

## CS150 Assignment 6 Complex Cryptography

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

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

**Total Points:** 60 pts

+ 10 pts extra credit if your program correctly  
decodes the secret message we give you

For this assignment, you are to use an encryption algorithm to encode and decode files. Your program should allow the user to select one of the two options (encode or decode) and input the names of the input and output file. Your program should then either encode a plain text file, or decode an encrypted file.

The algorithm you will use is a monalphabetic encryption algorithm. The algorithm encrypts on letter pairs.

A two dimensional 5 x 5 array can be used to represent all 26 letters of the alphabet if I/J are combined into one spot. Using an encryption phrase such as CARPENTERS SQUARE, the array would look like the one below, where the phrase is inserted into the array (no letters repeated) followed by the remaining letters of the alphabet (no letters repeated).

C	A	R	P	E
N	T	S	Q	U
B	D	F	G	H
I/J	K	L	M	O
V	W	X	Y	Z

The plain text letters in the message should be paired up and one of the following four options will work:

1. The two letters are in the same row. For each letter advance in the row to the next letter allowing it to wrap around when the end of the row is reached. For example if the two letters were TU it would be encrypted to SN.
2. The two letters are in the same column. For each letter advance in the column to the next letter allowing it to wrap around when the end of the column is reached. For example if the two letters were GY the encrypted text would be MP.
3. The two letters are in different columns and different rows. Advance in the plaintext's first letter's row until the plaintext's second letter's column is reached and make that the first encrypted letter. Go to the row of the plaintext's second letter and move in this row to the column of the plaintext's first letter and make that letter the second encrypted letter. For example if the letters are SH then the encrypted letters would be UF.

4. The two letters are the same. If this occurs, advance in the row one letter, wrapping if necessary to obtain both encrypted letters.
5. The last possibility is that the second letter is a whitespace, in which case substitute the first letter by advancing in the row one letter.

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

Inputs: A file that contains the encryption phrase on one line followed by the text to be encoded or decoded

Outputs: A file containing the encryption phrase on one line followed by the encoded or decoded text

Note: Your program should replace all j's with i's when decrypting. The text will still be readable

This program is more difficult than previous assignments. Don't waste a week or you might not be able to finish! Also, when writing this program you should build and test as you code. For example, after you have written the function to find identifiers, test it on a sample file then move on.

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

1. Create a new C++ project in Visual Studio. Name your project "06CryptoComplexxxxxxxxx", where xxxxxxxx should be replaced by your PU Net Id. As an example, my project would be called "06CryptoComplexkhaj0332". 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!!**