Homework 1

Due Date: January 24, 2008 **Total Points:** 100

Problems

1. (*10* points*)* text, §1.12, exercise 3: The aphorism "security through obscurity" suggests that hiding information provides some level of security. Give an example of a situation in which hiding information does not add appreciably to the security of a system. Then give an example of a situation in which it does.
2. (*50 points*) [Bi07a], exercise 16. Please modify the source code posted on the web page. Be sure you submit the *complete* library, so we can compile the library with our test driver. Don't change the name of the files, because our test script will compile our test driver and your library. Of course, apply all the principles of robust programming to your code.
3. (*20 points)* text, §13.6, exercise 3: Kernighan and Plauger argue a minimalist philosophy of tool building. Their thesis is that each program should perform exactly one task, and more complex programs should be formed by combining simpler programs. Discuss how this philosophy fits in with the principle of economy of mechanism. In particular, how does the advantage of the simplicity of each component of a software system offset the disadvantage of a multiplicity of interfaces among the various components?
4. (*20* points*)* text, §25.10, exercise 11: Consider the "counterworm" in the example on that begins on page 764.
    a. Pretend you are a technical expert called as a witness in a lawsuit between the sender of the "counterworm" and the target. What arguments could you make for and against the sending of the worm?
    b. How might the arguments for a company providing "worms" to fix security problems in their software differ from those for providing a "counterworm"? How would they be the same?

Extra Credit Problems

5. (*10 points*) text, §1.12, exercise 19: Argue for or against the following proposition. Ciphers that the government cannot cryptanalyze should be outlawed. How would your argument change if such ciphers could be used provided that the users registered the keys with the government?
6. (*10 points*) text, §13.6, exercise 5: A company publishes the design of its security software product in a manual that accompanies the executable software.
    a. In what ways does this satisfy the principle of open design? In what ways does it not?
    b. Given that the design is known, what advantages does keeping the source code unavailable give the company and those who purchase the software? What disadvantages does it cause?