

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

The image shows two terminal windows side-by-side. The left window displays the contents of a file named 'encodedP1.txt' which contains a long string of encrypted text. The right window shows the command being run: 'python3 ex1.py -i sherlock.txt -o encodedP1.txt -k 111 -m e'. The output of the command is also visible in the right terminal.

```
encodedP1.txt
if Hyaoxy Jvhu Kvfs1
Aopz Ivxr pz myx sol hzl wnfuf hufdolv, ha uv jyza huk dpo
hsitzva uv xlzavplaqzux dohazxclvly" Fvb thi jxel pe; npcl pa hdtf
yichz pa bukv sol alvtz vm sol Wyvqlja Nbauljvn Smiluzl pujshtk
Hnra Mora lskke, vy xwzhu ha dde-nbauljvn-vyn

Aopz! sol Qvbk vm sol Ihzrlvcassl
Hyaoxy) Hyaoxy Jvhu Kvfs1
Wyapim Khal) Vleavly?@! ?0?
X(xhsl Khal) Hlyavny; ??? "Lalea 2"?"?
Shuobmnl) Lwosazo

999 ZAHYA VM AOPZ WYVQLJA NBALUJVN LIVVR AOL OVBUK VM AOL IHZRLYCPSSLZ 999

Wxxkbilk if Aozz laera dhz wxxkbilk if W= R=Mloash +Mloash/msh=jxt-
Aol Qvbk vm sol Ihzrlvcassl
if Aox Hyaoxy Jvhu Kvfs1

JVALUAZ
Johnwlv <->T= Zolysvir Qvstlx
Johnwlv !<->Qvzvl vm sol Ihzrlvcassl
Johnwlv <->Qvzvl Qvzvl Ihzrlvcassl
Johnwlv $<->Qvzvl Kxvlu Asvihk
Johnwlv %<->Qvzvl Zehwslavuz vm Tlvywwoa Qvzvl
Johnwlv <->Qvzvl Kxvxa vm Ky= Dhazvu
Johnwlv <->Qvzvl Kxvxa vm Ky= Dhazvu
Johnwlv @7<->Legavnia myxt sol Kohmf vm Ky= Dhazvu
Johnwlv @8<->Aoi Thu vu so! Ayv
Johnwlv @9<->Aoi Dzvuk vm sol Ihzrlvcassl
Johnwlv @10<->Aoi Dzvuk vm sol Ihzrlvcassl
Johnwlv @11<->Aoi Dzvuk vm sol Ihzrlvcassl

Johnwlv =
T= Zolysvir Qvstlx

T= Zolysvir Qvstlx; dov dhz bzbhssf clvf shal pu sol_tvvypunz;
zhcl_hnu abzil uva sumykhva vlnhzpvz dolz ol dhz bw hsz
mopqzvz vlnhzpvz dolz ol dhz bw hsz
plivycsvn huk Wahrlik bw asr zmpir dpolis vby_czrpzv, ght slma
jloqu opt sol monor ilmyvl; Pa dhz h mpol; aspirc wlll vm svyks;
Aspivcavzjmlsbo sol zvks dpolis Re zpshh ha n Anhuan shiflyz;
Inra mduy sol mduy sol zvks dpolis Re zpshh ha n Anhuan shiflyz;
```

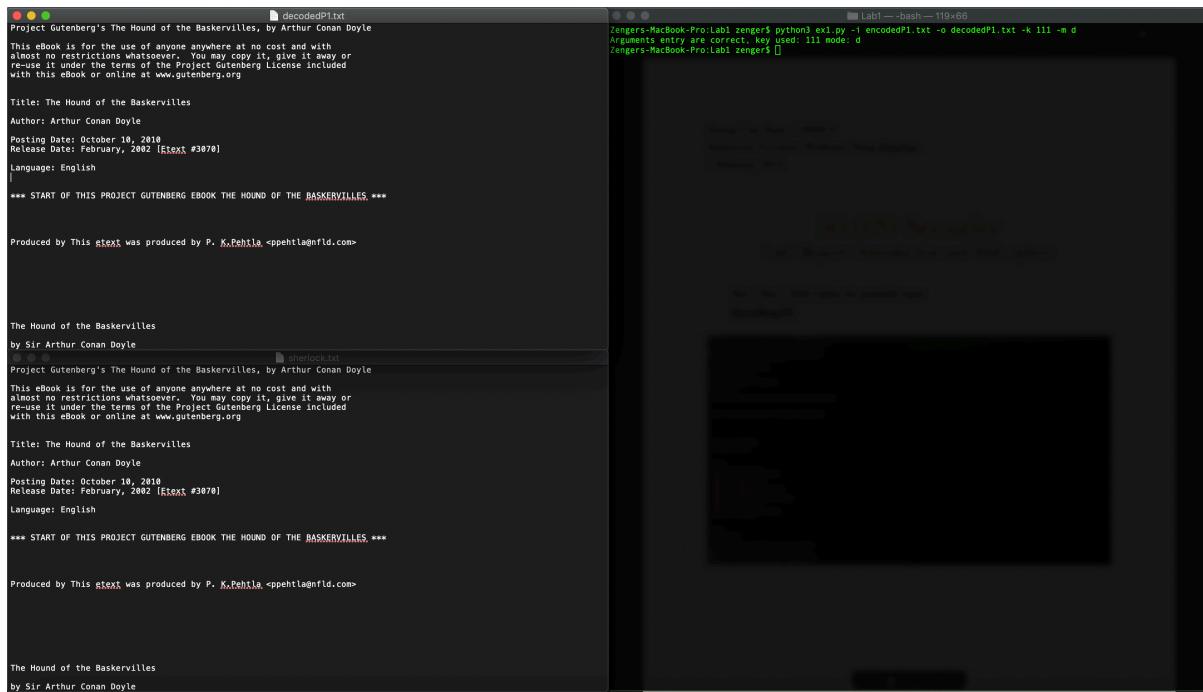
Using the Python Program in Bash:

```
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 Encrypted Text.

Decoding P1



```
Project Gutenberg's The Hound of the Baskervilles, by Arthur Conan Doyle
This eBook is for the use of anyone anywhere at no cost and with almost no restrictions whatsoever. You may copy it, give it away or re-use it under the terms of the Project Gutenberg License included with this eBook or online at www.gutenberg.org

Title: The Hound of the Baskervilles
Author: Arthur Conan Doyle
Posting Date: October 10, 2018
Release Date: February, 2002 [etext #3878]
Language: English

*** START OF THIS PROJECT GUTENBERG EBOOK THE HOUND OF THE BASKERVILLES ***

Produced by This etext was produced by P. K. Pehtila <ppehtila@nfld.com>

The Hound of the Baskervilles
by Sir Arthur Conan Doyle
Project Gutenberg's The Hound of the Baskervilles, by Arthur Conan Doyle
This eBook is for the use of anyone anywhere at no cost and with almost no restrictions whatsoever. You may copy it, give it away or re-use it under the terms of the Project Gutenberg License included with this eBook or online at www.gutenberg.org

Title: The Hound of the Baskervilles
Author: Arthur Conan Doyle
Posting Date: October 10, 2018
Release Date: February, 2002 [etext #3878]
Language: English

*** START OF THIS PROJECT GUTENBERG EBOOK THE HOUND OF THE BASKERVILLES ***

Produced by This etext was produced by P. K. Pehtila <ppehtila@nfld.com>

The Hound of the Baskervilles
by Sir Arthur Conan Doyle
```

Using the Python Program in Bash:

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

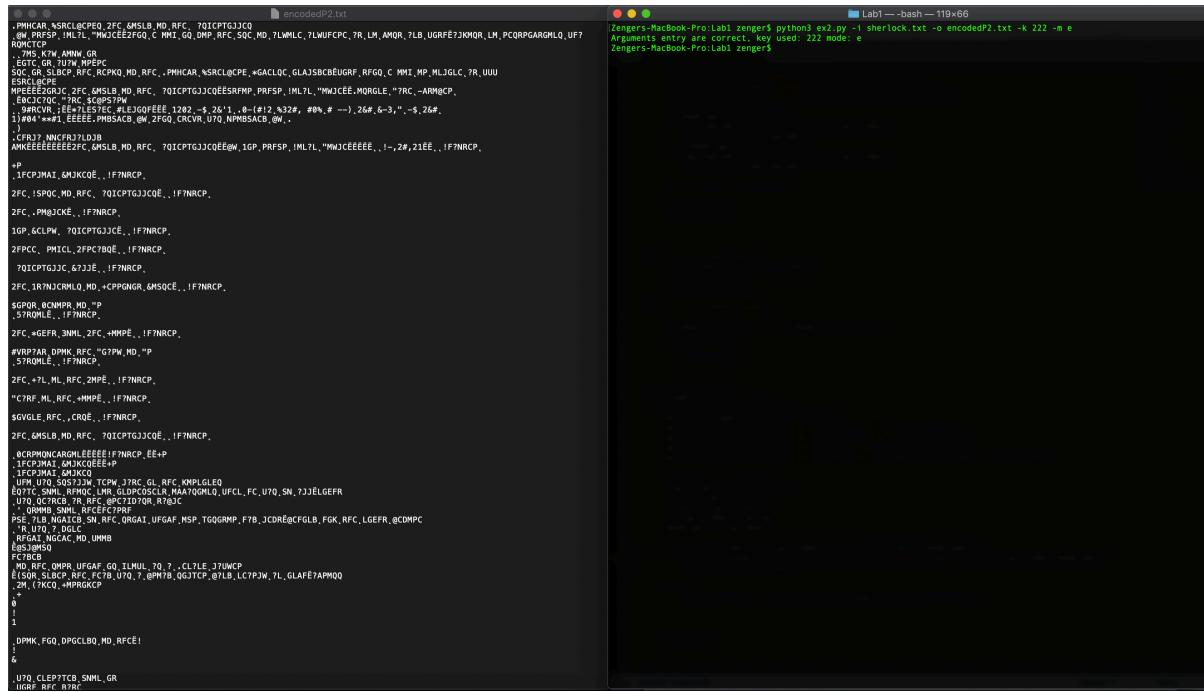
Using the above command, the Sherlock.txt is decoded with key value 111 and in decoding mode.

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



```
encodedP2.txt
Zenger's-MacBook-Pro:Lab1 zenger$ python3 ex2.py -i sherlock.txt -o encodedP2.txt -k 222 -m e
Arguments entry are correct; Key used: 222 mode: e
Zenger's-MacBook-Pro:Lab1 zenger$
```

The terminal window shows the command being run: `python3 ex2.py -i sherlock.txt -o encodedP2.txt -k 222 -m e`. The output pane shows the contents of `encodedP2.txt`, which is a large block of binary-like characters.

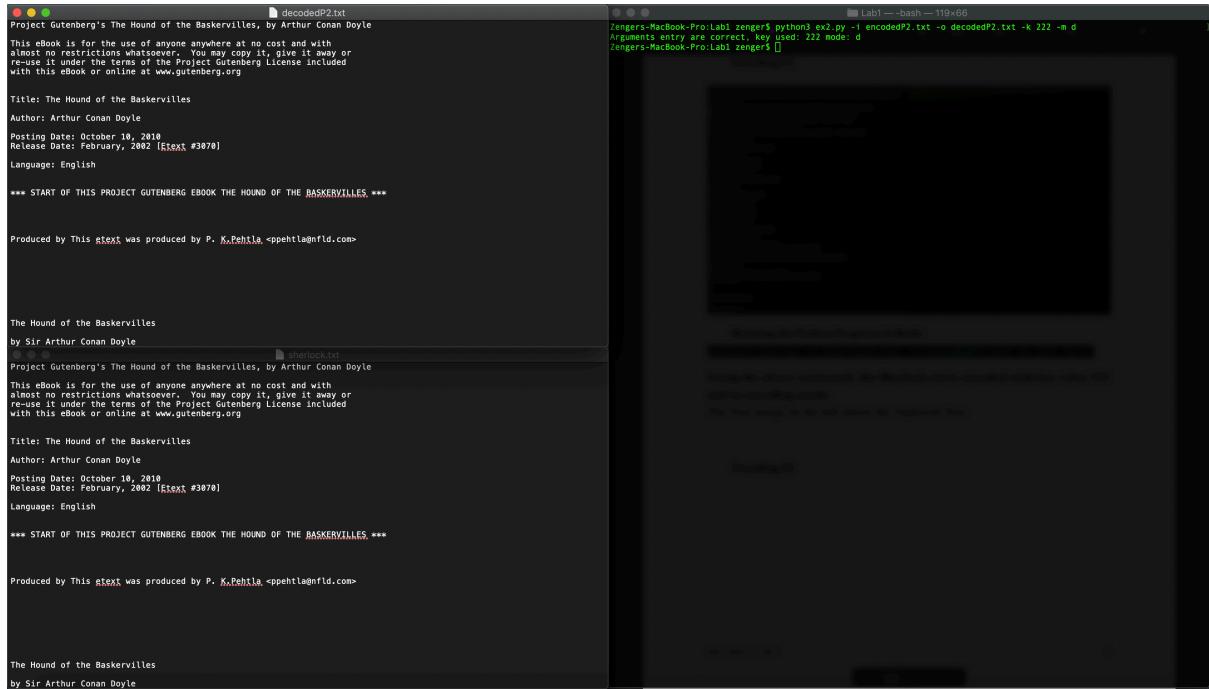
Running the Python Program in Bash:

```
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



```
Project Gutenberg's The Hound of the Baskervilles, by Arthur Conan Doyle
This eBook is for the use of anyone anywhere at no cost and with
almost no restrictions whatsoever. You may copy it, give it away or
re-use it under the terms of the Project Gutenberg License included
with this eBook or online at www.gutenberg.org

Title: The Hound of the Baskervilles
Author: Arthur Conan Doyle
Posting Date: October 10, 2002
Release Date: February, 2002 [Etext #3870]
Language: English

*** START OF THIS PROJECT GUTENBERG EBOOK THE HOUND OF THE BASKERVILLES ***

Produced by This etext was produced by P. K. Pehtla <ppehtla@mfld.com>

The Hound of the Baskervilles
by Sir Arthur Conan Doyle
Project Gutenberg's The Hound of the Baskervilles, by Arthur Conan Doyle
This eBook is for the use of anyone anywhere at no cost and with
almost no restrictions whatsoever. You may copy it, give it away or
re-use it under the terms of the Project Gutenberg License included
with this eBook or online at www.gutenberg.org

Title: The Hound of the Baskervilles
Author: Arthur Conan Doyle
Posting Date: October 10, 2002
Release Date: February, 2002 [Etext #3870]
Language: English

*** START OF THIS PROJECT GUTENBERG EBOOK THE HOUND OF THE BASKERVILLES ***

Produced by This etext was produced by P. K. Pehtla <ppehtla@mfld.com>

The Hound of the Baskervilles
by Sir Arthur Conan Doyle
```

```
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

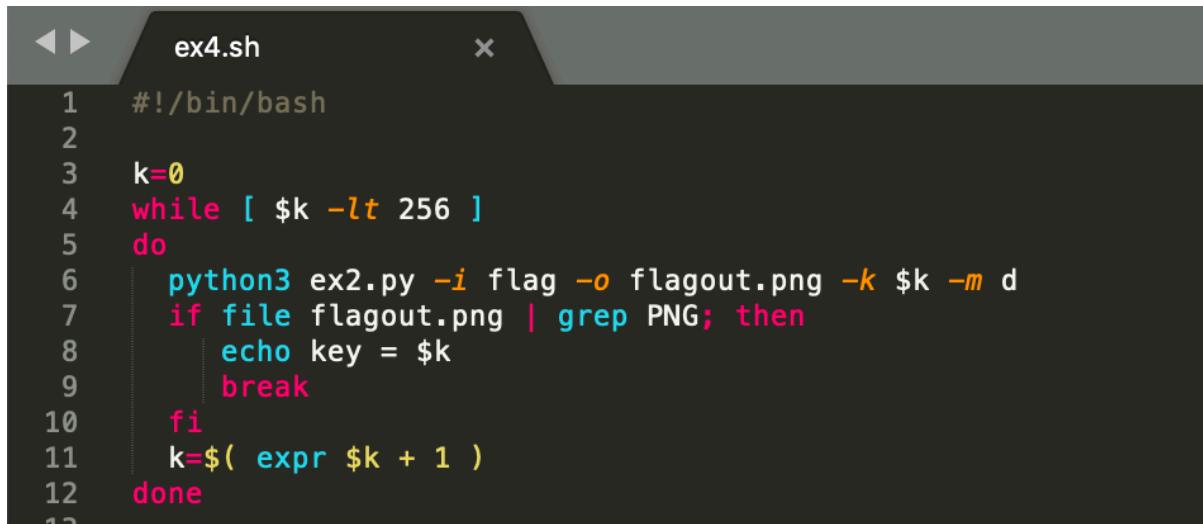
I have done the implementation in 3 different ways using shell script and python scripts

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



```
1 #!/bin/bash
2
3 k=0
4 while [ $k -lt 256 ]
5 do
6     python3 ex2.py -i flag -o flagout.png -k $k -m d
7     if file flagout.png | grep PNG; then
8         echo key = $k
9         break
10    fi
11    k=$( expr $k + 1 )
12 done
```

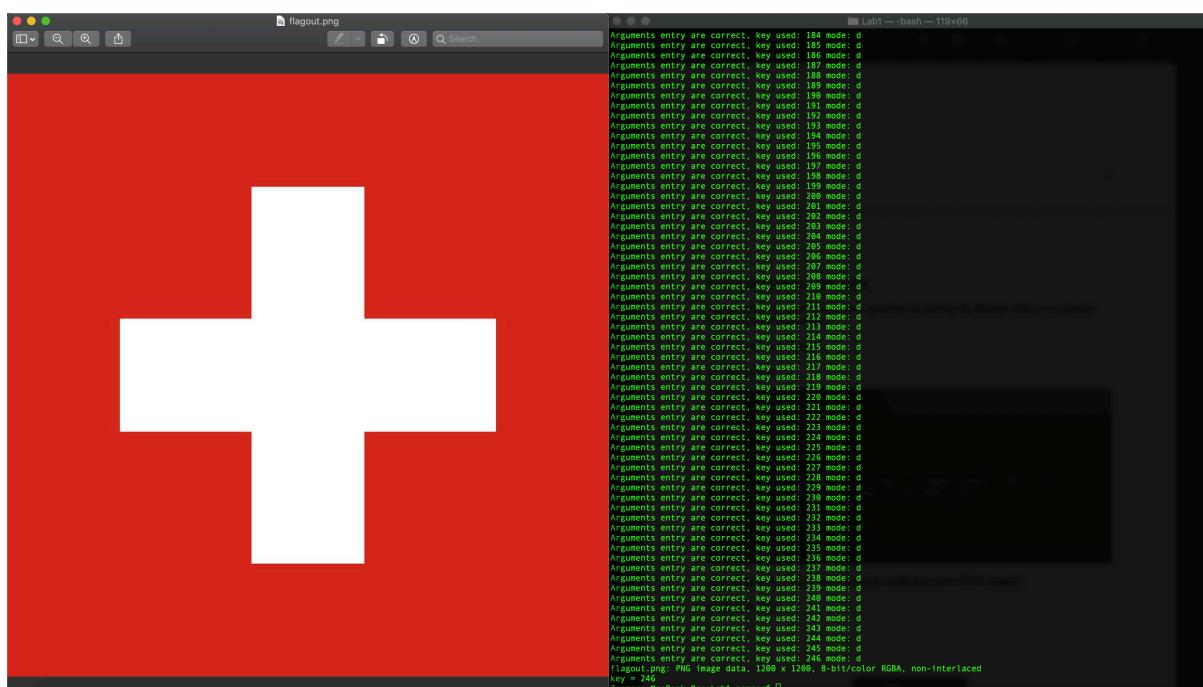
Above show the code to run the ex2.py until grep gets a PNG output.

Code in Action:

./ex3.sh

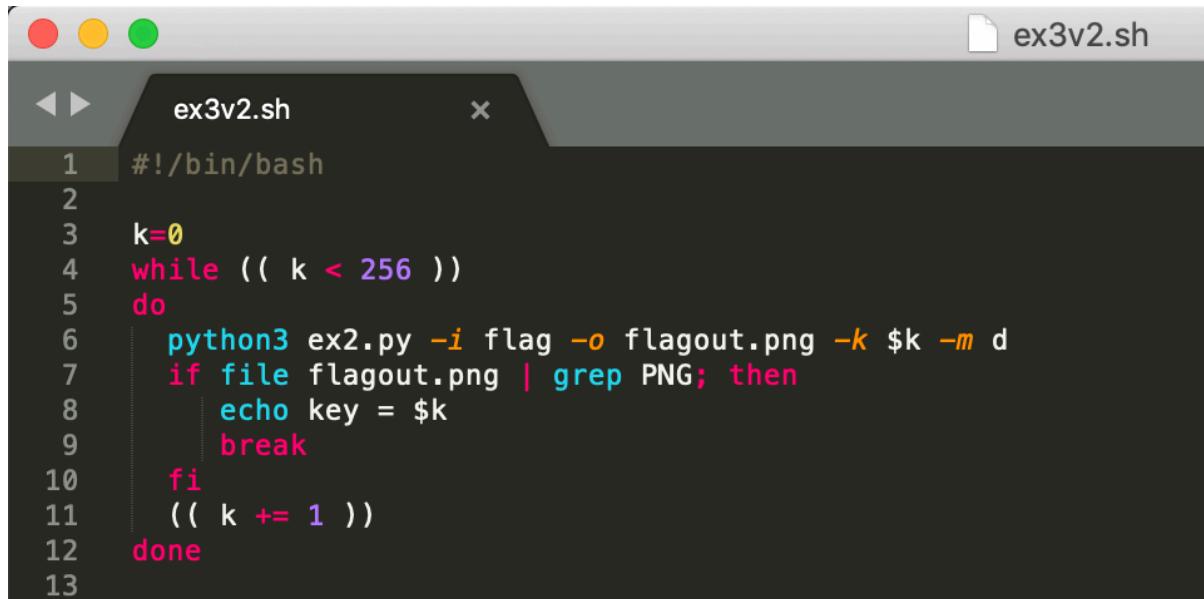
Just run the above line to execute the shell script, make sure command :

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



#2.Second Shell script methods

Code name : ex3v2.sh with ex2.py



```
#!/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.

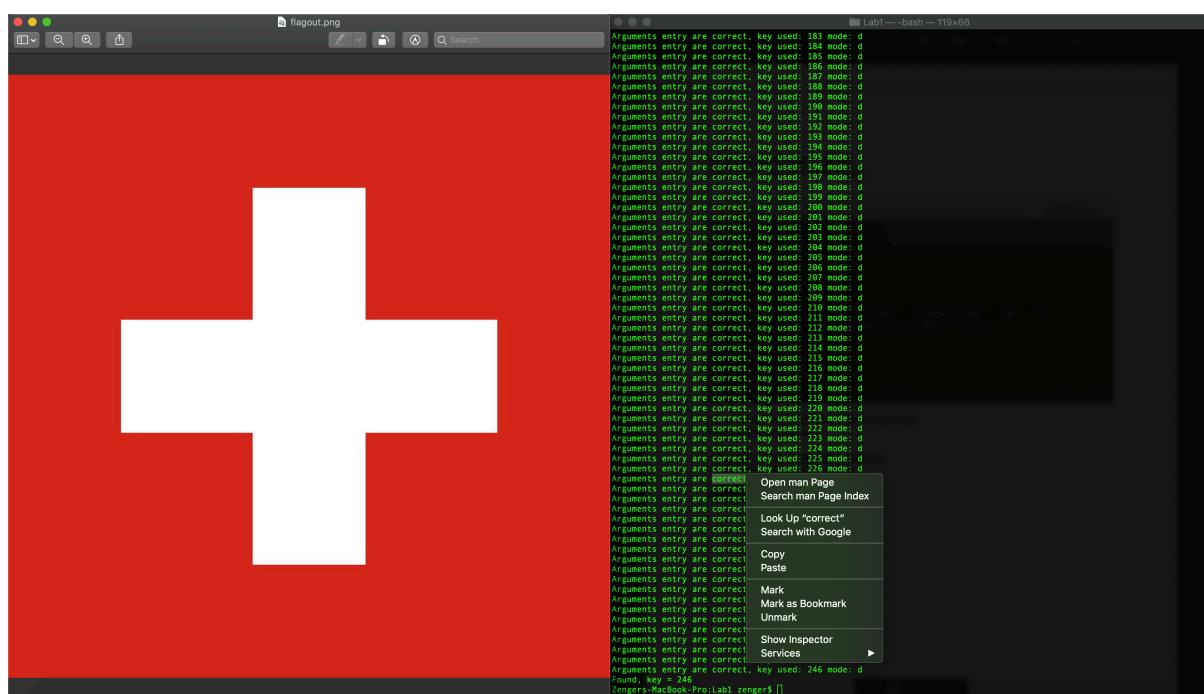
Same picture is returned!

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!