CSE539 Applied Cryptography – Project 1b

Project 1b is the first actual programming project. In this project you will be expected to write the entirety of the code on your own. It should be well commented for grading purposes and follow the good programming standards that you have learned in your programming classes. You may use C or C++, i.e. you are not required to use object oriented programming.

In this project you will use the file that comes with Ubuntu at /usr/share/dict/words. You need to copy this file and sort it so you can perform a binary search on its contents. I leave the binary search methodology to you.

Your program will be designed to perform a cryptanalysis of a reused one-time pad binary cipher-text using a method such as the Crib Drag method that you will research yourself (easily found on the internet). This means that you should have two or more cipher-texts as inputs to your program. You need to test your program by writing a second program to create a one-time pad and generate the two or more cipher-texts from two or more messages (the more cipher-texts the quicker decoding can take place). Your program will be graded based on its clarity and success at recovering messages during the grading process. You are required to compose your messages using only the words found in the above named words file as well as ' ', '.', '?', '!', and '\n'.

Input file names include ~/words, ~/cipher000, and ~/cipher001 and so on. Output files should be named ~/pad, ~/msg000, and ~/msg001 and so on. Programs must decode at least 2 files at once and as many as 4. These file names are standardized to facilitate grading.

The completed project should be a C++ project composed and executed in QT Creator on Ubuntu. Zip the project and submit it to the Blackboard by the due date. If it is a 32 bit project you must make note of it in your submission. All projects will be assumed to be 64 bit programs unless otherwise noted.

If your program is inefficient compared to the norm you will lose grade points, make a little effort.

You should discuss your strategies on the Blackboard but do your own work. Copied code with minor changes will be considered plagiarism.

Write a report indicating the methods used and the sources for your algorithms as well as your understanding of the one-time pad cipher.