IS2150/TEL 2810 Introduction to Computer Security
Homework 4
Due Date: Oct 30, 2006
(100 Points)

1. Problem 8.7.10 [**15**]

2. Problem 8.7.12 [**15**] (Hint: For *n*-1 case, use induction and the properties of modular arithmetic).

3. Problem 8.7.17 [**15**]

4. Java Programming language [**20 + 35**]

   a. Write a program to encipher and decipher a Caesar cipher. Use your code to answer problem 8.7.2.

   b. Write a program to demonstrate the encryption and decryption using **DES** and a **SHA** scheme using two classes – **MessageDigest** class and **Cipher** class. *Some* of the other important classes you will need to refer to are **Key**, **KeyGenerator**, **SecureRandom, bytes, String.**

   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