**CS211 -- Assignment 1**

Write a complete program that performs encryption/decryption of a text file. Encryption means you need to scramble the words of a file to become secure. Decryption means you need to apply some rules to an encrypted file in order to find the original file with its original content. An example of encryption is to replace each letter in a file with its consecutive letter in the alphabet. Therefore, ‘a’ is replaced by ‘b’, ‘b’ is replaced by ‘c’ and so on and finally ‘z’ is replaced by ‘a’. Thus, if the file contains the following message:

***I am a student at csusm***

The encrypted message becomes:

***J bn b tuvefou bu dtvtn***

Then if you get this encrypted message and the key is 1, it means you need to shift the alphabets in the decrypted message by 1 to the left to get the original message back.

This method is called “rot1” indicating that every alphabet rotates by 1 during the encryption. Similarly, rot10 means every alphabet should be rotated by 10 during encryption.

Another method of encryption is to create cryptogram. A cryptogram is a message or word where each letter is replaced with another letter. For example, the string:

***The birds name was squawk***

might be scrambled to form

***xms kbypo zhqs fho obrhfu***

Note that space or any punctuation is not scrambled. In this particular case, ‘T’ was replaced with ’x’, each ‘a’ was replaced with ‘h’. etc. We assume there is no difference between lower case or uppercase.

Your job is to write a program that performs different types of encryption or description. First, you need to ask the user to see if the user wants to do encryption or decryption. If the user wants to do encryption, you should find out if the user wants to use “rot” method or cryptogram method. If the user selects the “rot” method, you need to ask for the encryption key. For example, entering 15, means that the user wants to use “rot15” method to do encryption. If the user selects the cryptogram method, you should open the cryptogram text file where the cryptogram string is stored. The cryptogram string should contain a string of 26 letters where the first letter corresponds to letter ‘a’, the second letter corresponds to letter ‘b’ and so on. For example, your cryptogram file may contain the following message.

***wyijkcuvdpqlzhtgabmxefonrs***

which means ‘w’ corresponds to ‘a’, ‘y’ corresponds to ‘b’ and … and finally ‘s’ corresponds to ‘z’.

The same procedure should be followed for decryption. You need to ask the user which method the user wants to use (rot or cryptogram) for encryption. Then write the routines that takes an encrypted file and does the decryption to get the original file back.

You are responsible to user string and vector class in this program. For encryption, you need to read the file to be encrypted into a vector of string and place the words (one word per element) into a vector. Then read the elements of your vector one by one and do the encryption and place the encrypted word into another vector. Finally write the content of encrypted vector to an output file.

For decryption, you need to do the same process which is read the file that contains the encrypted information and place the encrypted words one by one into a vector. Then create another vector so that as you decrypt the information you can place the decrypted words into another vector. Finally, the vector that contains the decrypted words (original message) should be written to an output file.

Here is a message you can do your test:

The recently approved Academic Blueprint adds new academic programs to the campus and guides planning for physical and curricular support for those programs. The additional programs will enhance the campus service to the region and provide new options and opportunities for students. Criminology and justice studies starts in fall 2003. We are also preparing for four new majors in fall 2004 - physical education and kinesiology, mass media, biochemistry, a master’s in middle-level education and a doctorate in educational administration (in cooperation with SDSU and UCSD).

Place the above message in a text file called “original.txt” and test your program based on the following:

1. Encrypt the original message using “rot13” and call the file encrypt01.txt
2. Encrypt the original message using the following cryptogram and call the file encrypt02.txt

***wyijkcuvdpqlzhtgabmxefonrs***

1. Decrypt “encrypt01.txt” file using “rot13” (shifting every alphabet to the left 13 places and call it “decrypt01.txt”
2. Decrypt “encrypt02.txt” file using the above cryptogram and call it “decrypt02.txt”

Your “decrypt01.txt” and “decrypt02.txt” should be identical to your original file you used for encryption.

What to hand in:

1. Submit the hard copy (***print out of the program and print out of all of the required outputs***) within the first 10 minutes of the class on the due date.
2. Place only the source code into a folder (no output), call the folder based on your first name and your last name (ex: JohnSmith-A1), zip the folder and submit it through the COUGAR ACCOUNT.