Syllabus: C++ and Cryptology

Max Olivier

March 16, 2009

Introduction

Welcome to C++ and Cryptology! This is a 1 credit independent study course designed to introduce you to programming in C++ and basic notions of cryptology. I'm guessing if you are taking this course that you are already familiar with either C++, cryptology or both. If not, visit:
http://en.wikipedia.org/wiki/C%2B%2B
and http://en.wikipedia.org/wiki/Cryptology
for brief introductions on both.

Course Structure

The course is divided into 8 weekly modules and a final project. Each week has a set of assigned readings, a brief summary of keys points to take from those readings, and a list of programs to write. The course is designed so that work for each week should take between two and two and a half hours. The programs are divided into exercises from the reading and other assignments that I have written and hope will help reinforce both the C++ and cryptology you are learning. Solutions that I have written to all the book exercises and other assignments are linked on the course webpage, and the authors solutions to the book exercises are provided on the CD accompanying the book. I have tried to comment my solutions as much as possible to be clear about what the code is/should be doing, so my apologies if it sometimes seems like there are far too many comments. Also note that the solutions to the book exercises on the course website password protected, so you will need a Carleton ID and password to access them.

Final Project

This course is graded on a S/Cr/NC basis, and your grade will be entirely determined by the final project. For this course, the final project comes in three stages, and at each stage there will be one or two programs to write and hand in. Naturally solutions to these programs are not provided.

The Books

The C++ text for this course will be *C++ Without Fear: A Beginners Guide That Makes You Feel Smart* by Brian Overland (Prentice Hall 2004, ISBN 978-0321246950). It gives a very good introduction to C++, and is worth the $20 it will cost to buy.

There will be two cryptology texts for the course, and since the readings from them will be limited both will be on reserve at the Library. The books are *Cryptological Mathematics* by Robert Lewand and *Cryptography: Theory and Practice* by Douglas Stinson.

Prerequisites

The formal prerequisites for this course are CS 201: Data Structures and CS 202: Mathematics of Computer Science. The reason for the latter prerequisite, is that a background in "elementary" number theory often covered in CS 202 is required to understand the cryptology. If you have not taken CS 202, however, you could learn the necessary background material by reading the first 26 pages of Lewand.

Outline

Of course in a 1 credit course it would be impossible to cover everything C++ can do, but the hope is that by the end of the course you will have enough of a working knowledge of C++ so that with the help of a more advanced C++ book and some effort you can understand and eventually write advanced C++ programs. Similarly, since the course time is brief, we have limited our cryptology study to just simple monoalphabetic substitution ciphers (and no need to worry if you do not know what that means yet, you will soon). Hopefully studying just these ciphers will give some insight into cryptology more generally though. For the specifics covered in each week see the weekly pages, but a broad overview would be as follows:

- **Week 1:** Basics of C++ including arithmetic, conditionals, variables, and loops.
- **Week 2:** Introduction to cryptology, monoalphabetic substitution ciphers, and C++ functions.
- **Week 3:** More on functions as well as arrays and random number generation.
- **Week 4:** Pointers.
- **Week 5:** Strings (both C style and String Class).
- **Week 6:** Introduction to classes and objects.
- **Week 7:** More on classes and objects and more cryptology such as Euclidean algorithm, enriched Euclidean algorithm, and finding multiplicative inverses.
- **Week 8:** Memory management and creating a linked list.