Programming Assignment #1

Vigenere Cipher in CBC Mode
CIS 3360, Spring 2018

Contents

i. Source Code Files: **encipher.c** and **decipher.c**
ii. Executables: **encipher.exe** and **decipher.exe**
iii. Sample Text File: **input.txt**
iv. Assignment Report (Program Instruction)
v. Expected Program Output Screenshots

Developer: Zach Newsom

iv. Assignment Report (Program Instruction)

Both **encipher.c** and **decipher.c** were written so as to adhere to the original instructions outlined in Webcourses under 'Programming Assignment 1: Encryption and Decryption using Vigener with Cipher Block Chaining (CBC).'

At the command prompt, ensure you have all necessary source, executable and text files required to execute the encipher and decipher programs (all files are contained in the zip folder submission). At runtime, you should have in your current directory:

1. Source files encipher.c and decipher.c
2. The provided sample text file, input.txt, or a text file of your choosing (less than 4 kb)

You may also include both executable files in your current directory (this may not be necessary if you plan to compile the source files on your system and generate your own executables). Should you decide to compile and produce your own .exe files, your terminal prompt should look something like this:

```
za978545@net1547:~$ gcc -o encipher encipher.c
```

After compilation you may run the program by typing the following command at your terminal window:

```
za978545@net1547:~$ ./encipher input.txt dark rock
```

Note: You must enter **four** arguments at the terminal to run the program properly.

Argument 1: In the above screenshot I've used the name of the encipher.exe file provided with this submission. This argument may differ if you choose to compile and name your own executable file ('a.out' is the default name if you compile without the '-o' flag).

Argument 2: The second argument should be the name of your input text file residing in your current directory at runtime. In the example above I've used 'input.txt' but this may vary depending on the name of your file (be sure to include the file extension e.g. .txt).

Argument 3: This argument should be a short word between **two** and **ten** characters inclusive and in all lowercase. We refer to this word as the 'key.' Mimicking the assignment instructions, I've used the word 'dark' here.

Argument 4: The final argument is the Initialization Vector (IV). This argument should be equal in length to the key and preferrably a different word altogether. This word will be used to encipher the first block of plaintext in the program.

v. Expected Program Output

./encipher

Using the instructions provided above and the included input text file, the encipher program should deliver two forms of output

1. **stdout**: The requisite data outlined in the instructional video will be printed to your terminal window. This includes the plaintext from the input text file after having been processed and stripped down, among other information pertinent to the programs functionality (character count, padding characters added, etc.).
2. **.txt files:** encipher will create 2 new text (.txt) files named: **plain.txt** and **cipher.txt.** The plain.txt file is the result of the pre-processing function within the encipher program. This pre-processing function removes all special characters including spaces and converts all characters to lowercase. The cipher.txt file, of course, contains the pre-processed plaintext converted to ciphertext. The ciphertext file will serve as input for…

./decipher

Similarly, this program produces output to both stdout and a text file. Output to stdout includes the ciphertext passed into the program and the corresponding plaintext afterwards; in addition to some key data points. File output is simply the plaintext converted from ciphertext.

Turn the page for some super excellent screenshots…

Output Screenshots

```
[za978545@net1547:~$ ./encipher input.txt dark rock                                ]
 ==================================
*           ./encipher             *
 ==================================
Input file: input.txt
Key: dark
IV: rock
Block size: 4

Plaintext (after preprocessing):
myfirstloversmelledofindianacigarettesdustandcheapleathertheoneafterhimkentuckybourbona
ndbrokenhorsesandthelastahintoffloridacitrussaltandspringbreakandadashoftexasbarbequehe
attheydontcommentonmyhundredsorunshavedlegsonlyyourskinmakesyouworthitastheypassthemone
ytenderlyipackitawaybeneathbrokenfloorboardsandgazeoverholesinthewallstheypayleavecallt
othesnowoutsideprayaboveforanotherpaycheckiwelcomethenextonenewyorklemonandabible

# of plaintext characters (before padding): 429

Ciphertext:
gmycaeixrzdymlytapsrixwetxaoyfxysjhbzbbfuuscawqqdlsegeqsaxogrkjqzderjlhlqyrpvigamcoldpf
ijqngwurxnlalileyeszthkjdrsngixjbzoiocqhrwkqtzvadpyjcjgnsnxicaxmpdadrnozuulqwylyhfbjvpf
aylmvgrazjwocfdbmdtnbuqavvxdetrxivbxujhipzcwtuduyyxmzqnyqkuqfirmkjntjmqltdxjznsbjeznobg
lypwotqkmspnothjogrkpborplfvgqzctmuthufkhcsfhgfohwtfcrupqtikyxluckvintysrixvpklykfxbvha
sofonbkuevuwpypvjyefnmqtvaydloiusfoethmsyrlyfcewugonbtjuxhninlaqecbllogiobassjsnzggu

Ciphertext file: ciphered.txt
# of padding characters: 3
```

```
[za978545@net1547:~$ ./decipher cipher.txt dark rock                               ]
 ==================================
*           ./decipher             *
 ==================================
Input file: cipher.txt
Key: dark
IV: rock
Block size: 4

Cipher Text (input):
gmycaeixrzdymlytapsrixwetxaoyfxysjhbzbbfuuscawqqdlsegeqsaxogrkjqzderjlhlqyrpvigamcoldpf
ijqngwurxnlalileyeszthkjdrsngixjbzoiocqhrwkqtzvadpyjcjgnsnxicaxmpdadrnozuulqwylyhfbjvpf
aylmvgrazjwocfdbmdtnbuqavvxdetrxivbxujhipzcwtuduyyxmzqnyqkuqfirmkjntjmqltdxjznsbjeznobg
lypwotqkmspnothjogrkpborplfvgqzctmuthufkhcsfhgfohwtfcrupqtikyxluckvintysrixvpklykfxbvha
sofonbkuevuwpypvjyefnmqtvaydloiusfoethmsyrlyfcewugonbtjuxhninlaqecbllogiobassjsnzggu

# of plaintext characters (before padding): 432

Plaintext:
myfirstloversmelledofindianacigarettesdustandcheapleathertheoneafterhimkentuckybourbona
ndbrokenhorsesandthelastahintoffloridacitrussaltandspringbreakandadashoftexasbarbequehe
attheydontcommentonmyhundredsorunshavedlegsonlyyourskinmakesyouworthitastheypassthemone
ytenderlyipackitawaybeneathbrokenfloorboardsandgazeoverholesinthewallstheypayleavecallt
othesnowoutsideprayaboveforanotherpaycheckiwelcomethenextonenewyorklemonandabiblexxx

Plaintext file: deciphered.txt
# of padding characters: 4
```

Developer: Zach Newsom