CSU200 Discrete Structures	Eric Miles
Spring 2009	February 11, 2009

Written Homework 02

Assigned: Wed 11 Feb 2009
Due: Thu 19 Feb 2009

Instructions:

- The assignment is due at the *beginning* of class on the due date specified. Late assignments will be penalized 50%, as stated in the course information sheet. Late assignments *will not be accepted* after the solutions have been distributed.
- We expect that you will study with friends and often work out problem solutions together, but *you must write up your own solutions, in your own words*. Cheating will not be tolerated. Professors, TAs, and peer tutors will be available to answer questions but will not do your homework for you. One of our course goals is to teach you how to think on your own.
- We expect your homework to be neat, organized, legible, and *stapled*. If your handwriting is unreadable, please type. We will *not* accept pages that are ripped from a spiral notebook. Please use 8.5in by 11in loose-leaf or printer paper.

Problem 1 [30 pts; (4,9,10,4,3)]: Linear ciphers.

A spy has been captured, but all attempts to interrogate him have failed; he speaks a language, unintelligible to any of the translators. However, this spy was caught with a number of documents. Linguists who have studied these documents believe that they were written in the spy's language, but that they have been encrypted. Decrypting these documents to obtain valid text in the spy's language would be incredibly helpful; your job is to decrypt the spy's documents and hopefully determine where he's from and what language he speaks.

The spy's language uses the familiar 26 English letters, which are encoded using the numbers $\{0, \ldots, 25\}$ in the usual way. You suspect that the spy has used a linear encryption scheme with $m = 15$ and $k = 11$ since symbols representing these values were found tattooed on the spy's scalp. As mentioned, the linguists and interrogators are particularly interested in the encrypted pass phrase, given below:

lu entyet uttgk jty

i. Encode each letter in the above phrase in the usual way, i.e., a $\rightarrow$ 0, b $\rightarrow$ 1, and so on.

ii. Since you suspect that these values were encrypted using the function

$$num \rightarrow (15 \cdot num + 11) \bmod 26$$

you must subtract 11 and then multiply by the multiplicative inverse of 15 (mod 26) in order to decrypt these values. Start by determining the multiplicative inverse of 15 (mod 26).

iii. Decrypt each value by inverting the linear encryption.

iv. Decode these values in the usual way to obtain a phrase in the spy's language. (It will *not* be intelligible to most people.)

v. Conduct some research on the web to see if you can determine what this phrase means. (Try typing the decrypted words or the entire phrase into Google.) What is the English translation of this phrase? Where does our spy come from, and what language does he speak?

Problem 2 [20 pts]**: The RSA cryptosystem.**

You have just successfully deciphered a collection of important documents in a strange language, thanks to a mastery of modular arithmetic, and are enjoying a well-deserved vacation in the Caribbean. Alas, your reverie on the beach is short-lived and you are called to decipher what appears to be an even more important message. This is a message sent by one of the spies in your own unit, who is suspected of being a mole (foreign agent). This message has been encrypted using the RSA cryptosystem.

You are told that in the RSA system being used, $n = 119$, and the public key exponent $e = 35$. You suspect that the message being exchanged is in English, using the standard encoding of letters to the numbers from 0 to 25.

Thus, for instance, the message "DOG" will be encrypted as follows. The letter D corresponds to 3, and 3^{35} mod 119 equals 61. The letter O corresponds to 14, and 14^{35} mod 119 equals 7. The letter G corresponds to 6, and 6^{35} mod 119 equals 97. So the message "DOG", when encrypted, reads as follows.

61 7 97

The message that you need to decrypt reads as follows.

25 105 30 25 82 45 0 59 30

Decrypt the above message. Show *all* your work. What is the private key of this RSA cryptosystem?

Problem 3 [25 pts; (5,15,5)]**: Mod Multiplication Patterns.**

i. List all natural numbers less than 25 that are relatively prime to 25 (i.e., do not share a common factor with 25).

ii. Construct the multiplication table mod 25 for only the numbers that you obtained in your solution for part (i). That is, the row headers and the column headers of the table should include precisely the numbers you obtained in your solution for part (i).

iii. Discuss any patterns you see in the multiplication table and why they occur.

Problem 4 [25 pts; (6,6,6,7)]**: GCD and LCM Computations**

Compute the following. Show *all* of your work.

i. GCD$(506, 374)$ using Euclid's algorithm.

ii. GCD$(1575, 495)$ using prime factorization.

iii. GCD$(639, 93)$ using Euclid's algorithm.

iv. LCM$(63, 420)$ by first computing the gcd using Euclid's algorithm.