

CS150 Assignment 7 Basic Cryptography

Date Assigned: Friday, November 9, 2012

Date Due: Monday, November 19, 2012

Total Points: 40 pts

Cryptography is an exciting area of Computer Science concerned with hiding and protecting information. This is a branch of Computer Science that allows you to send your credit card 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 outline of the program is available in the CS 150 Public folder on Turing. The file is called: cryptography.cpp

Encryption Scheme:

Encryption methods have historically been divided into two categories: substitution ciphers and transposition ciphers. This encryption algorithm deals with a substitution cipher revolving around a code key which the user must know. With a substitution cipher, each letter or group of letters is replaced by another letter, group of letters, or numbers to disguise the message. Consider the following text to be encoded and a code key of: TRIGRAMS

```
codekey:   TRIGRAMSTRIGRAMSTRI
plaintext: ENCODE THIS MESSAGE
```

If we take the ASCII values of the code key in each of the positions and add (unsigned) the plain text ASCII values in each corresponding position we would have the following:

```
codekey:    84  82  73  71  82  65...
plaintext: + 69  78  67  79  68  69...
ciphertext: 153 160 140 150 150 134
```

Notice that E encoded the first time is 153 and E encoded the second time is 134. This is important because we do not want the intruder to see patterns of characters to help them break the code. To get the message decoded, simply reverse the process as follows:

```
ciphertext: 153 160 140 150 150 134
codekey:    - 84  82  73  71  82  65
plaintext:   69  78  67  79  68  69
```

For this assignment, you need to allow the user to encrypt or decrypt as many files as they want.

Run #1



```
C:\Windows\system32\cmd.exe
*****
*   Cryptography   *
*****

E)ncode Message
D)ecode Message
Q)uit

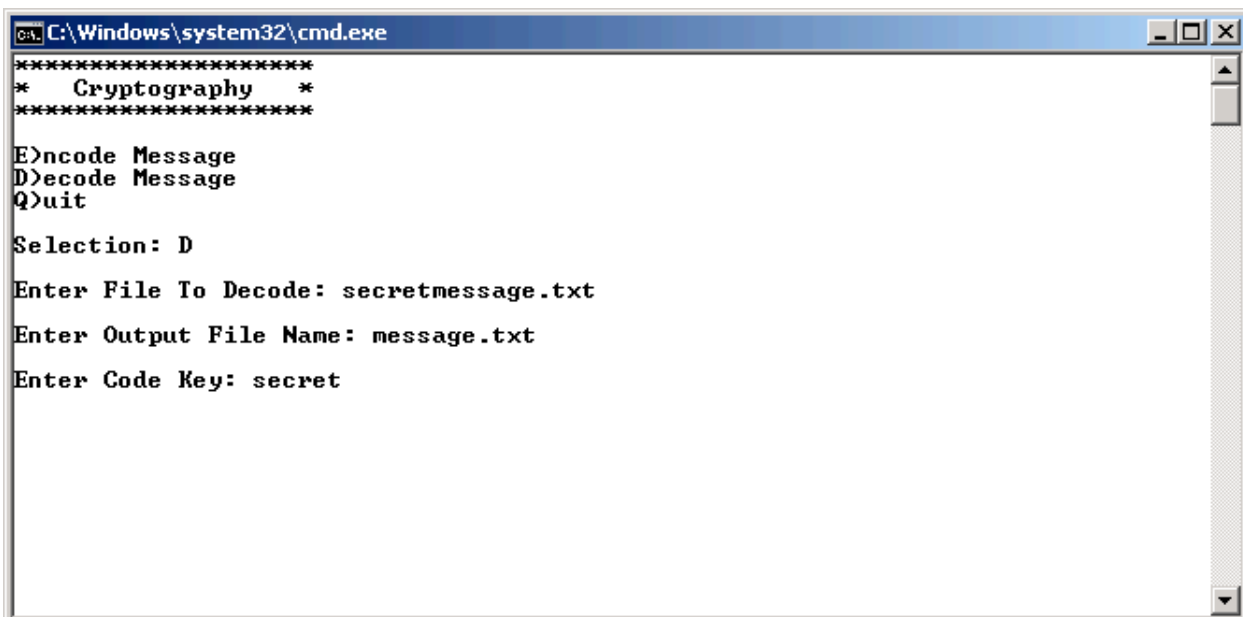
Selection: E

Enter File To Encode: message.txt

Enter Output File Name: secretmessage.txt

Enter Code Key: secret
```

Run #2



```
C:\Windows\system32\cmd.exe
*****
*   Cryptography   *
*****

E)ncode Message
D)ecode Message
Q)uit

Selection: D

Enter File To Decode: secretmessage.txt

Enter Output File Name: message.txt

Enter Code Key: secret
```

► You are to use arrays in your program to help you encrypt and decrypt your message. You cannot use string variables at all in your solution. You can use string literals when needed.

► Be sure to validate all input. Continue asking for input until valid input is given. The user will enter a secret key that is all one word with no whitespace but you don't have to error check the secret key.

► A partial program exists called `cryptography.cpp` with function prototypes. You are to write the definition for each function prototype.

► An encrypted file **secretCS15002F12.txt** will be provided by Wednesday, November 14. You can test that your program decodes correctly on this file.

► You need to encrypt your favorite joke in a file called **joke.txt** which is placed in your Resources folder. **You must include the code key as a comment at the top of your solution, below the description of your project.**

To complete this assignment you must submit the following:

1. An electronic copy of your program on Turing

a. Add a new project named **07_Cryptography** to your previously created assignment solution called **PUNetID-Assignments**. It is vital that you name your project correctly!

b. Type your program (fully documented/commented) into the project. You must follow the coding standards!

c. Pay attention to the example output! Your program's output must look **exactly** like the example output! The spacing and newlines in your output must match exactly.

d. Make sure that your program compiles and runs correctly. If you get any errors, double check that you typed everything correctly.

e. Make sure that your program does not produce any warnings.

f. 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 solution folder in the **CS150-01** Drop folder. This solution folder must contain seven projects.

g. The program must be in the drop folder by 9:15am on the day that it is due. Anything submitted after that will be considered late.

2. A hard copy of your program

a. The hard copy must be placed on the instructor's desk by 1pm on the day that it is due.

b. The hard copy must be printed in color, double-sided, and stapled if necessary.

c. Your tab size must be set to 2 and you must not go past column 80 in your output.

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