COMP 7402
ASSIGNMENT 2

Rina Hong
A00964022
02/07/2019

Contents

User Guide

- To run program, please install python3.

In terminal:

- Note: Please include file extension if you want to pass a file to encrypt i.e “filename.txt”
- Note: -I argument only accepts ‘s’ for string input type or ‘f’ for filename input type

To encode: total 8 arguments

python3 te.py -i <plainTextInputType s/f> -t <plaintext> -k <keysize> -f <ciphertextfilename>

```
ex)python3 te.py –i f –t "MobyDick.txt" –k 3 –f "cipherMobyDick.txt"
ex) python3 te.py –i s –t "Hi how are you" –k 3 –f "c.txt"
```

To decode: total 4 arguments

python3 td.py -i <inputType s/f> -t <ciphertext>

```
ex) python3 td.py –i f –t "cipherMobyDick.txt"
ex) python3 td.py –i s –t "Hh eoioa u wry"
```

Design

te.py:

- This will encrypt the plain text transposition cipher

main ():

- main() expects 8 arguments -I, input type (s or f), -t, plain text string or file name, -k, key size, -f, ouput file name
- If arguments are correctly entered then encrypt the message and store the result into specified output file name.

encryptMessage ():

- encryptMessage () takes two arguments: key and message.
- Specified key is a number of columns
- Loop through String message (plain text), each element of message will be appended to cipher text array
- Return result as a string.

td.py:

- This will decrypt the transposition cipher text with the every possible key length.

main ():

- main() expects 4 arguments -I, input type (s or f), -t, plain text string or file name.
- If arguments are correctly entered then decrypt the message and call detectEnglish.FindEnglish() to find a match a word in dictionary.

decryptMessage():

- decryptMessage() takes two arguments: key and message.
- With given key and message, decryptMessage() will calculate number of columns and rows.
- Loop through String message (ciphered text), each element of String message will be appended to plaint text String.
- Return result as a string.

Report

Testing and Supporting Data

1) To encrypt the string plain text

```
rinahong@Rinas-MacBook-Pro assign2 $ python3 te.py -i s -t "Hi hello how are you Rina" -k 3
Usage: python3 te.py -i <plainTextInputType s/f> -t <plaintextfilename> -k <keysize> -f <ciphertextfilename>
rinahong@Rinas-MacBook-Pro assign2 $ python3 te.py -i s -t "Hi hello how are you Rina" -k 3 -f "ctext.txt"
```

2) To decrypt the cipher text in file and stop the program when find a match find a match

```
rinahong@Rinas-MacBook-Pro assign2 $ python3 td.py -i f -t "ctext.txt"
keylen:  1
keylen:  2
keylen:  3
Word match found -->  HELLO
Here is your first 50 characters:  HI HELLO HOW ARE YOU RINA
Press enter key to continue the attach or y to stop: y
rinahong@Rinas-MacBook-Pro assign2 $
```

3) To decrypt the same file as 2) but continue attacking

```
rinahong@Rinas-MacBook-Pro assign2 $ python3 td.py -i f -t "ctext.txt"
keylen:  1
keylen:  2
keylen:  3
Word match found -->  HELLO
Here is your first 50 characters:  HI HELLO HOW ARE YOU RINA
Press enter key to continue the attach or y to stop:
keylen:  4
keylen:  5
keylen:  6
keylen:  7
keylen:  8
keylen:  9
keylen:  10
keylen:  11
keylen:  12
keylen:  13
keylen:  14
keylen:  15
keylen:  16
keylen:  17
keylen:  18
keylen:  19
keylen:  20
keylen:  21
keylen:  22
keylen:  23
keylen:  24
keylen:  25
```

Pressed Enter key

4) Encrypt a large file such as MobyDick.txt

```
rinahong@Rinas-MacBook-Pro assign2 $ python3 te.py -i f -t "MobyDick.txt" -k 5 -f "cMobyDick.txt"
```

5) Decrypt a large file as ciphered MobyDick with continue attacking until found a correct key

```
rinahong@Rinas-MacBook-Pro assign2 $ python3 td.py -i f -t "cMobyDick.txt"
keylen:  1
Word match found -->  TEA
Here is your first 50 characters:  EUEBOBCR E ALEIOS UFONR ONTMNST SROYY  WRUTEEM PC
Press enter key to continue the attach or y to stop:
keylen:  2
Word match found -->  USE
Here is your first 50 characters:  R IEHUAESBAOSBIC RO GEI MANLAEYI OOS
 NURF OTNERA
Press enter key to continue the attach or y to stop:
keylen:  3
Word match found -->  RIO
Here is your first 50 characters:  H  DCERWUNNEERBTIOA BHNCOBRIY N E M DIAOLSPEILILTO
Press enter key to continue the attach or y to stop:
keylen:  4
Word match found -->  RAT
Here is your first 50 characters:  YRR II EOHWURA ENSYBCANOYSABIIOCO YR OE AG ENIT  M
Press enter key to continue the attach or y to stop:
keylen:  5
Word match found -->  THE
Here is your first 50 characters:
THE PROJECT GUTENBERG EBOOK OF MOBY DICK OR THE W
Press enter key to continue the attach or y to stop: y
rinahong@Rinas-MacBook-Pro assign2 $
```