

## CS150 Assignment 6 Basic Cryptography

**Date:** Wednesday, November 15, 2006

**Date Due:** Friday, December 1, 2006

**Total Points:** 60 pts

A cryptogram is a coded message formed by substituting a code character for each letter of an original message. The substitution is performed uniformly throughout the original message. In order to break this code, you must first learn how the message was coded.

This cryptogram formula revolves around a code key, which will be the first piece of character data entered by the user.

### Example:

Suppose the code key was **b**. If we take a look at our normal alphabet and the new alphabet produced by the code key, things will become clear.

```
old:  abcdefghijklmnopqrstuvwxyz
new:  bcdefghijklmnopqrstuvwxyz
```

Notice: The new alphabet begins with the code key and then wrap around occurs at the end.

Suppose we wanted to send a secret message to a friend. This particular message consists of the word **today** and the code key is **b**. Then **today** encoded would become **upez** since **t** in the old corresponds to **u** in the new, **o** to **p**, and so on.

This assignment is to write a program that allows the user the ability to enter an E (or e) for encode or a D (or d) for Decode followed by the name of two files. Here is an example of how your program is to work:

```
*****
*                               Secret Message                               *
*****
```

```
Enter (E for encode or D for decode): E
```

```
Enter the name of the file you wish to encode: message.dat
```

```
Enter the name of the file where the decoded message will be stored:
secret.dat
```

```
Your message has been encoded
```

If you are decoding a message, then your output should be:

```
*****  
*                               Secret Message                               *  
*****
```

Enter (E for encode or D for decode): D

Enter the name of the file you wish to decoded: secret.dat

Enter the name of the file where the decoded message will be stored:  
decoded.dat

The secret message has been decoded

The data file will be organized as follows:

- 1) The first line of the data file will contain a single character that will be the code key. This character will be any single character from 'a' to 'z' (notice that it's in lower case).
- 2) The rest of the data file will contain the coded or regular message that you must decode or code using the code key.

Your program must:

- 1) Work for any arbitrary code and message using the pattern described above.
- 2) Only alphabetic characters are to be decoded--any other characters are to be left as is and outputted. This includes any punctuation, spaces, returns, etc.
- 3) There are both lower and uppercase alphabetic characters in the file. You must be able to decode both and output the decoded character in the same case.

You are to use an array to help you decode your message. This array will help you easily determine how to decode your character based on its placement in the alphabet.

### ***To complete this assignment you must***

1. Create a new C++ project in Visual Studio. Name your project "06CryptoBasicxxxxxxx", where xxxxxxxx should be replaced by your PU Net Id. As an example, my project would be called "06CryptoBasickhoj0332". It is vital that you name your project correctly!
2. Type the solution (fully documented/commented) to the problem into your project.
3. Make sure that your program compiles and runs correctly. If you get any errors, double check that you typed everything correctly. Be aware that C++ is case-sensitive.
4. Don't forget to use the debugger!!
5. Once you are sure that the program works correctly it is time to submit your program. You do this by logging on to Turing and placing your complete project folder in the CS150-01 drop folder. Make sure that you copy your program folder and don't move it. If you move it, then you will not have your own copy!

6. You must submit a stapled, hard copy of your program. You must also submit a hard copy of the decoded files for the test cases that we will provide you with next week.

## **Notes**

1. You must follow the coding standards.
2. You must check that the files opened correctly. If not, then you should exit the program.
3. You must use constants when possible.
4. You must use functions to break up your program appropriately.
5. Your program will be graded on efficiency. In other words, you will be marked down for repeating code statements unnecessarily.
6. You may only use the C++ programming concepts covered thus far in class. Do not use any more advanced concepts that we have not covered or any other programming concepts that you have had experience with.
7. Your output must look exactly like the sample given.
8. You must comment your code appropriately.
9. Refer to the syllabus for what constitutes plagiarism, and the consequences for plagiarizing.

To receive full credit for this assignment, your project must be in the drop box by 1pm on the day that it is due. Anything later will be considered late. Further, you must bring a hard copy of your program to class and place it on the instructor's desk by 1pm.

**Good luck! And remember, if you have any problems, come and see me straight away.**

**START EARLY!!**