网安实训报告

LAB7

57118139 顾宸玮

# Word实验

1.

def findindexkey(subarr):

visiable\_chars=[]

for x in range(32,126):

visiable\_chars.append(chr(x))

#print(vi)

test\_keys=[]

ans\_keys=[]

for x in range(0x00,0xFF):

test\_keys.append(x)

ans\_keys.append(x)

for i in test\_keys:

for s in subarr:

if chr(s^i) not in visiable\_chars:

ans\_keys.remove(i)

break

#print(ans\_keys)

return ans\_keys

strmi='F96DE8C227A259C87EE1DA2AED57C93FE5DA36ED4EC87EF2C63AAE5B9A7EFF\

D673BE4ACF7BE8923CAB1ECE7AF2DA3DA44FCF7AE29235A24C963FF0DF3CA3\

599A70E5DA36BF1ECE77F8DC34BE129A6CF4D126BF5B9A7CFEDF3EB850D37CF\

0C63AA2509A76FF9227A55B9A6FE3D720A850D97AB1DD35ED5FCE6BF0D138A\

84CC931B1F121B44ECE70F6C032BD56C33FF9D320ED5CDF7AFF9226BE5BDE3F\

F7DD21ED56CF71F5C036A94D963FF8D473A351CE3FE5DA3CB84DDB71F5C17F\

ED51DC3FE8D732BF4D963FF3C727ED4AC87EF5DB27A451D47EFD9230BF47CA\

6BFEC12ABE4ADF72E29224A84CDF3FF5D720A459D47AF59232A35A9A7AE7D3\

3FB85FCE7AF5923AA31EDB3FF7D33ABF52C33FF0D673A551D93FFCD33DA35B\

C831B1F43CBF1EDF67F0DF23A15B963FE5DA36ED68D378F4DC36BF5B9A7AFF\

D121B44ECE76FEDC73BE5DD27AFCD773BA5FC93FE5DA3CB859D26BB1C63CE\

D5CDF3FE2D730B84CDF3FF7DD21ED5ADF7CF0D636BE1EDB79E5D721ED57CE\

3FE6D320ED57D469F4DC27A85A963FF3C727ED49DF3FFFDD24ED55D470E69E\

73AC50DE3FE5DA3ABE1EDF67F4C030A44DDF3FF5D73EA250C96BE3D327A84D\

963FE5DA32B91ED36BB1D132A31ED87AB1D021A255DF71B1C436BF479A7AF0\

C13AA14794'

arr=[]

for x in range(0,len(strmi),2):

arr.append(int(strmi[x:2+x],16))

for keylen in range(1,14):

for index in range(0,keylen):

subarr=arr[index::keylen]

ans\_keys=findindexkey(subarr)

print('keylen=',keylen,'index=',index,'keys=',ans\_keys)

if ans\_keys:

ch=[]

for x in ans\_keys:

ch.append(chr(x^subarr[0]))

print(ch)

print('###############')

import string

def findindexkey2(subarr):

test\_chars=string.ascii\_letters+string.digits+','+'.'+' '

#print(test\_chars)

test\_keys=[]

ans\_keys=[]

for x in range(0x00,0xFF):

test\_keys.append(x)

ans\_keys.append(x)

for i in test\_keys:

for s in subarr:

if chr(s^i) not in test\_chars:

ans\_keys.remove(i)

break

return ans\_keys

vigenerekeys=[]

for index in range(0,7):

subarr=arr[index::7]

vigenerekeys.append(findindexkey2(subarr))

print(vigenerekeys)

print("#########")

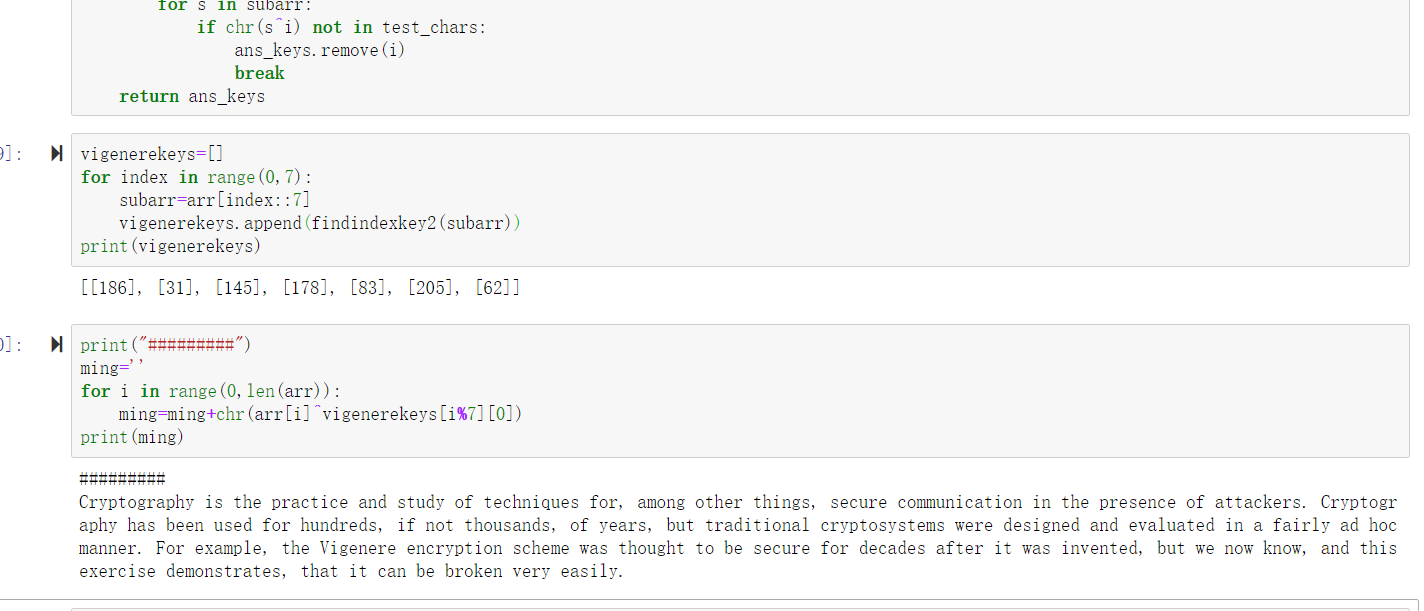
ming=''

for i in range(0,len(arr)):

ming=ming+chr(arr[i]^vigenerekeys[i%7][0])

print(ming)

最终输出



2、import sys

ciphertexts=[

"BB3A65F6F0034FA957F6A767699CE7FABA855AFB4F2B520AEAD612944A801E",

"BA7F24F2A35357A05CB8A16762C5A6AAAC924AE6447F0608A3D11388569A1E",

"A67261BBB30651BA5CF6BA297ED0E7B4E9894AA95E300247F0C0028F409A1E",

"A57261F5F0004BA74CF4AA2979D9A6B7AC854DA95E305203EC8515954C9D0F",

"BB3A70F3B91D48E84DF0AB702ECFEEB5BC8C5DA94C301E0BECD241954C831E",

"A6726DE8F01A50E849EDBC6C7C9CF2B2A88E19FD423E0647ECCB04DD4C9D1E",

"BC7570BBBF1D46E85AF9AA6C7A9CEFA9E9825CFD5E3A0047F7CD009305A71E"

]

NUM\_CIPHER=len(ciphertexts)

THRESHOLD\_VALUE=6

def strxor(a, b):

"""xor two strings of different lengths"""

if len(a) > len(b):

return "".join([chr(ord(x) ^ ord(y)) for (x, y) in zip(a[:len(b)], b)])

else:

return "".join([chr(ord(x) ^ ord(y)) for (x, y) in zip(a, b[:len(a)])])

def letter\_position(s):

""" Return the position of letters in the given string """

position=[]

for idx in range(len(s)):

if (s[idx]>='A' and s[idx]<='Z') or (s[idx]>='a' and s[idx]<='z'):

position.append(idx)

return position

def find\_space(cipher):

"""Find the position of space"""

space\_position={}

space\_possible={}

for cipher\_idx\_1 in range(NUM\_CIPHER):

space\_xor=[]

for cipher\_idx\_2 in range(NUM\_CIPHER):

plain\_xor=strxor(cipher[cipher\_idx\_1].decode('hex'),cipher[cipher\_idx\_2].decode('hex'))

if cipher\_idx\_2!=cipher\_idx\_1:

space\_xor.append(letter\_position(plain\_xor)) # record the possible value of space

space\_possible[cipher\_idx\_1]=space\_xor

for cipher\_idx\_1 in range(NUM\_CIPHER):

spa=[]

for position in range(100):

count=0

for cipher\_idx\_2 in range(NUM\_CIPHER-1):

if position in space\_possible[cipher\_idx\_1][cipher\_idx\_2]:

count+=1

if count>THRESHOLD\_VALUE: # if possible position value appear more than THRESHOLD\_VALUE times,

# we consider it as a space position

spa.append(position)

space\_position[cipher\_idx\_1]=spa;

return space\_position

def calculate\_key(cipher):

key=[0]\*100

space=find\_space(cipher)

for cipher\_idx\_1 in range(NUM\_CIPHER):

for position in range(len(space[cipher\_idx\_1])):

idx=space[cipher\_idx\_1][position]\*2; # ciphertext is hex-encoded, so its scale times two

key[space[cipher\_idx\_1][position]]=ord((ciphertexts[cipher\_idx\_1][idx]+ciphertexts[cipher\_idx\_1][idx+1]).decode('hex'))^ord(' '); #derive key

key\_str="";

for k in key:

key\_str+=chr(k);

return key\_str

result="";

key=calculate\_key(ciphertexts)

for i in range(7):

for letter in strxor(ciphertexts[i].decode('hex'),key): # decrypt the target cipher

if (letter>='a' and letter<='z') or (letter>='A' and letter<='Z'):

result+=letter;

elif letter==' ':

result+=letter;

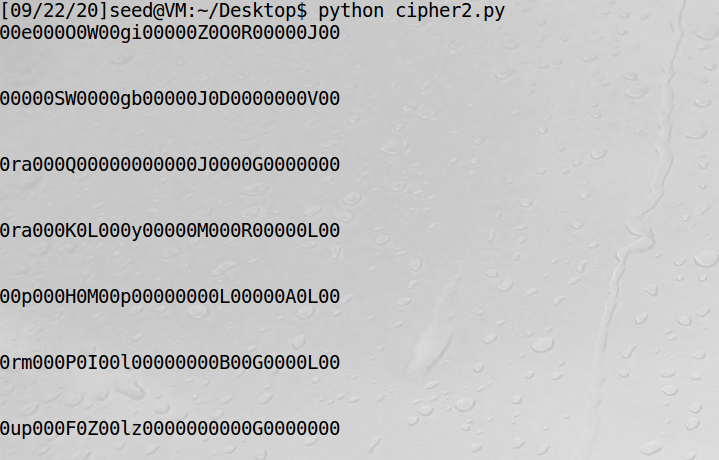
else:

result+='0';

print result;

print '\n'

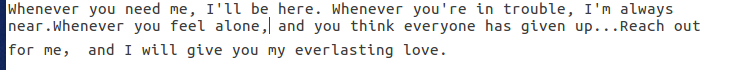
result=''



# Lab1

**Task 1: Frequency Analysis Against Monoalphabetic Substitution Cipher**

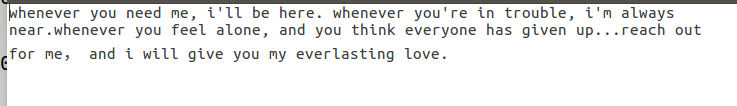
1.首先找一首有大小写交替还有标点的诗歌



输入以下指令



打开“lowercase.txt”

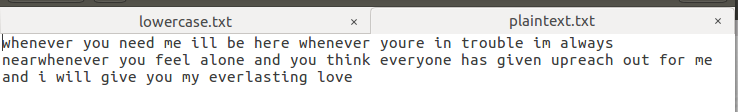


大写变成了小写，但是空格标点保留着。

再输入以下指令：

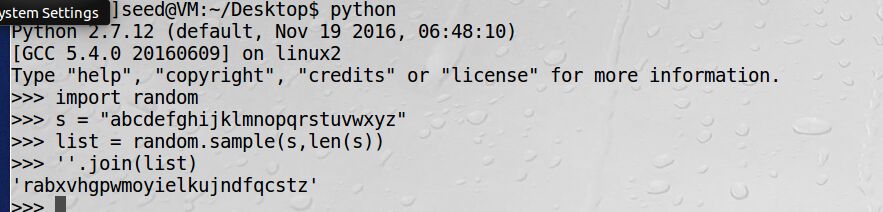


空格保留，标点没有了。



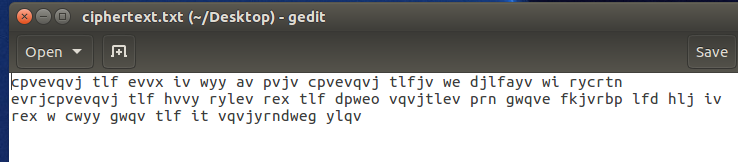
2. let us generate the encryption key, i.e., the substitution table. We will permute the alphabet

from a to z using Python, and use the permuted alphabet as the key. See the following program.



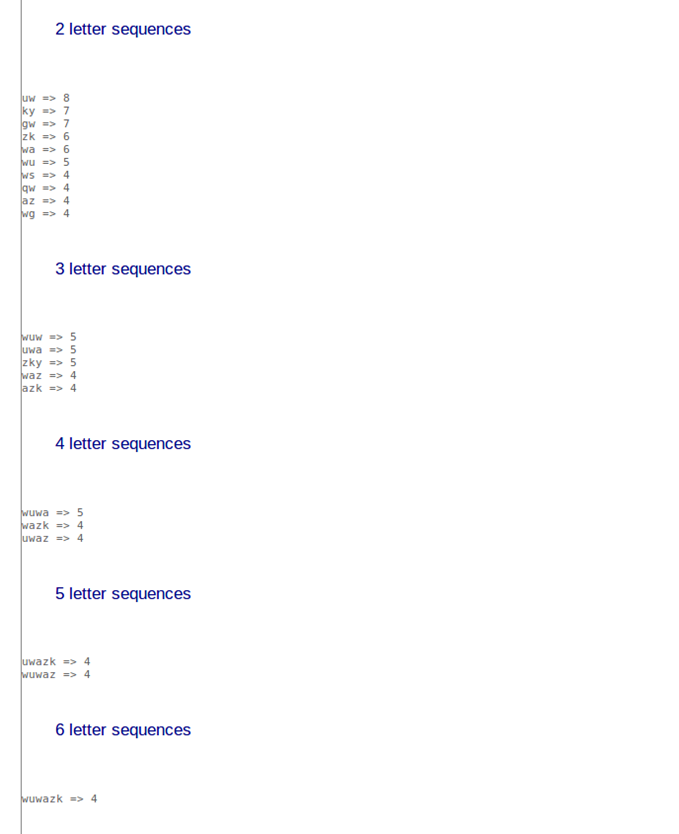
3. we use the tr command to do the encryption. We only encrypt letters, while leaving the space and return characters alone.





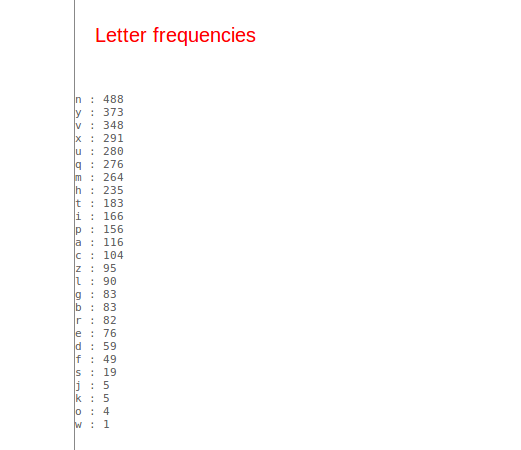
将以上密文放到网站中进行分析，字符频率如下：



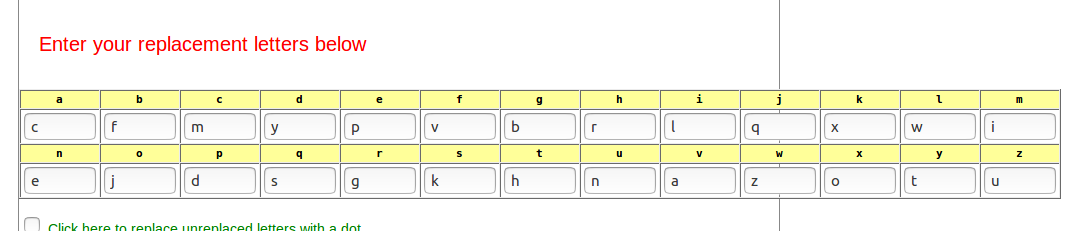


4.解密文

首先将密文输入到网站中去，统计文本个数



对照标准英文文本概率表并进行一步步修改，最后得到以下对应关系：



明文如下：

THE OSCARS TURN ON SUNDAY WHICH SEEMS ABOUT RIGHT AFTER THIS LONG STRANGE AWARDS TRIP THE BAGGER FEELS LIKE A NONAGENARIAN TOO THE AWARDS RACE WAS BOOKENDED BY THE DEMISE OF HARVEY WEINSTEIN AT ITS OUTSET AND THE APPARENT IMPLOSION OF HIS FILM COMPANY AT THE END AND IT WAS SHAPED BY THE EMERGENCE OF METOO TIMES UP BLACKGOWN POLITICS ARMCANDY ACTIVISM AND A NATIONAL CONVERSATION AS BRIEF AND MAD AS A FEVER DREAM ABOUT WHETHER THERE OUGHT TO BE A PRESIDENT WINFREY THE SEASON DIDNT JUST SEEM EXTRA LONG IT WAS EXTRA LONG BECAUSE THE OSCARS WERE MOVED TO THE FIRST WEEKEND IN MARCH TO AVOID CONFLICTING WITH THE CLOSING CEREMONY OF THE WINTER OLYMPICS THANKS PYEONGCHANG ONE BIG QUESTION SURROUNDING THIS YEARS ACADEMY AWARDS IS HOW OR IF THE CEREMONY WILL ADDRESS METOO ESPECIALLY AFTER THE GOLDEN GLOBES WHICH BECAME A JUBILANT COMINGOUT PARTY FOR TIMES UP THE MOVEMENT SPEARHEADED BY POWERFUL HOLLYWOOD WOMEN WHO HELPED RAISE MILLIONS OF DOLLARS TO FIGHT SEXUAL HARASSMENT AROUND THE COUNTRY SIGNALING THEIR SUPPORT GOLDEN GLOBES ATTENDEES SWATHED THEMSELVES IN BLACK SPORTED LAPEL PINS AND SOUNDED OFF ABOUT SEXIST POWER IMBALANCES FROM THE RED CARPET AND THE STAGE ON THE AIR E WAS CALLED OUT ABOUT PAY INEQUITY AFTER ITS FORMER ANCHOR CATT SADLER QUIT ONCE SHE LEARNED THAT SHE WAS MAKING FAR LESS THAN A MALE COHOST AND DURING THE CEREMONY NATALIE PORTMAN TOOK A BLUNT AND SATISFYING DIG AT THE ALLMALE ROSTER OF NOMINATED DIRECTORS HOW COULD THAT BE TOPPED AS IT TURNS OUT AT LEAST IN TERMS OF THE OSCARS IT PROBABLY WONT BE WOMEN INVOLVED IN TIMES UP SAID THAT ALTHOUGH THE GLOBES SIGNIFIED THE INITIATIVES LAUNCH THEY NEVER INTENDED IT TO BE JUST AN AWARDS SEASON CAMPAIGN OR ONE THAT BECAME ASSOCIATED ONLY WITH REDCARPET ACTIONS INSTEAD A SPOKESWOMAN SAID THE GROUP IS WORKING BEHIND CLOSED DOORS AND HAS SINCE AMASSED MILLION FOR ITS LEGAL DEFENSE FUND WHICH AFTER THE GLOBES WAS FLOODED WITH THOUSANDS OF DONATIONS OF OR LESS FROM PEOPLE IN SOME COUNTRIES NO CALL TO WEAR BLACK GOWNS WENT OUT IN ADVANCE OF THE OSCARS THOUGH THE MOVEMENT WILL ALMOST CERTAINLY BE REFERENCED BEFORE AND DURING THE CEREMONY ESPECIALLY SINCE VOCAL METOO SUPPORTERS LIKE ASHLEY JUDD LAURA DERN AND NICOLE KIDMAN ARE SCHEDULED PRESENTERS ANOTHER FEATURE OF THIS SEASON NO ONE REALLY KNOWS WHO IS GOING TO WIN BEST PICTURE ARGUABLY THIS HAPPENS A LOT OF THE TIME INARGUABLY THE NAILBITER NARRATIVE ONLY SERVES THE AWARDS HYPE MACHINE BUT OFTEN THE PEOPLE FORECASTING THE RACE SOCALLED OSCAROLOGISTS CAN MAKE ONLY EDUCATED GUESSES THE WAY THE ACADEMY TABULATES THE BIG WINNER DOESNT HELP IN EVERY OTHER CATEGORY THE NOMINEE WITH THE MOST VOTES WINS BUT IN THE BEST PICTURE CATEGORY VOTERS ARE ASKED TO LIST THEIR TOP MOVIES IN PREFERENTIAL ORDER IF A MOVIE GETS MORE THAN PERCENT OF THE FIRSTPLACE VOTES IT WINS WHEN NO MOVIE MANAGES THAT THE ONE WITH THE FEWEST FIRSTPLACE VOTES IS ELIMINATED AND ITS VOTES ARE REDISTRIBUTED TO THE MOVIES THAT GARNERED THE ELIMINATED BALLOTS SECONDPLACE VOTES AND THIS CONTINUES UNTIL A WINNER EMERGES IT IS ALL TERRIBLY CONFUSING BUT APPARENTLY THE CONSENSUS FAVORITE COMES OUT AHEAD IN THE END THIS MEANS THAT ENDOFSEASON AWARDS CHATTER INVARIABLY INVOLVES TORTURED SPECULATION ABOUT WHICH FILM WOULD MOST LIKELY BE VOTERS SECOND OR THIRD FAVORITE AND THEN EQUALLY TORTURED CONCLUSIONS ABOUT WHICH FILM MIGHT PREVAIL IN IT WAS A TOSSUP BETWEEN BOYHOOD AND THE EVENTUAL WINNER BIRDMAN IN WITH LOTS OF EXPERTS BETTING ON THE REVENANT OR THE BIG SHORT THE PRIZE WENT TO SPOTLIGHT LAST YEAR NEARLY ALL THE FORECASTERS DECLARED LA LA LAND THE PRESUMPTIVE WINNER AND FOR TWO AND A HALF MINUTES THEY WERE CORRECT BEFORE AN ENVELOPE SNAFU WAS REVEALED AND THE RIGHTFUL WINNER MOONLIGHT WAS CROWNED THIS YEAR AWARDS WATCHERS ARE UNEQUALLY DIVIDED BETWEEN THREE BILLBOARDS OUTSIDE EBBING MISSOURI THE FAVORITE AND THE SHAPE OF WATER WHICH IS THE BAGGERS PREDICTION WITH A FEW FORECASTING A HAIL MARY WIN FOR GET OUT BUT ALL OF THOSE FILMS HAVE HISTORICAL OSCARVOTING PATTERNS AGAINST THEM THE SHAPE OF WATER HAS NOMINATIONS MORE THAN ANY OTHER FILM AND WAS ALSO NAMED THE YEARS BEST BY THE PRODUCERS AND DIRECTORS GUILDS YET IT WAS NOT NOMINATED FOR A SCREEN ACTORS GUILD AWARD FOR BEST ENSEMBLE AND NO FILM HAS WON BEST PICTURE WITHOUT PREVIOUSLY LANDING AT LEAST THE ACTORS NOMINATION SINCE BRAVEHEART IN THIS YEAR THE BEST ENSEMBLE SAG ENDED UP GOING TO THREE BILLBOARDS WHICH IS SIGNIFICANT BECAUSE ACTORS MAKE UP THE ACADEMYS LARGEST BRANCH THAT FILM WHILE DIVISIVE ALSO WON THE BEST DRAMA GOLDEN GLOBE AND THE BAFTA BUT ITS FILMMAKER MARTIN MCDONAGH WAS NOT NOMINATED FOR BEST DIRECTOR AND APART FROM ARGO MOVIES THAT LAND BEST PICTURE WITHOUT ALSO EARNING BEST DIRECTOR NOMINATIONS ARE FEW AND FAR BETWEEN

将以上明文编辑成文本，然后输入



明文如下：

the oscars turn on sunday which seems about right after this long strange awards trip the bagger feels like a nonagenarian too the awards race was bookended by the demise of harvey weinstein at its outset and the apparent implosion of his film company at the end and it was shaped by the emergence of metoo times up blackgown politics armcandy activism and a national conversation as brief and mad as a fever dream about whether there ought to be a president winfrey the season didnt just seem extra long it was extra long because the oscars were moved to the first weekend in march to avoid conflicting with the closing ceremony of the winter olympics thanks pyeongchang one big question surrounding this years academy awards is how or if the ceremony will address metoo especially after the golden globes which became a jubilant comingout party for times up the movement spearheaded by powerful hollywood women who helped raise millions of dollars to fight sexual harassment around the country signaling their support golden globes attendees swathed themselves in black sported lapel pins and sounded off about sexist power imbalances from the red carpet and the stage on the air e was called out about pay inequity after its former anchor catt sadler quit once she learned that she was making far less than a male cohost and during the ceremony natalie portman took a blunt and satisfying dig at the allmale roster of nominated directors how could that be topped as it turns out at least in terms of the oscars it probably wont be women involved in times up said that although the globes signified the initiatives launch they never intended it to be just an awards season campaign or one that became associated only with redcarpet actions instead a spokeswoman said the group is working behind closed doors and has since amassed million for its legal defense fund which after the globes was flooded with thousands of donations of or less from people in some countries no call to wear black gowns went out in advance of the oscars though the movement will almost certainly be referenced before and during the ceremony especially since vocal metoo supporters like ashley judd laura dern and nicole kidman are scheduled presenters another feature of this season no one really knows who is going to win best picture arguably this happens a lot of the time inarguably the nailbiter narrative only serves the awards hype machine but often the people forecasting the race socalled oscarologists can make only educated guesses the way the academy tabulates the big winner doesnt help in every other category the nominee with the most votes wins but in the best picture category voters are asked to list their top movies in preferential order if a movie gets more than percent of the firstplace votes it wins when no movie manages that the one with the fewest firstplace votes is eliminated and its votes are redistributed to the movies that garnered the eliminated ballots secondplace votes and this continues until a winner emerges it is all terribly confusing but apparently the consensus favorite comes out ahead in the end this means that endofseason awards chatter invariably involves tortured speculation about which film would most likely be voters second or third favorite and then equally tortured conclusions about which film might prevail in it was a tossup between boyhood and the eventual winner birdman in with lots of experts betting on the revenant or the big short the prize went to spotlight last year nearly all the forecasters declared la la land the presumptive winner and for two and a half minutes they were correct before an envelope snafu was revealed and the rightful winner moonlight was crowned this year awards watchers are unequally divided between three billboards outside ebbing missouri the favorite and the shape of water which is the baggers prediction with a few forecasting a hail mary win for get out but all of those films have historical oscarvoting patterns against them the shape of water has nominations more than any other film and was also named the years best by the producers and directors guilds yet it was not nominated for a screen actors guild award for best ensemble and no film has won best picture without previously landing at least the actors nomination since braveheart in this year the best ensemble sag ended up going to three billboards which is significant because actors make up the academys largest branch that film while divisive also won the best drama golden globe and the bafta but its filmmaker martin mcdonagh was not nominated for best director and apart from argo movies that land best picture without also earning best director nominations are few and far between

# 实验感想

本次实验是关于密码学的内容，主要讲了单表代换和简单的多表代换等一些基础知识。在实验的基础上让我对上学期密码学课程有了更深的认识，并且能够进行实践。在实验过程中也遇到了许多困难，比如，代码编写问题以及字符频率对照问题，在对长篇的密文进行解密时还是花费了很多时间。但是这是实训课程的一个重要实践，让我感触很深。