CS150 Assignment 6
Basic Cryptography

Date Due: Friday, November 30, 2007
Total Points: 60

Cryptography is an exciting area of Computer Science concerned with hiding and protecting information. This is the branch of Computer Science that allows you to send your credit card details securely to a web site or a spy to communicate secretly with her colleagues.

For this project, you will be building a program that will take a plain text file and produce an encrypted file (or vice versa). The encryption scheme you need to implement is inspired by the Enigma Machine, a German encryption machine from WWII (http://en.wikipedia.org/wiki/Enigma_machine).

Encryption Scheme:

Simple substitution

A simple substitution cipher (sometimes called a Caesar cipher) maps each letter of the alphabet to another letter of the alphabet as shown below:

Input

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

Output

To encrypt a letter, find the letter on the top and use the letter below it as the encrypted output. Using the above table, the encrypted output for C would be Z. To decrypt a letter, find the letter on the bottom and use the letter above it as the decrypted output.

To make things more interesting, a secret key is used to specify how the input characters are mapped to output characters. The key, which is a single character, specifies which letter the output row starts on. The key in the above example is X. (The input row always starts with A).

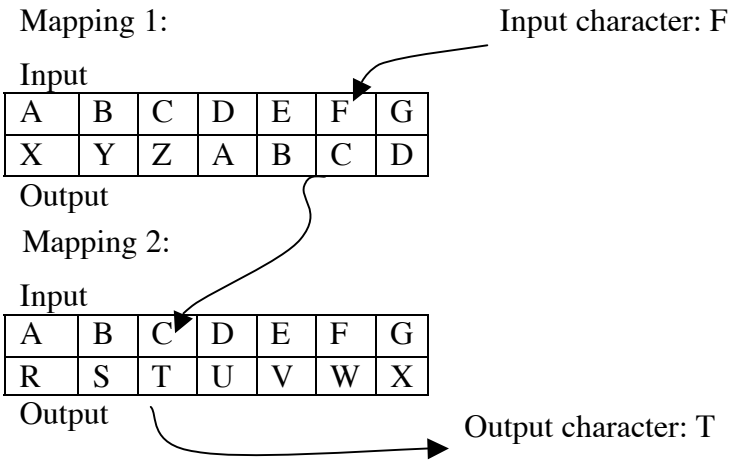
Double Substitution with a Twist!

You will need to implement a double substitution (with a twist) encryption scheme. This means you will have two substitution mappings. The character to be encrypted will be used as the input to the first mapping; the output of the first mapping will be the input to the second mapping. The output of the second mapping will be the encrypted character.

After each character is encrypted, the output characters in the first mapping are twisted to the left one space. Once the first mapping has made one full revolution (26 twists), the second mapping makes one twist to the left as well (on this occasion, both mappings twist one to the left).

Each mapping has its own key, so you will have a total of two secret keys for this scheme.

An example is show below.



After this encryption the new mappings (after the twist) will look like the following. Note that in this case only the first mapping has twisted.

Mapping 1:

Input

A	B	C	D	E	F	G
Y	**Z**	**A**	**B**	**C**	**D**	**E**

Output

Mapping 2:

Input

A	B	C	D	E	F	G
R	S	T	U	V	W	X

Output

For this assignment, you need to allow the user to encrypt or decrypt as many files as they want. The user will need to specify the two keys and the input and output files.

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

Enter (E for encrypt or D for decrypt): E

Enter the two keys: P U
Enter the name of the input file: message.dat
Enter the name of the output file: secret.dat

Your message has been encrypted!

Would you like to encrypt or decrypt another file? N
```

☐You are to use arrays to help you encrypt and decrypt your message.

☐Be sure to validate all input. Continue asking for input until valid input is given. The secret keys *must* be uppercase letters

☐You *must* have at least three functions, other than main, in your program.

☐Only upper case alphabetic characters are to be encrypted and decrypted--any other characters are to be left as is and outputted. This includes any punctuation, spaces, returns, etc.

☐ Sample input and output files will be provided on Wednesday, November 14.

☐You need to encrypt your favorite joke (keep it clean!) and email the encrypted message to me by 1pm the day the project is due. In the subject line of the email, specify the two secret keys.

What will your program need to do conditionally? What data will this decision be based on?

_____

_____

_____

_____

What data will need to be stored in an array?

_____

_____

_____

_____

_____

What will your program need to do in a loop? When data will your program use to stop the loop?

_____

_____

_____

_____

_____

_____

To complete this assignment you must

1. Create a new C++ project in Visual Studio. Name your project "06Cryptoxxxxxxx", where xxxxxxxx should be replaced by your PU Net Id. As an example, my project would be called "06Cryptokhoj0332". 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. 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!
5. You must submit a stapled, hard copy of your program.

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 and the answers to the above question to class and place it on the instructor's desk by 1pm. Don't forget to email me the encrypted joke!

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

START EARLY!!