for secure information flow in the example for iterative statements (see Section 16.3.2.4)? (*text*, problem 16.5)

Extra Credit

1. (*30 points*) Prove that a system that meets the definition of generalized noninterference security also meets the definition of deducible security. (*text*, problem 8.6)