Soong Cun Yuan / SID :1002074
Instructor/Lecturer :Professor Tang Zhaohui
6 February 2019

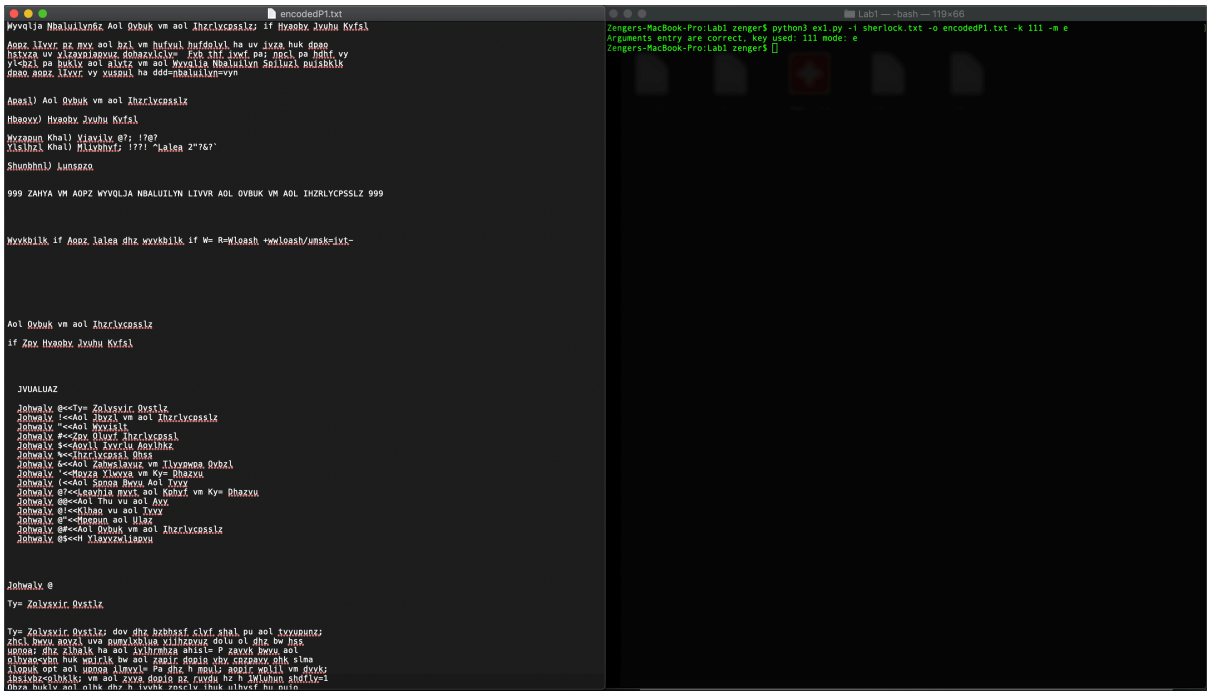
50.020 Security

Lab1 Report /Introduction and Shift ciphers

Part I: Shift Cipher for printable input

Code filename: ex1.py

Encoding P1



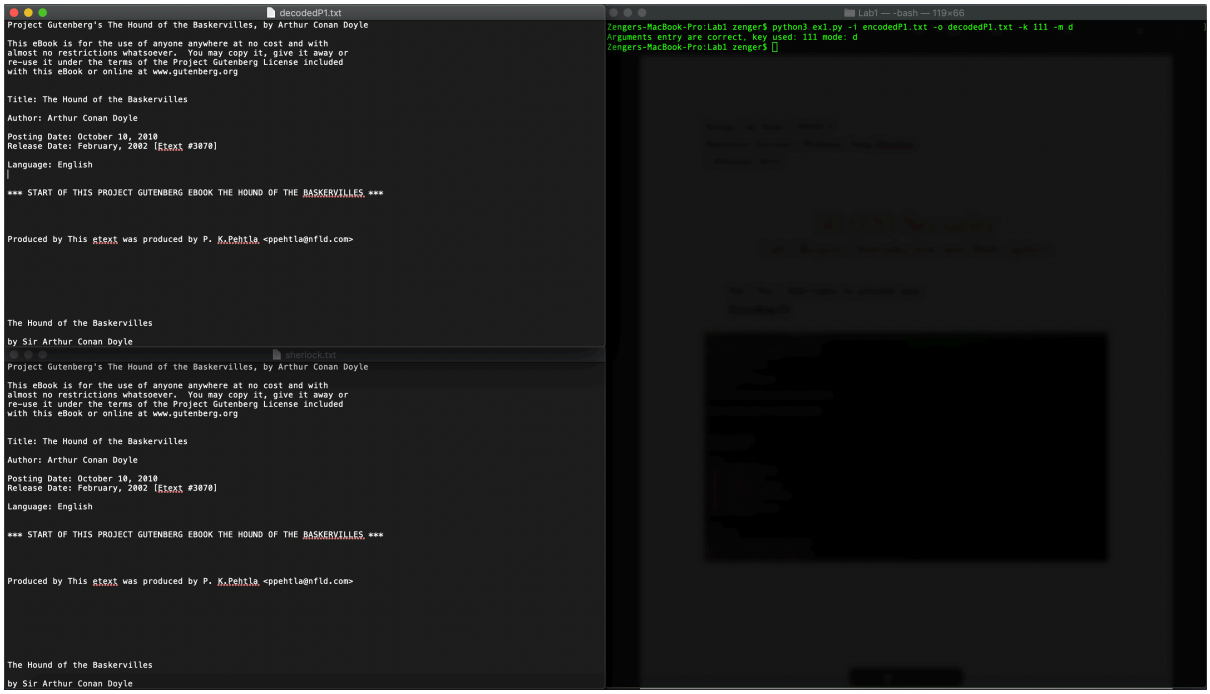
Using the Python Program in Bash:

```
python3 ex1.py -i sherlock.txt -o encodedP1.txt -k 111 -m e
```

Using the above command, the Sherlock.txt is encoded with key value 111 and in encoding mode.

The Text image on the left shows the Ciphered Text.

Decoding P1



Using the Python Program in Bash:

```
ex1.py -i encodedP1.txt -o decodedP1.txt -k 111 -m d
```

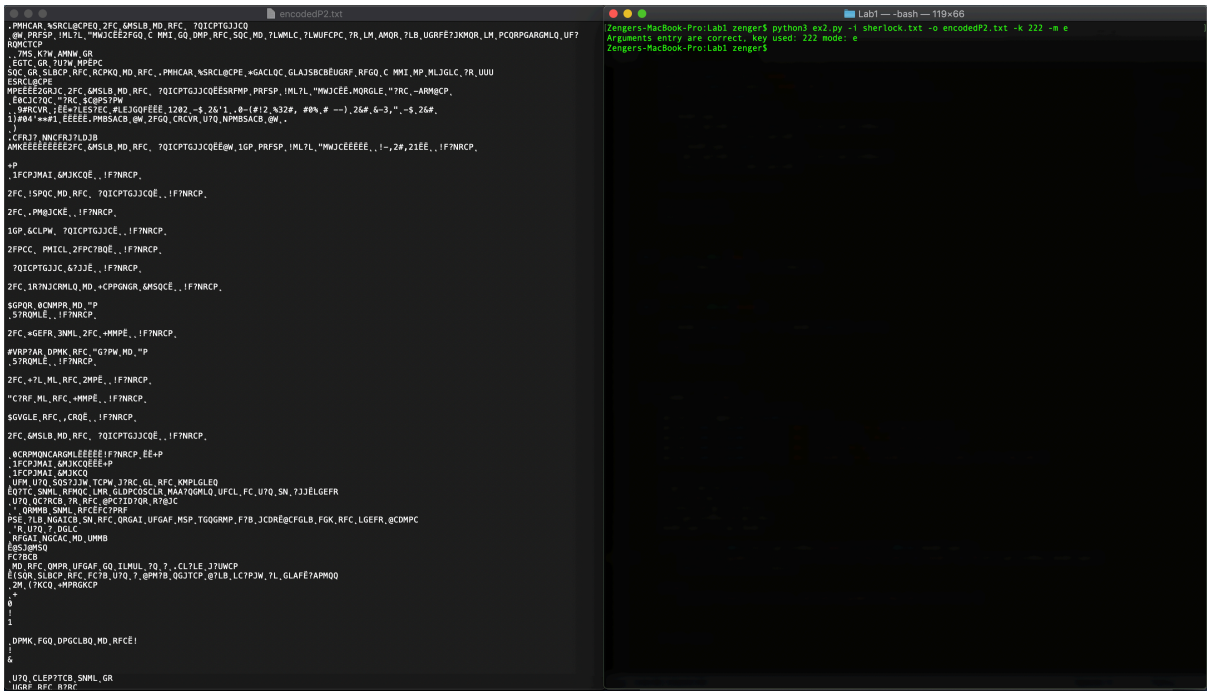
Using the above command, the Sherlock.txt is decoded with key value 111 and in decoding mode.

The Text image on the top left show the deciphered plain texted and comparing with the original(right bottom), they are the same, after encoding and decoding.

Part II: Shift Cipher for binary input

Code filename: ex2.py

Encoding P2



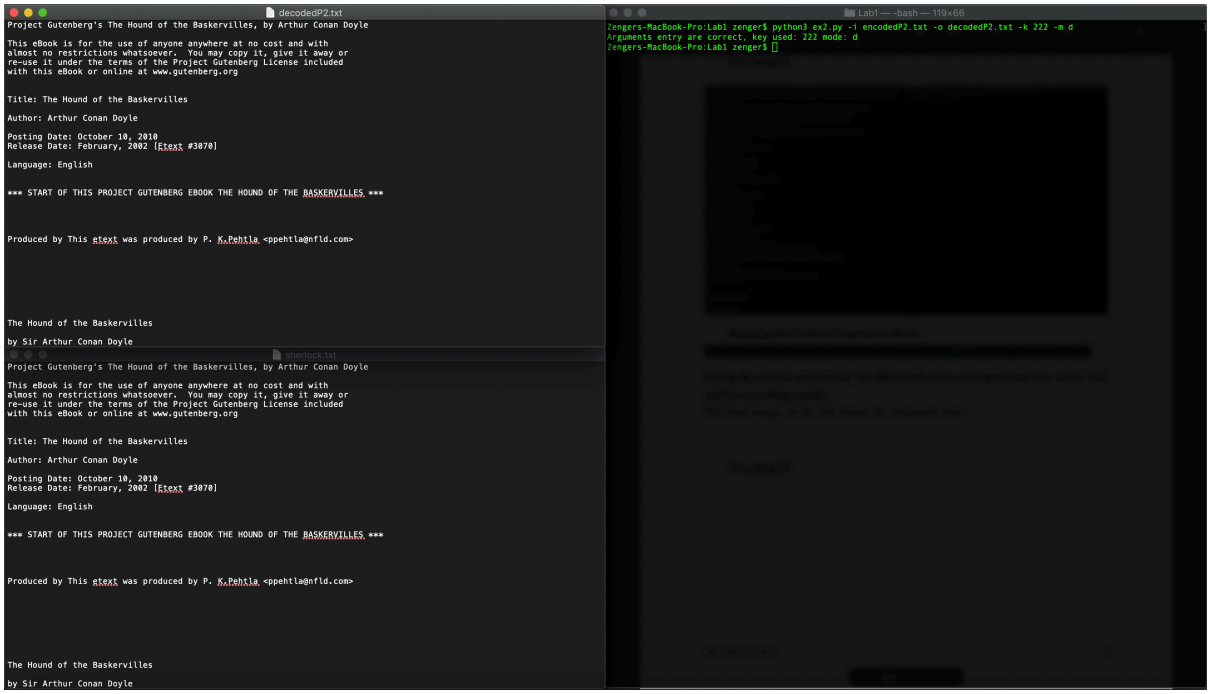
Running the Python Program in Bash:

```
python3 ex2.py -i sherlock.txt -o encodedP2.txt -k 222 -m e
```

Using the above command, the Sherlock.txt is encoded with key value 222 and in encoding mode.

The Text image on the left shows the Ciphered Text.

Decoding P2




```
python3 ex2.py -i encodedP2.txt -o decodedP2.txt -k 222 -m d
```

Using the above command, the Sherlock.txt is decoded with key value 222 and in decoding mode.

The Text image on the top left show the deciphered plain texted and comparing with the original(right bottom), they are the same, after encoding and decoding.

Part III: Break Shift Cipher of flag

I have done the implementation in 3 different ways using shell script and python scripts

Using code from part2 to solve the question, by testing the filetype after every decode step with key from 0-255.

Multiple ways to solve

#1. Shell script

Code name : ex3.sh with ex2.py

ex4.sh

```
#!/bin/bash

k=0
while [ $k -lt 256 ]
do
    python3 ex2.py -i flag -o flagout.png -k $k -m d
    if file flagout.png | grep PNG; then
        echo key = $k
        break
    fi
    k=$( expr $k + 1 )
done
```

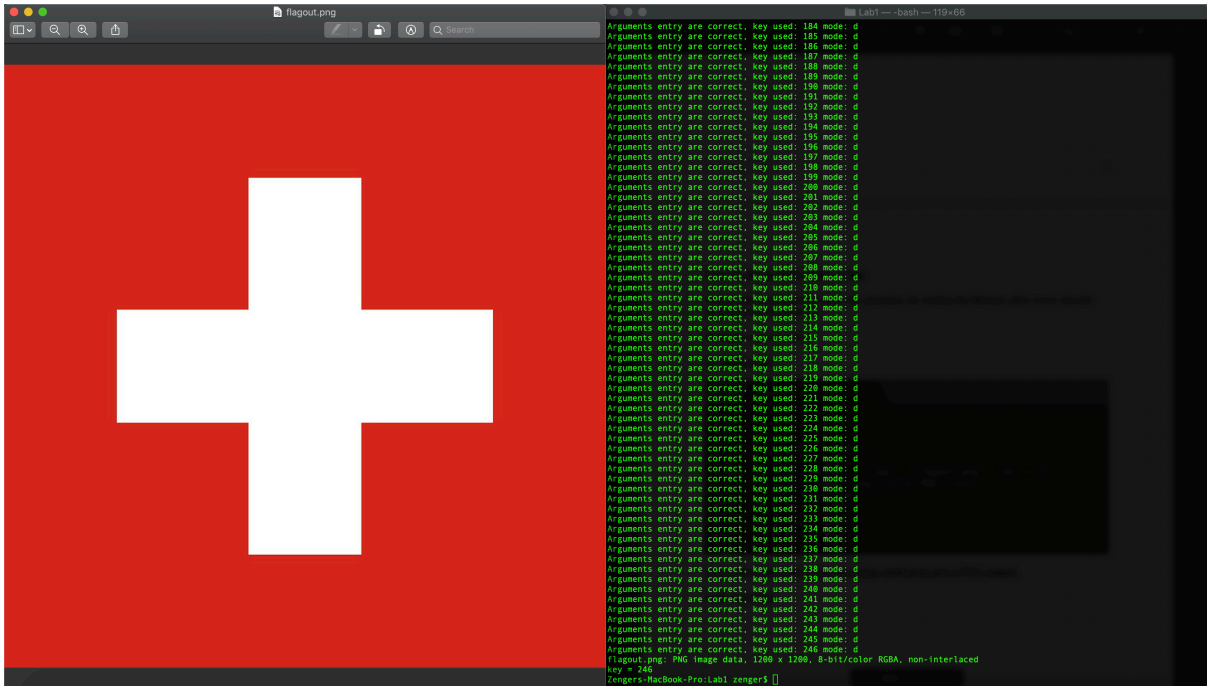
Above show the code to run the ex2.py until grep gets a PNG output.

Code in Action:

```
./ex3.sh
```

Just run the above line to execute the shell script, make sure command :

chmod +x ex3.sh is ran prior! Key is 246!



#2.Second Shell script methods
Code name : ex3v2.sh with ex2.py

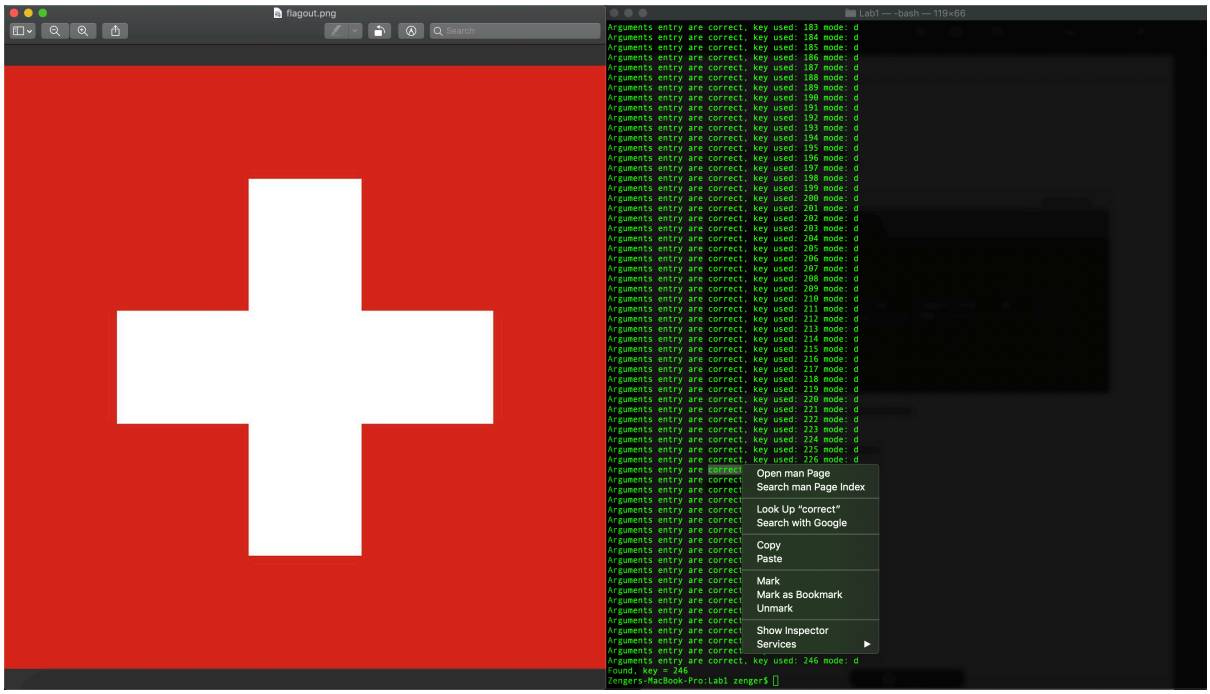
ex3v2.sh

```
#!/bin/bash

k=0
while (( k < 256 ))
do
    python3 ex2.py -i flag -o flagout.png -k $k -m d
    if file flagout.png | grep PNG; then
        echo key = $k
        break
    fi
    (( k += 1 ))
done
```

Same as ex3.sh just different implementation.
Same picture is returned!
Key is 246!
#3 Python script methods(Os Library)
Code name : ex3.py with ex2.py

```
python3 ex3.py
```



Result is the same as the shell script methods, just different implementation! Key is 246!