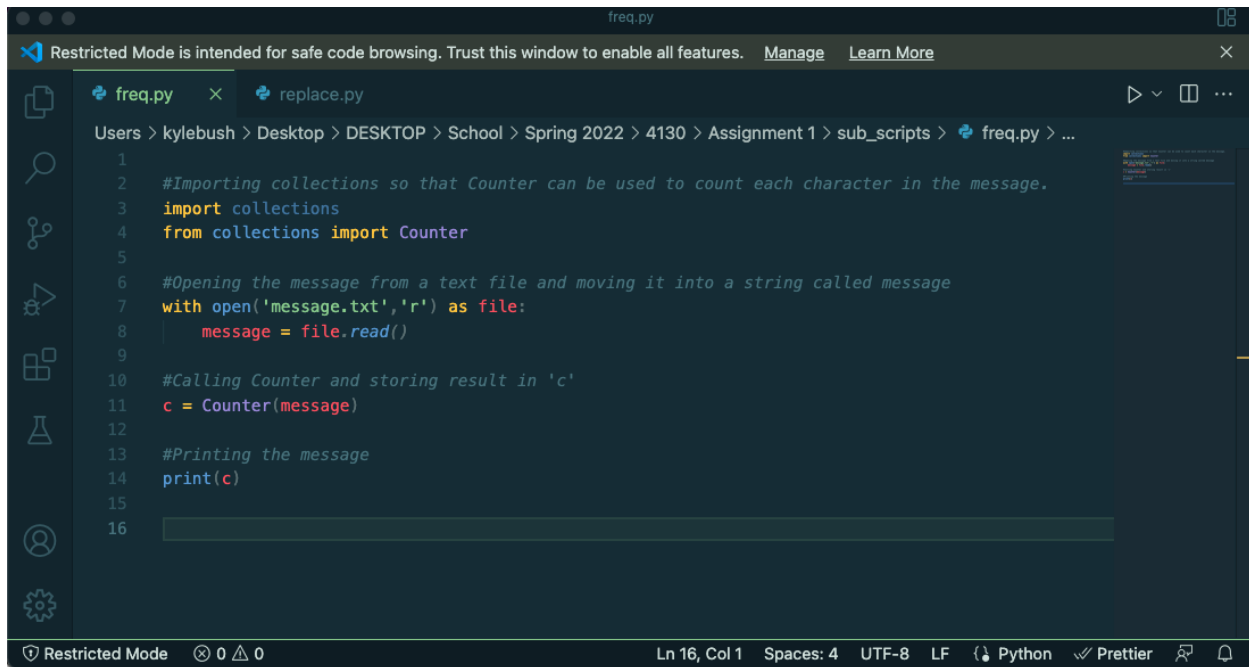


Kyle Bush
CSCI4130
Assignment 1

To figure out the key, I decided to see how far I could get using a frequency attack. I started by writing a python script called freq.py that would use the collections library to find the frequency of characters. The code and results are below.

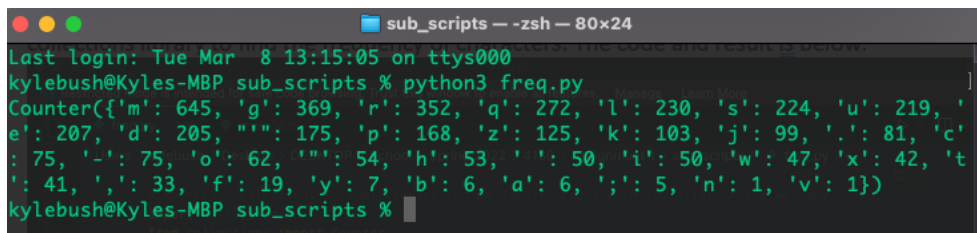


```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
#Importing collections so that Counter can be used to count each character in the message.
import collections
from collections import Counter

#Opening the message from a text file and moving it into a string called message
with open('message.txt','r') as file:
    message = file.read()

#Calling Counter and storing result in 'c'
c = Counter(message)

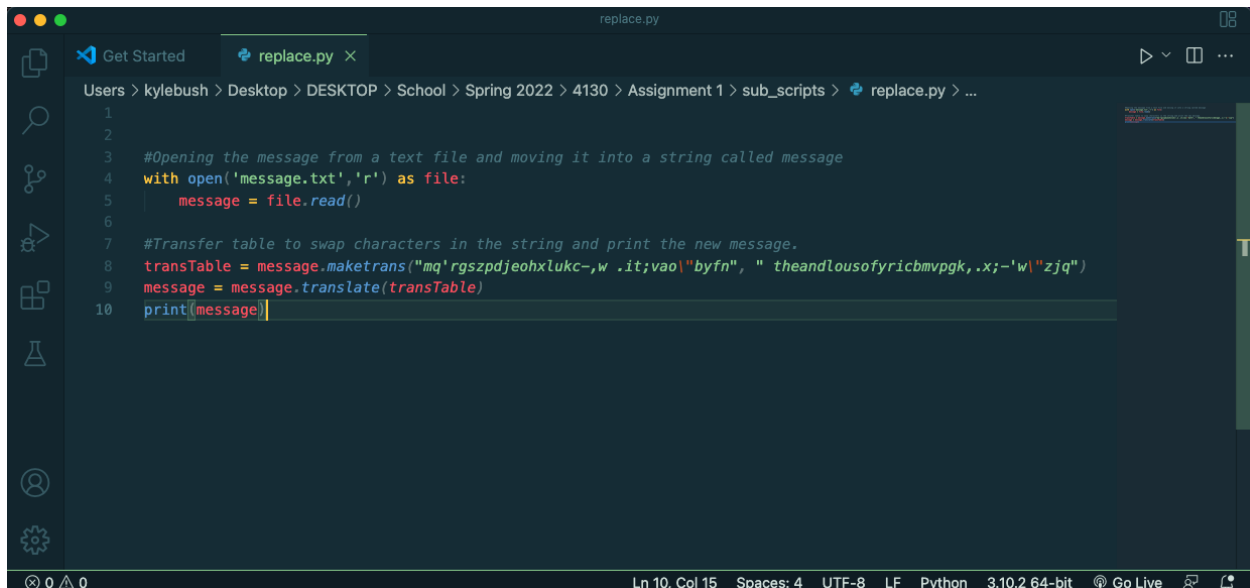
#Printing the message
print(c)
```



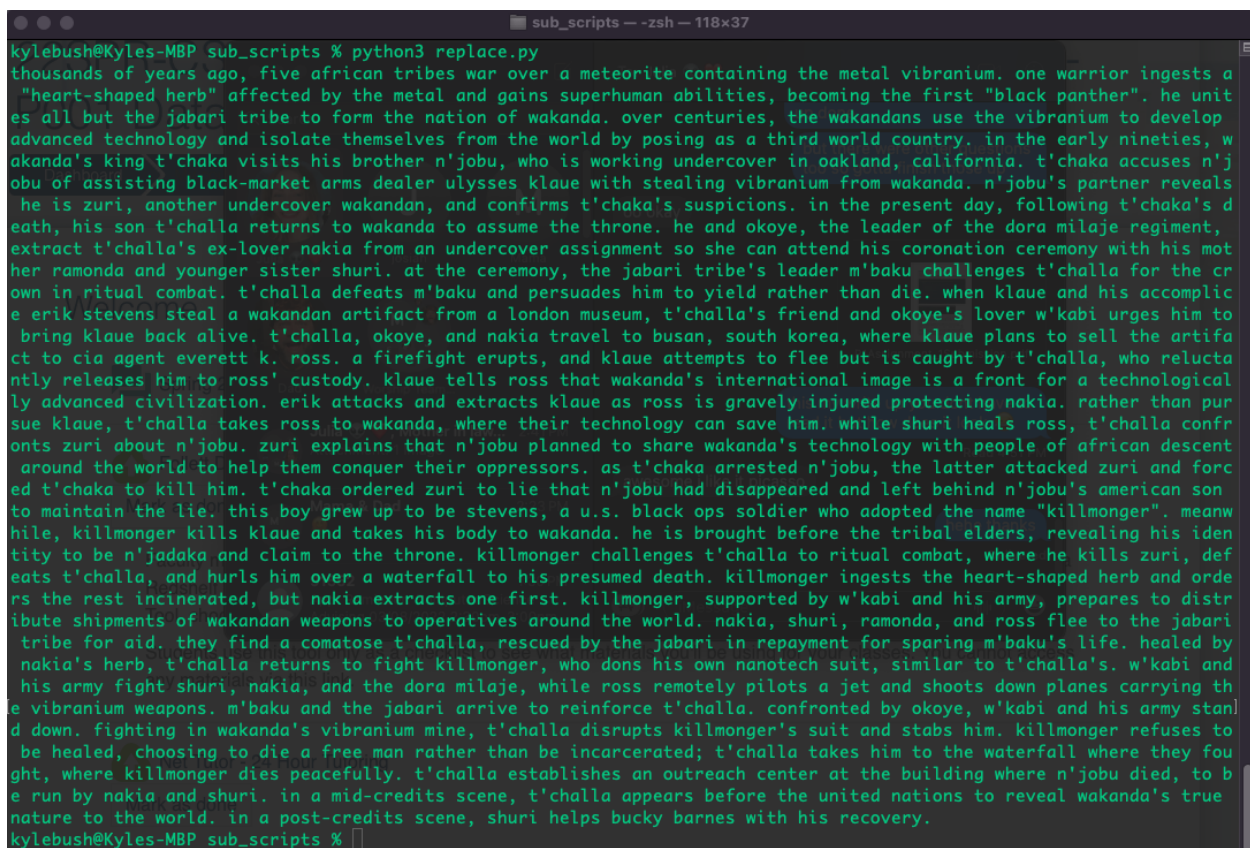
```
sub_scripts - zsh - 80x24
Last login: Tue Mar  8 13:15:05 on ttys000
kylebush@Kyles-MBP sub_scripts % python3 freq.py
Counter({'m': 645, 'g': 369, 'r': 352, 'q': 272, 'l': 230, 's': 224, 'u': 219, 'e': 207, 'd': 205, '"': 175, 'p': 168, 'z': 125, 'k': 103, 'j': 99, '.': 81, 'c': 75, '-': 75, 'o': 62, "'": 54, 'h': 53, ' ': 50, 'i': 50, 'w': 47, 'x': 42, 't': 41, ',': 33, 'f': 19, 'y': 7, 'b': 6, 'a': 6, ';': 5, 'n': 1, 'v': 1})
kylebush@Kyles-MBP sub_scripts %
```

I knew that since spaces were also encrypted, the most frequent character from the cipher text would most likely be able to be substituted for the space character. I wrote another python script named replace.py and started using a transfer table to swap all “m” characters to “ “. I referred to many frequencies of character graphs and saw “e” and “t” were among the most common. I decided to see if I could substitute any common three-character long words for “the,” since it is the most frequently used three letter word. Two three letter combinations frequently appeared: “q’r” and “gsz.” I saw that “q” and “r” were high in the original message frequency, so I substituted “q’r” for “the.” I decided I would just substitute “gsz” for “and” since “g” was also very common and “a” is a very common character, which could be a replacement for “g.” I then got sort of lucky, since after making these substitutions, the first word in the message started with “th” and contained “and.” I used a site called wordhippo.com which let me look up a 9 character long word that contained the characters “thand.” I saw “thousand” as a result and substituted this in, which led to me being able to find out the opening phrase

“thousands of years ago.” I then just went through and pieced together the broken words to make them readable and ended with the following python script and output.



```
1
2
3 #Opening the message from a text file and moving it into a string called message
4 with open('message.txt','r') as file:
5     message = file.read()
6
7 #Transfer table to swap characters in the string and print the new message.
8 transTable = message.maketrans("mq'rgszpdjeohxlukc~,.it;vaol"byfn", " theandlousofyricbmvpqk,.x;-w"zjq")
9 message = message.translate(transTable)
10 print(message)]
```



```
kylebush@Kyles-MBP sub_scripts % python3 replace.py
thousands of years ago, five african tribes war over a meteorite containing the metal vibranium. one warrior ingests a
"heart-shaped herb" affected by the metal and gains superhuman abilities, becoming the first "black panther". he unit
es all but the jabari tribe to form the nation of wakanda. over centuries, the wakandans use the vibranium to develop
advanced technology and isolate themselves from the world by posing as a third world country. in the early nineties, w
akanda's king t'chaka visits his brother n'jobu, who is working undercover in oakland, california. t'chaka accuses n'j
obu of assisting black-market arms dealer ulysses klaue with stealing vibranium from wakanda. n'jobu's partner reveals
he is zuri, another undercover wakandan, and confirms t'chaka's suspicions. in the present day, following t'chaka's d
eath, his son t'challa returns to wakanda to assume the throne. he and okoye, the leader of the dora milaje regiment,
extract t'challa's ex-lover nakia from an undercover assignment so she can attend his coronation ceremony with his mot
her ramonda and younger sister shuri. at the ceremony, the jabari tribe's leader m'baku challenges t'challa for the cr
own in ritual combat. t'challa defeats m'baku and persuades him to yield rather than die. when klaue and his accomplic
e erik stevens steal a wakandan artifact from a london museum, t'challa's friend and okoye's lover w'kabi urges him to
bring klaue back alive. t'challa, okoye, and nakia travel to busan, south korea, where klaue plans to sell the artifa
ct to cia agent everett k. ross. a firefight erupts, and klaue attempts to flee but is caught by t'challa, who relucta
ntly releases him to ross' custody. klaue tells ross that wakanda's international image is a front for a technological
ly advanced civilization. erik attacks and extracts klaue as ross is gravely injured protecting nakia. rather than pur
sue klaue, t'challa takes ross to wakanda, where their technology can save him. while shuri heals ross, t'challa confr
onts zuri about n'jobu. zuri explains that n'jobu planned to share wakanda's technology with people of african descent
around the world to help them conquer their oppressors. as t'chaka arrested n'jobu, the latter attacked zuri and forc
ed t'chaka to kill him. t'chaka ordered zuri to lie that n'jobu had disappeared and left behind n'jobu's american son
to maintain the lie. this boy grew up to be stevens, a u.s. black ops soldier who adopted the name "killmonger". meanw
hile, killmonger kills klaue and takes his body to wakanda. he is brought before the tribal elders, revealing his iden
tity to be n'jadaka and claim to the throne. killmonger challenges t'challa to ritual combat, where he kills zuri, def
eats t'challa, and hurls him over a waterfall to his presumed death. killmonger ingests the heart-shaped herb and orde
rs the rest incinerated, but nakia extracts one first. killmonger, supported by w'kabi and his army, prepares to distr
ibute shipments of wakandan weapons to operatives around the world. nakia, shuri, ramonda, and ross flee to the jabari
tribe for aid. they find a comatose t'challa, rescued by the jabari in repayment for sparing m'baku's life. healed by
nakia's herb, t'challa returns to fight killmonger, who dons his own nanotech suit, similar to t'challa's. w'kabi and
his army fight shuri, nakia, and the dora milaje, while ross remotely pilots a jet and shoots down planes carrying th
e vibranium weapons. m'baku and the jabari arrive to reinforce t'challa. confronted by okoye, w'kabi and his army stan
d down. fighting in wakanda's vibranium mine, t'challa disrupts killmonger's suit and stabs him. killmonger refuses to
be healed, choosing to die a free man rather than be incarcerated; t'challa takes him to the waterfall where they fou
ght, where killmonger dies peacefully. t'challa establishes an outreach center at the building where n'jobu died, to b
e run by nakia and shuri. in a mid-credits scene, t'challa appears before the united nations to reveal wakanda's true
nature to the world. in a post-credits scene, shuri helps bucky barnes with his recovery.
kylebush@Kyles-MBP sub_scripts %
```

Plain-Text:

thousands of years ago, five african tribes war over a meteorite containing the metal vibranium. one warrior ingests a "heart-shaped herb" affected by the metal and gains superhuman abilities, becoming the first "black panther". he unites all but the jabari tribe to form the nation of wakanda. over centuries, the wakandans use the vibranium to develop advanced technology and isolate themselves from the world by posing as a third world country. in the early nineties, wakanda's king t'chaka visits his brother n'jobu, who is working undercover in oakland, california. t'chaka accuses n'jobu of assisting black-market arms dealer ulysses klaue with stealing vibranium from wakanda. n'jobu's partner reveals he is zuri, another undercover wakandan, and confirms t'chaka's suspicions. in the present day, following t'chaka's death, his son t'challa returns to wakanda to assume the throne. he and okoye, the leader of the dora milaje regiment, extract t'challa's ex-lover nakia from an undercover assignment so she can attend his coronation ceremony with his mother ramonda and younger sister shuri. at the ceremony, the jabari tribe's leader m'baku challenges t'challa for the crown in ritual combat. t'challa defeats m'baku and persuades him to yield rather than die. when klaue and his accomplice erik stevens steal a wakandan artifact from a london museum, t'challa's friend and okoye's lover w'kabi urges him to bring klaue back alive. t'challa, okoye, and nakia travel to busan, south korea, where klaue plans to sell the artifact to cia agent everett k. ross. a firefight erupts, and klaue attempts to flee but is caught by t'challa, who reluctantly releases him to ross' custody. klaue tells ross that wakanda's international image is a front for a technologically advanced civilization. erik attacks and extracts klaue as ross is gravely injured protecting nakia. rather than pursue klaue, t'challa takes ross to wakanda, where their technology can save him. while shuri heals ross, t'challa confronts zuri about n'jobu. zuri explains that n'jobu planned to share wakanda's technology with people of african descent around the world to help them conquer their oppressors. as t'chaka arrested n'jobu, the latter attacked zuri and forced t'chaka to kill him. t'chaka ordered zuri to lie that n'jobu had disappeared and left behind n'jobu's american son to maintain the lie. this boy grew up to be stevens, a u.s. black ops soldier who adopted the name "killmonger". meanwhile, killmonger kills klaue and takes his body to wakanda. he is brought before the tribal elders, revealing his identity to be n'jadaka and claim to the throne. killmonger challenges t'challa to ritual combat, where he kills zuri, defeats t'challa, and hurls him over a waterfall to his presumed death. killmonger ingests the heart-shaped herb and orders the rest incinerated, but nakia extracts one first. killmonger, supported by w'kabi and his army, prepares to distribute shipments of wakandan weapons to operatives around the world. nakia, shuri, ramonda, and ross flee to the jabari tribe for aid. they find a comatose t'challa, rescued by the jabari in repayment for sparing m'baku's life. healed by nakia's herb, t'challa returns to fight killmonger, who dons his own nanotech suit, similar to t'challa's. w'kabi and his army fight shuri, nakia, and the dora milaje, while ross remotely pilots a jet and shoots down planes carrying the vibranium weapons. m'baku and the jabari arrive to reinforce t'challa. confronted by okoye, w'kabi and his army stand down. fighting in wakanda's vibranium mine, t'challa disrupts killmonger's suit and stabs him. killmonger refuses to be healed, choosing to die a free man rather than be incarcerated; t'challa takes him to the waterfall where they fought, where killmonger dies peacefully. t'challa establishes an outreach center at the building where n'jobu died, to be run by nakia and shuri. in a mid-credits scene, t'challa appears before the united nations to reveal wakanda's true nature to the world. in a post-credits scene, shuri helps bucky barnes with his recovery.

Key:

gbkzrh 'uf.p-sdwnleqj,";xymboiatv

abcdefghijklmnopqrstuvwxyz "' ,-.;

1.3

- 1.) If a single ASIC engine costs \$50, there is also 100% overhead meaning a total of \$100 for an ASIC engine, and there is a budget of \$1,000,000, then $1,000,000/50 = 10,000$ engines.

To find the search speed:

$5 * 10^8 * 10,000 = 5 * 10^8 * 10^4 = 5 * 10^{12}$ keys per second. There are 2^{127} keys.

$2^{127} / 5 * 10^{12} = 3.4 * 10^{25}$ seconds.

$3.4 * 10^{25}$ seconds = $1.08 * 10^{18}$ years, which is much longer than the 10^{10} years that the universe has been around.

1.4

- 1.) Key space would be 128^8 .
- 2.) 8 letters with 7 bits per character give $8 * 7 = 56$ bits
- 3.) The possible characters would change from 127 to 26. This would give 26^8 .

1.7

Z4 Multiplication:

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Z5 Addition

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Z5 Multiplication

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Z6 Addition

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Z6 Multiplication

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The elements with a multiplicative inverse in Z_4 are 1 and 3, and in Z_6 are 1, 5, and 5. A multiplicative inverse exists for all nonzero elements in Z_5 since 5 is prime.

1.9

- 1.) $x = 3^2 \bmod 13 = 9 \bmod 13$
- 2.) $x = 7^2 \bmod 13 = 49 \bmod 13 = 10 \bmod 13$
- 3.) $x = 3^{10} \bmod 13 = 9^5 \bmod 13 = 81^2 * 9 \bmod 13 = 3^2 * 9 \bmod 13 = 81 \bmod 13 = 3 \bmod 13$
- 4.) $x = 7^{100} \bmod 13 = 49^{50} \bmod 13 = 10^{50} \bmod 13 = (-3)^{50} \bmod 13 = (3^{10})^5 \bmod 13 = 3^5 \bmod 13 = 3^2 \bmod 13 = 9 \bmod 13$

1.13

For chosen plaintext attack, plaintexts are chosen that: $\gcd(x_2 - x_1, m) = 1$. "m" is the amount of characters being encrypted, which means that $x_2 - x_1$ can be thought to have multiplicative inverse in m.

Oscar can then derive these equations:

$$a = (x_1 - x_2)^{-1}(y_1 - y_2) \bmod m$$

$$b = y_1 - ax_1 \bmod m$$

1.14

1.) $k_1 = (a_1, b_1)$ and $k_2 = (a_2, b_2)$

$$ek_1(x) = y = a_1 * x + b_1 \bmod 26$$

$$ek_2(ek_1(x)) = y = a_2 * (a_1 * x + b_1) + b_2 \bmod 26$$

If you then double encrypt with (a_1, b_1) and (a_2, b_2) :

$$k_3 = (a_1 a_2, a_2 b_1 + b_2) \bmod 26$$

2.) $k_3 = (3 * 11 \bmod 26, 11 * 5 + 7 \bmod 26)$