IS2935/TEL 2810 Introduction to Computer Security
Homework 6
Due Date: November 8, 2006
(100 Points)

1. Problem 9.8.11 [**20**]

2. Problem 9.8.13 (For *n*-1 case, you could use induction and the properties of modular arithmetic) [**30**]

3. Java Programming language [**50**]

   Write a program to encipher and decipher a Caesar cipher. Use your code to answer problem 9.8.2.

   Next exercise will be similar to the previous year's Java homework – so this assignment should be used to brush up your Java. If you have difficulties I will arrange a Java review session with the GSA.

The following property of modular arithmetic will be helpful in solving some problems

- $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
- $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
- $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$
- $(-1) \bmod n = n - 1$ (Using $b = q.n + r$, with $b = -1$, $q = -1$ and $r = n-1$)

Some basic information for Java Programming

If you prefer, you can also use Java on your own PC but you will need to download and install Java Software Development Kit yourself.

Java is an object-oriented programming language. This means that you create classes of objects. In Java, the name of a source file must match the name of the public class defined and implemented in that file. So a class named ProtectedServer must be defined and implemented inside a file named ProtectedServer.java.

All Java source code files end with .java extension. To compile a source file named ProtectedServer.java, type the following at the command prompt:

```
javac ProtectedServer.java
```

If you have multiple source files in your project, you can compile all of them at once by typing:

```
javac *.java
```

The compilation produces files with .class extension. The number of files produced is the same as the number of classes that you have. The entry point of a Java program is the *main* function, which is defined in one of the source files. So if your *main* function is defined inside the ProtectedServer class in ProtectedServer.java file, you can execute your program by typing:

```
java ProtectedServer
```

Note that you only specify the class name, without the .class extension.

You will need to consult Java API documentation to learn how to use java classes. You can download and install the documentation yourself, or you can access them from this URL:

http://java.sun.com/j2se/1.4.2/docs/api/index.html

Here is a java tutorial by Dr. Mike Spring:
http://www.sis.pitt.edu/~mbsclass/tutorial/mbs/Java_Short_Course.html

If you search the web, you should be able to find several nice Java tutorials.