Week Two

Max Olivier

March 6, 2009

Readings
For this week please read pages 81-96 in Chapter 4 (up until recursive functions), and the pages 111-117 in Chapter 5 (until example 5.2) of Overland. Also please read pages 27-34 in Lewand's *Cryptological Mathematics*, and pages 1-12 (until section 1.1.4) and pages 18-20 (section 1.1.6) in Stinson's *Cryptography: Theory and Practice.* The two readings cover the simple ciphers that we will be spending a lot of time with this term. There are also a lot of other ciphers talked about in the books that we will not do much with, but that you should feel free to learn about and even code them if you so wish. Remember to that the first 27 pages of Lewand are a review of some of the math necessary if you feel you need/want a review.

Main Ideas

- The goals of this are twofold. First, to get familiarize you with the cryptography part of the cryptology that we will be studying this term. The second is to introduce you to C++ functions, which, along with the things you covered last week, will be the building blocks of every program you write in C++. The reading in chapter 5 also covers the basics of arays. So, hopefully by the end of the week you should know:
- How the additive, multiplicative, and affine ciphers work.
- The syntax, structure, and use of functions in C++.
- How to declare and access arrays.

Exercise 1 (Exercises from the Reading)
All the exercises from the reading, including those on page 117.

Exercise 2 (Cryptology Program)
Note: don't attempt to write this program until after you have done all the reading, otherwise it will no make any sense! If you have not done the reading yet, go do it and then come back to this.

The first step is to look at the program cipher_skeleton.cpp. You will see that it contains several functions, including a main function, but they are all either blank or not complete. Now, using what the comments say the functions should be doing as a guide, write and test the necessary code for each of the functions in a program called cipher_functions.cpp,. As always, there is a sample solution on the Week 2 page.