Homework 5

Due: December 3, 2021 **Points:** 100

1. (*24 points*) Consider the statement

   if $(x = 1)$ **and** $(y = 1)$ **then** $z := 1$

   where x and y can each be 0 or 1, with both equally likely and z is initially 0. Compute the conditional entropies $H(x|z')$ and $H(y|z')$, where z' is the value of z after the statement is executed.

2. (*32 points*) Most operating systems define two types of names. A *direct alias* (name or link) identifies the specific entry in a file allocation table (such as an inode), and an *indirect alias* is itself a file containing the path name of a second file. When one opens an indirect alias for certain actions (such as reading or writing), the operating system instead opens the file named in the indirect alias. Specific commands operate on the indirect alias itself (as opposed to the file it names).

   (a) Can indirect aliases ever loop; that is, can there exist a chain of indirect aliases $i_1, \ldots, i_n$ such that $i_1 = i_n$? If so, how would the system detect such loops? What should it do when one is discovered?

   (b) Can a loop with direct aliases occur?

   (c) The text points out the difference between a file name and a file descriptor. How does the introduction indirect aliases complicate the resolution of an alias to a device number and inode?

   (d) On some systems, a direct alias cannot refer to an inode on a different device. Suppose the system were altered to allow a device number to be included in the alias, so a direct alias could refer to a file on another device. What complications might arise? Do indirect aliases, which can reference files on other devices, have the same complications?

3. (*20 points*) What problems might the failure to quantify the levels of trust in an OpenPGP certificate pose?

4. (*24 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, and that the recipient does not know the sender.

   (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?

Extra credit

1. (*20 points*) Prove that we can 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 17.3.2.4).