COMP 7402
ASSIGNMENT 3

Rina Hong
A00964022
02/14/2019

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 <key> -f <ciphertextfilename>

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

Design

a3.py:

- This will encrypt the plain text with otp and xor with given key

main ():

- main() expects 8 arguments -I, input type (s or f), -t, plain text string or file name.
- If arguments are correctly entered then encrypt the message with otp and xor

getText ():

- getText () takes two arguments: textOption and plainText.
- If textOption is s then return second parameter
- If textOption is f then second parameter is the filename. Read this file and return all texts in the file.

generateRand ():

- generateRand () takes one argument: textLen.
- Passing returned value from getText() to this function.
- Generate random numbers as many as textLen
- Store random number into an array and return this.

getKey():

- This function is written for the case of different length of key and the plain text
- getKey() takes two argument: key and plainTextLen
- Get the division of plainTextLen and length of key
- Get the modulo of plainTextLen and length of key
- Repeat the key for the division value of times.
- Append the substring of key using modulo value and append it to the above value
- This calculated value is the real key to use for xor cipher

ecryptWithOTP():

- ecryptWithOTP() takes 2 arguments: randomNumArr, plainText
- Loop through the randomNumArr and plainText.

- For each letter of plainText, convert it to binary and add randomNum of the same index
- Convert it back to char and store into an array
- Convert this array to string and return.

ecryptWithXOR ():

- ecryptWithXOR () takes 2 arguments: key, otpCipherText
- Loop through the smaller length of the key and plainText.
- For each letter of plaintext and key, convert it to binary and add them.
- Convert it back to char and store into an array
- Convert this array to string and return.

Report

Testing and Supporting Data

1) To encrypt the string plain text

```
rinahong@Rinas-MacBook-Pro rinahong_A3 $ python3 a3.py -i s -t "Money is power" -k hello -f "result.txt"
[92, 50, 71, 98, 51, 76, 88, 100, 80, 80, 77, 41, 81, 69]
otp cipher:  ©¡µÇ¬lÁ×pÀ¼ ¶·
xor cipher:  ÁÄÙ«Ã¤»¯ÔÅÚÛ
rinahong@Rinas-MacBook-Pro rinahong_A3 $
```