中南大學

CENTRAL SOUTH UNIVERSITY

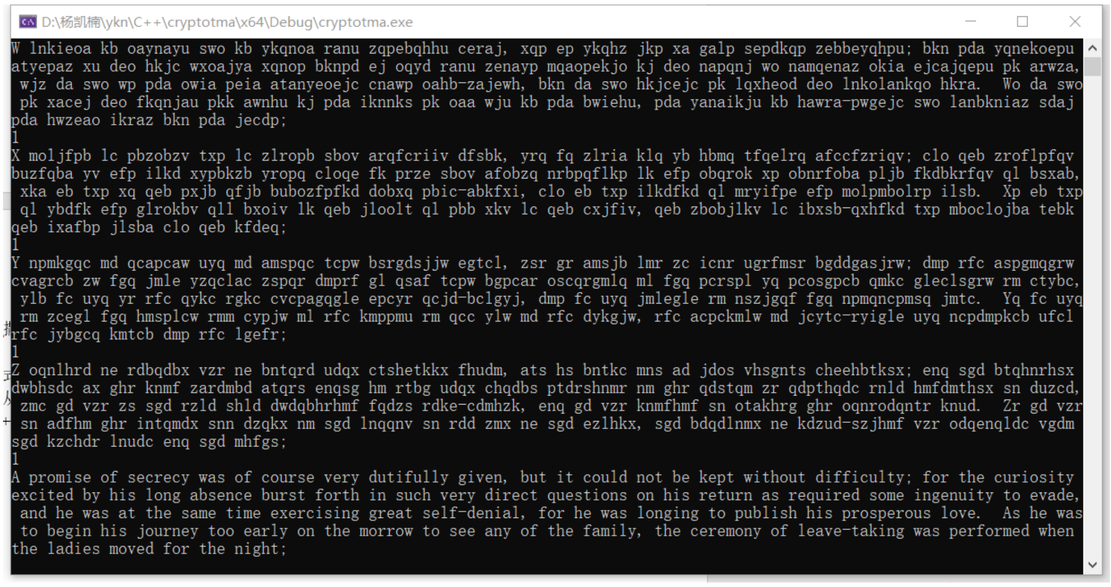
密码学与应用

实验报告(古典密码部分)

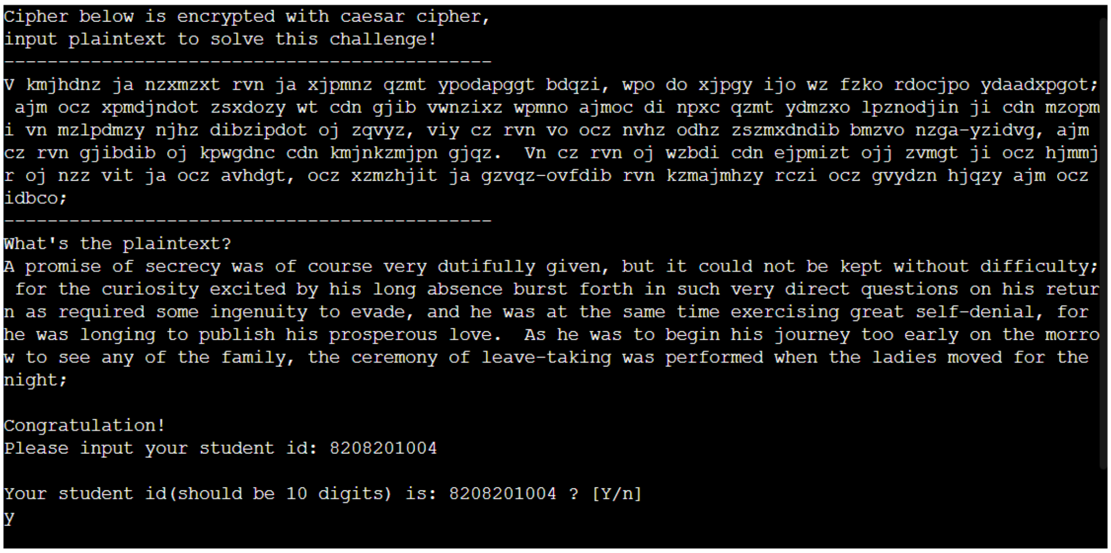
学生姓名	**杨凯楠**
学　　号	8208201004
专业班级	**信息安全 2002 班**
指导教师	段桂华
学　　院	计算机学院
完成时间	2021 年 12 月 1 日

一、　凯撒密码

攻击方式：本试验较为简单，只需要对密码进行移位就可，因为比较简单所以我设置为了移位长度从零开始移位，肉眼识别是否成功的方法，成功就结束，不成功移位长度加一。语言采用 C++。



```
W lnkieoa kb oaynayu swo kb ykqnoa ranu zqpebqhhu ceraj, xqp ep ykqhz jkp xa galp sepdkqp zebbeyqhpu; bkn pda yqnekoepu
atyepaz xu deo hkjc wxoajya xqnop bknpd ej oqyd ranu zenayp mqaopekjo kj deo napqnj wo namqenaz okia ejcajqepu pk arwza,
 wjz da swo wp pda owia peia atanyeoejc cnawp oahb-zajewh, bkn da swo hkjcejc pk lqxheod deo lnkolankqo hkra.  Wo da swo
 pk xacej deo fkqnjau pkk awnhu kj pda iknnks pk oaa wju kb pda bwiehu, pda yanaikju kb hawra-pwgejc swo lanbkniaz sdaj
pda hwzeao ikraz bkn pda jecdp;
1
X moljfpb lc pbzobzv txp lc zlropb sbov arqfcriiv dfsbk, yrq fq zlria klq yb hbmq tfqelrq afccfzriqv; clo qeb zroflpfqv
buzfqba yv efp ilkd xypbkzb yropq cloqe fk prze sbov afobzq nrbpqflkp lk efp obqrok xp obnrfoba pljb fkdbkrfqv ql bsxab,
 xka eb txp xq qeb pxjb qfjb bubozfpfkd dobxq pbic-abkfxi, clo eb txp ilkdfkd ql mryifpe efp molpmbolrp ilsb.  Xp eb txp
 ql ybdfk efp glrokbv qll bxoiv lk qeb jloolt ql pbb xkv lc qeb cxjfiv, qeb zbobjlkv lc ibxsb-qxhfkd txp mboclojba tebk
qeb ixafbp jlsba clo qeb kfdeq;
1
Y npmkgqc md qcapcaw uyq md amspqc tcpw bsrgdsjjw egtcl, zsr gr amsjb lmr zc icnr ugrfmsr bgddgasjrw; dmp rfc aspgmqgrw
cvagrcb zw fgq jmle yzqclac zspqr dmprf gl qsaf tcpw bgpcar oscqrgmlq ml fgq pcrspl yq pcosgpcb qmkc gleclsgrw rm ctybc,
 ylb fc uyq yr rfc qykc rgkc cvcpagqgle epcyr qcjd-bclgyj, dmp fc uyq jmlegle rm nszjgqf fgq npmqncpmsq jmtc.  Yq fc uyq
 rm zcegl fgq hmsplcw rmm cypjw ml rfc kmppmu rm qcc ylw md rfc dykgjw, rfc acpckmlw md jcytc-ryigle uyq ncpdmpkcb ufcl
rfc jybgcq kmtcb dmp rfc lgefr;
1
Z oqnlhrd ne rdbqdbx vzr ne bntqrd udqx ctshetkkx fhudm, ats hs bntkc mns ad jdos vhsgnts cheehbtksx; enq sgd btqhnrhsx
dwbhsdc ax ghr knmf zardmbd atqrs enqsg hm rtbg udqx chqdbs ptdrshnmr nm ghr qdstqm zr qdpthqdc rnld hmfdmthsx sn duzcd,
 zmc gd vzr zs sgd rzld shld dwdqbhrhmf fqdzs rdke-cdmhzk, enq gd vzr knmfhmf sn otakhrg ghr oqnrodqntr knud.  Zr gd vzr
 sn adfhm ghr intqmdx snn dzqkx nm sgd lnqqnv sn rdd zmx ne sgd ezlhkx, sgd bdqdlnmx ne kdzud-szjhmf vzr odqenqldc vgdm
sgd kzchdr lnudc enq sgd mhfgs;
1
A promise of secrecy was of course very dutifully given, but it could not be kept without difficulty; for the curiosity
excited by his long absence burst forth in such very direct questions on his return as required some ingenuity to evade,
 and he was at the same time exercising great self-denial, for he was longing to publish his prosperous love.  As he was
 to begin his journey too early on the morrow to see any of the family, the ceremony of leave-taking was performed when
the ladies moved for the night;
```



```
Cipher below is encrypted with caesar cipher,
input plaintext to solve this challenge!
---------------------------------------------
V kmjhdnz ja nzxmzxt rvn ja xjpmnz qzmt ypodapgt bdqzi, wpo do xjpgy ijo wz fzko rdocjpo ydaadxpgot;
 ajm ocz xpmdjndot zsxdozy wt cdn gjib vwnzixz wpmno ajmoc di npxc qzmt ydmzxo lpznodjin ji cdn mzopm
i vn mzlpdmzy njhz dibzipdot oj zqvyz, viy cz rvn vo ocz nvhz odhz zszmxdndib bmzvo nzga-yzidvg, ajm
cz rvn gjibdib oj kpwgdnc cdn kmjnkzmjpn gjqz.  Vn cz rvn oj wzbdi cdn ejpmizt ojj zvmgt ji ocz hjmmj
r oj nzz vit ja ocz avhdgt, ocz xzmzhjit ja gzvqz-ovfdib rvn kzmajmhzy rczi ocz gvydzn hjqzy ajm ocz
idbco;
---------------------------------------------
What's the plaintext?
A promise of secrecy was of course very dutifully given, but it could not be kept without difficulty;
 for the curiosity excited by his long absence burst forth in such very direct questions on his retur
n as required some ingenuity to evade, and he was at the same time exercising great self-denial, for
he was longing to publish his prosperous love.  As he was to begin his journey too early on the morro
w to see any of the family, the ceremony of leave-taking was performed when the ladies moved for the
night;

Congratulation!
Please input your student id: 8208201004

Your student id(should be 10 digits) is: 8208201004 ? [Y/n]
y
```

代码：

```
#include<iostream>
#include<string>
using namespace std;
int main(void) {
    string str = “  ”;
    int i = 0, j = 1, key;
    cin >> key;
    while (key == 1 && j < 26) {
        while (str[i] != '\0') {
            if (str[i] >= 'a' && str[i] <= 'z')
```

```
                cout << char((str[i] - 'a' + j) % 26 + 'a');
            else if ((str[i] >= 'A' && str[i] <= 'Z'))
                cout << char((str[i] - 'A' + j) % 26 + 'A');
            else
                cout << str[i];
            i++;
        }
        j++;
        i = 0;
        cout << endl;
        cin >> key;
    }
    return 0;
}
```

二、　仿射密码

仿射密码也是一类经典的古典密码，通常加密方式为将字符映射到数字后计算

c=m*a+b mod n　$c=m*a+b \bmod n$,

再对应回字母表表示密文，解密则使用

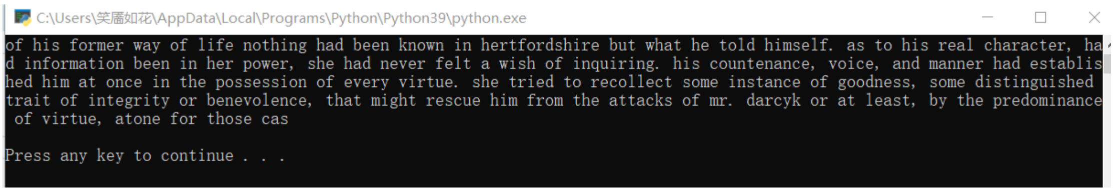
m=(c-b)*a^{-1} mod n　$m=(c-b)*a^{-1} \bmod n$

移位密码可以看做 a=1$a=1$ 的仿射密码。

现已知字母表为"abcdefghijklmnopqrstuvwxyz .,"，分别对应 0~28，连接服务器，获得密文后向服务器输入对应的明文（空格也要附上）。

分析：从本题以后的题我都是用 python 写的，本道题中，首先进行字母数字转换，将字母标点对应成相应的数字，然后对其所有 311 个秘钥空间进行爆破攻击，在判断是否攻击成功时，我采用了“e”字母频率初步判断外加关键字匹配方式辅助的方法。取得了不错的攻击效果。在求逆元的时候使用了 gmpy2 库，初步认识到了这一库的强大之处。

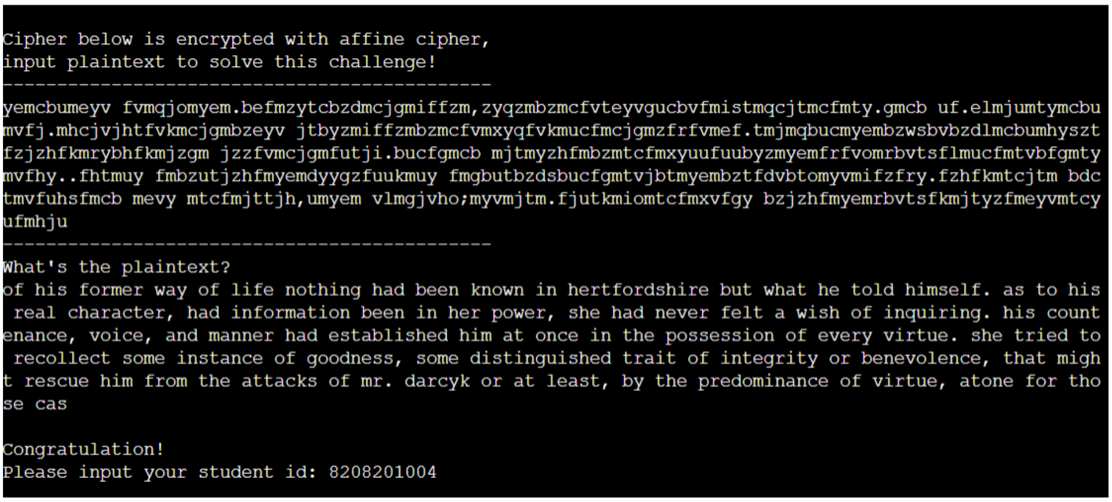
结果：



C:\Users\笑靥如花\AppData\Local\Programs\Python\Python39\python.exe

```
of his former way of life nothing had been known in hertfordshire but what he told himself. as to his real character, ha
d information been in her power, she had never felt a wish of inquiring. his countenance, voice, and manner had establis
hed him at once in the possession of every virtue. she tried to recollect some instance of goodness, some distinguished
trait of integrity or benevolence, that might rescue him from the attacks of mr. darcyk or at least, by the predominance
 of virtue, atone for those cas

Press any key to continue . . .
```



```
Cipher below is encrypted with affine cipher,
input plaintext to solve this challenge!
---------------------------------------------
yemcbumeyv fvmqjomyem.befmzytcbzdmcjgmiffzm,zyqzmbzmcfvteyvgucbvfmistmqcjtmcfmty.gmcb uf.elmjumtymcbu
mvfj.mhcjvjhtfvkmcjgmbzeyv jtbyzmiffzmbzmcfvmxyqfvkmucfmcjgmzfrfvmef.tmjmqbucmyembzwsbvbzdlmcbumhyszt
fzjzhfkmrybhfkmjzgm jzzfvmcjgmfutji.bucfgmcb mjtmyzhfmbzmtcfmxyuufuubyzmyemfrfvomrbvtsflmucfmtvbfgmty
mvfhy..fhtmuy fmbzutjzhfmyemdyygzfuukmuy fmgbutbzdsbucfgmtvjbtmyembztfdvbtomyvmifzfry.fzhfkmtcjtm bdc
tmvfuhsfmcb mevy mtcfmjttjh,umyem vlmgjvho;myvmjtm.fjutkmiomtcfmxvfgy bzjzhfmyemrbvtsfkmjtyzfmeyvmtcy
ufmhju
---------------------------------------------
What's the plaintext?
of his former way of life nothing had been known in hertfordshire but what he told himself. as to his
 real character, had information been in her power, she had never felt a wish of inquiring. his count
enance, voice, and manner had established him at once in the possession of every virtue. she tried to
 recollect some instance of goodness, some distinguished trait of integrity or benevolence, that migh
t rescue him from the attacks of mr. darcyk or at least, by the predominance of virtue, atone for tho
se cas

Congratulation!
Please input your student id: 8208201004
```

关键代码：

攻击：

```python
count=0
for b in range(0,29):
    for a in range(2,29):
        count=0
        nia=gmpy2.invert(a,29)
        for c in C:
            P.append(((c-b)*nia)%29)
        for c in P:
            if c==(ord('e')-97):
                count+=1
        if count/lenstr>0.08:
            printff()
        P.clear()
```

三、列移位攻击

分析：在列移位密码中，首先将明文写入给定尺寸的网格中，然后以密钥中给定的模式读出。

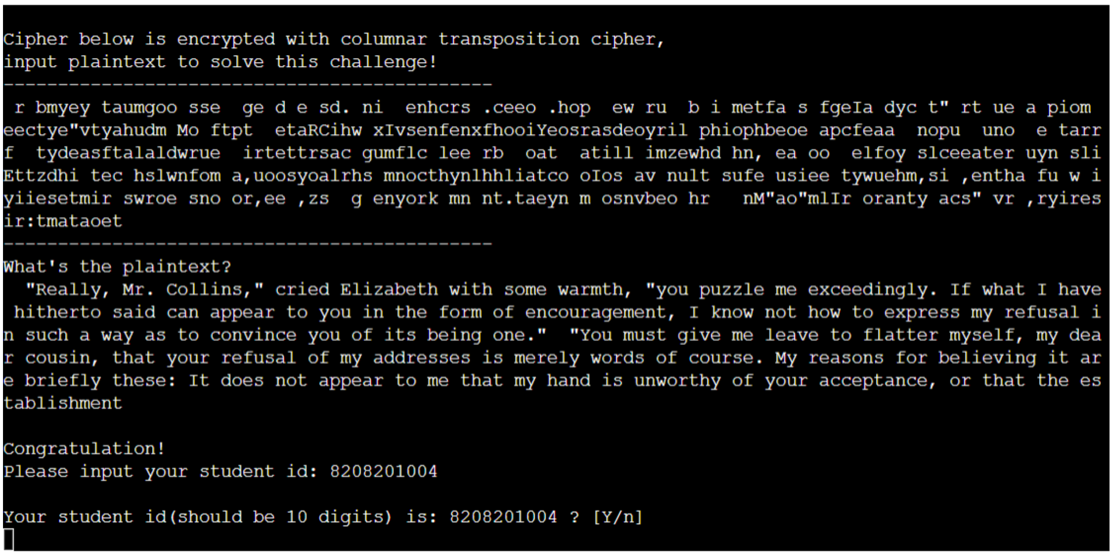
如有明文 WEAREDISCOVEREDFLEEATONCE，并用密钥 3 进行加密，则首先将信息写为（竖着写）

```
W R I O R F E O E
E E S V E L A N J
A D C E D E T C X
```

然后将信息横着读出，得到 WRIORFEOEEESVELANJADCEDETCX，即是最后的密文。（字符不足时会补空格）

本道题由于网页所给形式的问题，我并不知道在密文最后一个字母后面是否还跟随有空格，所以我查看了源码，才发现，源码中根本没有考虑空格的形式，而是直接将情况达到了完美状态：都是标准的矩形，没有空缺。这也是我给学长提的意见之一。针对这种方式我设计了

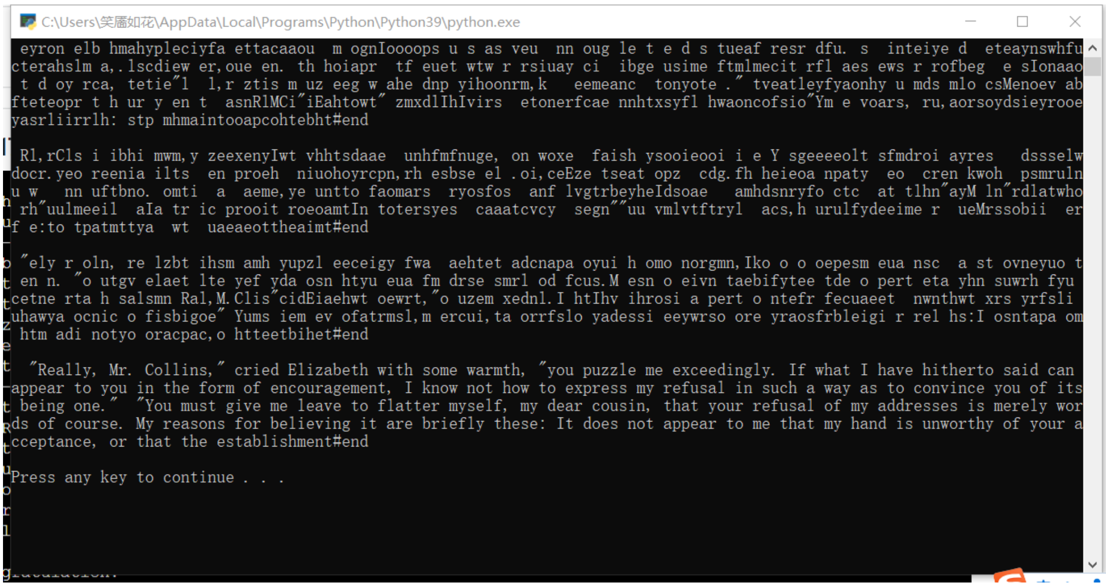
简便的攻击方式，那便是计算密文长度，然后根据密文长度的因子进行攻击，简便快捷。



```
Cipher below is encrypted with columnar transposition cipher,
input plaintext to solve this challenge!
---------------------------------------------
 r bmyey taumgoo sse  ge d e sd. ni  enhcrs .ceeo .hop  ew ru  b i metfa s fgeIa dyc t" rt ue a piom
eectye"vtyahudm Mo ftpt  etaRCihw xIvsenfenxfhooiYeosrasdeoyril phiophbeoe apcfeaa  nopu  uno  e tarr
f  tydeasftalaldwrue  irtettrsac gumflc lee rb  oat  atill imzewhd hn, ea oo  elfoy slceeater uyn sli
Ettzdhi tec hslwnfom a,uoosyoalrhs mnocthynlhhliatco oIos av nult sufe usiee tywuehm,si ,entha fu w i
yiiesetmir swroe sno or,ee ,zs  g enyork mn nt.taeyn m osnvbeo hr   nM"ao"mlIr oranty acs" vr ,ryires
ir:tmataoet
---------------------------------------------
What's the plaintext?
  "Really, Mr. Collins," cried Elizabeth with some warmth, "you puzzle me exceedingly. If what I have
 hitherto said can appear to you in the form of encouragement, I know not how to express my refusal i
n such a way as to convince you of its being one."  "You must give me leave to flatter myself, my dea
r cousin, that your refusal of my addresses is merely words of course. My reasons for believing it ar
e briefly these: It does not appear to me that my hand is unworthy of your acceptance, or that the es
tablishment

Congratulation!
Please input your student id: 8208201004

Your student id(should be 10 digits) is: 8208201004 ? [Y/n]
```



C:\Users\笑靥如花\AppData\Local\Programs\Python\Python39\python.exe

```
 eyron elb hmahypleciyfa ettacaaou  m ognIoooops u s as veu  nn oug le t e d s tueaf resr dfu. s  inteiye d  eteaynswhfu
cterahslm a,.lscdiew er,oue en. th hoiapr  tf euet wtw r rsiuay ci  ibge usime ftmlmecit rfl aes ews r rofbeg  e sIonaao
 t d oy rca, tetie"l  l,r ztis m uz eeg w ahe dnp yihoonrm,k   eemeanc  tonyote ." tveatleyfyaonhy u mds mlo csMenoev ab
fteteopr t h ur y en t  asnRlMCi"iEahtowt" zmxdlIhIvirs  etonerfcae nnhtxsyfl hwaoncofsio"Ym e voars, ru,aorsoydsieyrooe
yasrliirrlh: stp mhmaintooapcohtebht#end

 Rl,rCls i ibhi mwm,y zeexenyIwt vhhtsdaae  unhfmfnuge, on woxe  faish ysooieooi i e Y sgeeeeolt sfmdroi ayres   dssselw
docr.yeo reenia ilts  en proeh  niuohoyrcpn,rh esbse el .oi,ceEze tseat opz  cdg.fh heieoa npaty  eo  cren kwoh  psmruln
u w   nn uftbno. omti  a  aeme,ye untto faomars  ryosfos  anf lvgtrbeyheIdsoae   amhdsnryfo ctc  at tlhn"ayM ln"rdlatwho
 rh"uulmeeil  aIa tr ic prooit roeoamtIn totersyes  caaatcvcy  segn""uu vmlvtftryl  acs,h urulfydeeime r  ueMrssobii  er
f e:to tpatmttya  wt  uaeaeottheaimt#end

 "ely r oln, re lzbt ihsm amh yupzl eeceigy fwa  aehtet adcnapa oyui h omo norgmn,Iko o o oepesm eua nsc  a st ovneyuo t
 en n. "o utgv elaet lte yef yda osn htyu eua fm drse smrl od fcus.M esn o eivn taebifytee tde o pert eta yhn suwrh fyu
cetne rta h salsmn Ral,M.Clis"cidEiaehwt oewrt,"o uzem xednl.I htIhv ihrosi a pert o ntefr fecuaeet  nwnthwt xrs yrfsli
uhawya ocnic o fisbigoe" Yums iem ev ofatrmsl,m ercui,ta orrfslo yadessi eeywrso ore yraosfrbleigi r rel hs:I osntapa om
 htm adi notyo oracpac,o htteetbihet#end

  "Really, Mr. Collins," cried Elizabeth with some warmth, "you puzzle me exceedingly. If what I have hitherto said can
appear to you in the form of encouragement, I know not how to express my refusal in such a way as to convince you of its
 being one."  "You must give me leave to flatter myself, my dear cousin, that your refusal of my addresses is merely wor
ds of course. My reasons for believing it are briefly these: It does not appear to me that my hand is unworthy of your a
cceptance, or that the establishment#end

Press any key to continue . . .
```

代码：

```python
str='  '
lenstr=len(str)
for a in range(3,13):
    if lenstr%a==0:
        for j in range(0,len(str)//a):
            for i in range(0,a):
                print(str[j+lenstr//a*i],end="")
        print('#end\n')
```

四、维吉尼亚密码

例如，假设明文为：

ATTACKATDAWN

选择某一关键词并重复而得到密钥，如关键词为 LEMON 时，密钥为：

LEMONLEMONLE

对于明文的第一个字母 A，对应密钥的第一个字母 L，于是使用表格中 L 行字母表进行加密，得到密文第一个字母 L。类似地，明文第二个字母为 T，在表格中使用对应的 E 行进行加密，得到密文第二个字母 X。以此类推，可以得到：

明文：ATTACKATDAWN

密钥：LEMONLEMONLE

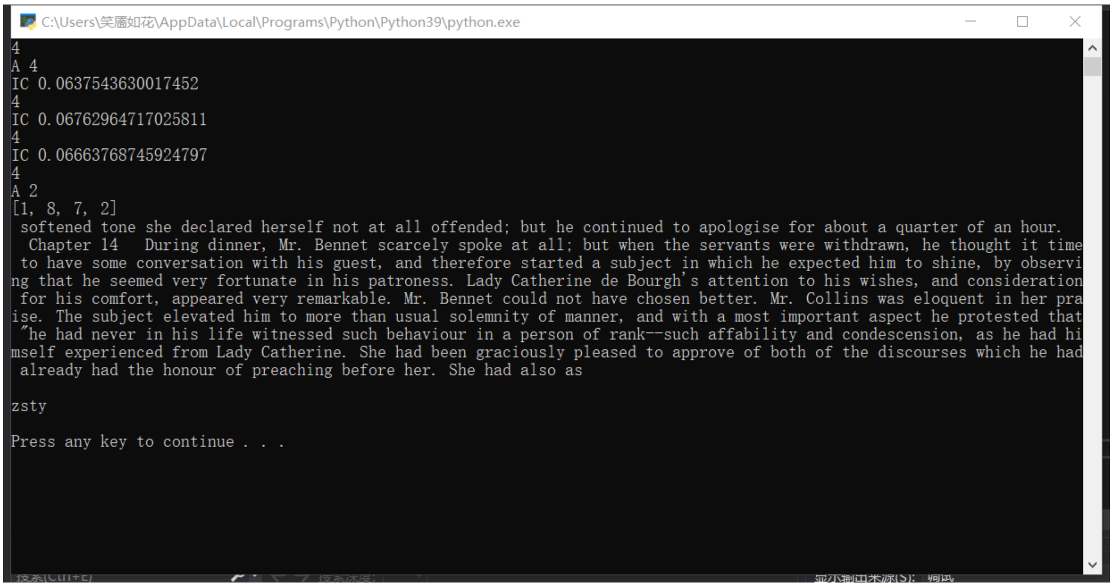
密文：LXFOPVEFRNHR

分析：本实验比较难，难点在于寻找密钥的长度、确定密钥长度后重合指数攻击，参数的选择也是尤为重要的。寻找密钥长度时，我遍历了密文，将所有重复出现的密文片段间的长度计算出其公因子，这就是密钥长度，公因子计算中，采用从头到尾 gcd 函数遍历法求得。求得密钥长度后，再将密文分片，分成密钥长度的片，在维吉尼亚密码中，由于较难使用关键字匹配，所以应用重合指数攻击，重合指数攻击中对 IC 范围极其敏感，稍有偏差便不能破解密文（也可能是我算法问题很多，水平比较低）。重合指数的计算方法：

```
IC+=(CountLetter[i]-1)*CountLetter[i]/(countlen*(countlen-1))
```

代码：[click_here](#) （由于是初学 python 写的代码，并且是零碎时间写的，代码可读性不好）

实现：



C:\Users\笑靥如花\AppData\Local\Programs\Python\Python39\python.exe

```
4
A 4
IC 0.0637543630017452
4
IC 0.06762964717025811
4
IC 0.06663768745924797
4
A 2
[1, 8, 7, 2]
 softened tone she declared herself not at all offended; but he continued to apologise for about a quarter of an hour.
  Chapter 14   During dinner, Mr. Bennet scarcely spoke at all; but when the servants were withdrawn, he thought it time
 to have some conversation with his guest, and therefore started a subject in which he expected him to shine, by observi
ng that he seemed very fortunate in his patroness. Lady Catherine de Bourgh's attention to his wishes, and consideration
 for his comfort, appeared very remarkable. Mr. Bennet could not have chosen better. Mr. Collins was eloquent in her pra
ise. The subject elevated him to more than usual solemnity of manner, and with a most important aspect he protested that
 "he had never in his life witnessed such behaviour in a person of rank--such affability and condescension, as he had hi
mself experienced from Lady Catherine. She had been graciously pleased to approve of both of the discourses which he had
 already had the honour of preaching before her. She had also as

zsty

Press any key to continue . . .
```

五、 多次一次一密

一次一密是不可攻破的，但是协商、传输密钥却是非常头疼的事情，于是就有人考虑多次使用密钥，但是这样是非常危险的！

已知密钥为 50 个字节，明文为英文句子，加密使用的方式是异或，连接服务器，输入学号，并输入根据获取的密文组解密出密钥，并发到服务器。

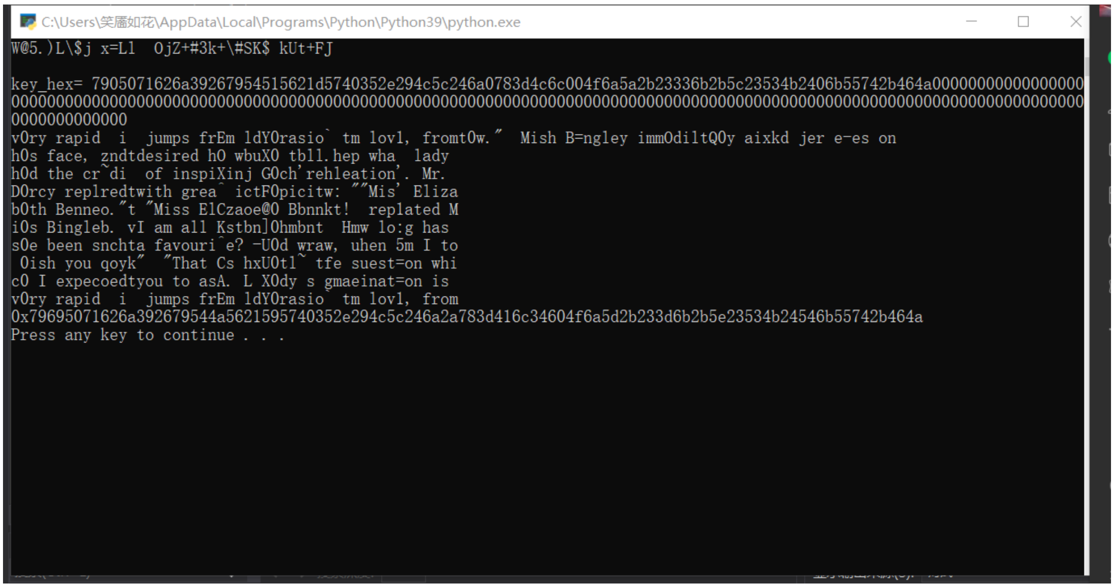
注意，应当发送密钥对应的十六进制编码，如密钥是"31"，则应当发送 3331（3 和 1 的 ascii 码）。

本道题我认为是最难的一道题，甚至难度直接比肩协议题，耗费了大量时间写代码，并且调试良久也没有将参数改合适，只能获得残破的明文，然后对熟悉的单词进行补全，再从老师法的明文来源里找到原文才能 congratulation，可能是我技术太差了吧，还需要不断学习。

程序首先进行双重循环来寻找空字符，每一条密文均与其他密文异或，保存可能的空格符对应的位置，然后还需要进一步判断已记录的位置是否是空字符。

解出“残破的”密钥后，用其对所有密文解密，然后猜测出一组明文，再得出正确的密钥。

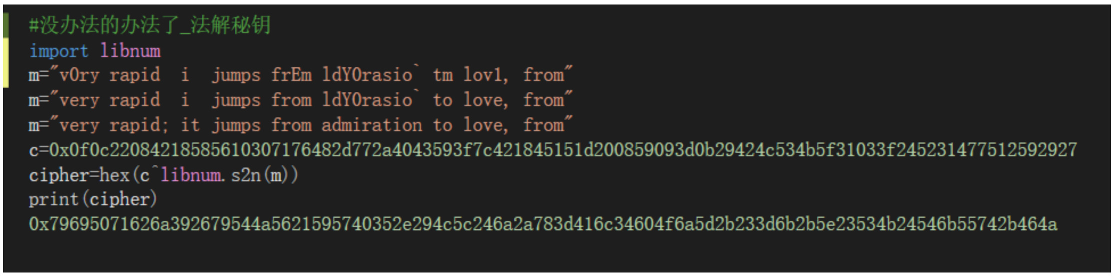
实现：



C:\Users\笑靥如花\AppData\Local\Programs\Python\Python39\python.exe

```
W@5.)L\$j x=L1  0jZ+#3k+\#SK$ kUt+FJ

key_hex= 7905071626a39267954515621d5740352e294c5c246a0783d4c6c004f6a5a2b23336b2b5c23534b2406b55742b464a00000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000
v0ry rapid  i  jumps frEm ldY0rasio` tm lov1, fromt0w.″  Mish B=ngley imm0diltQ0y aixkd jer e-es on
h0s face, zndtdesired h0 wbuX0 tbll.hep wha  lady
h0d the cr˜di  of inspiXinj G0ch'rehleation'. Mr.
D0rcy replredtwith grea` ictF0picitw: ″″Mis' Eliza
b0th Benneo.″t ″Miss ElCzaoe@0 Bbnnkt!  replated M
i0s Bingleb. vI am all Kstbn]0hmbnt  Hmw lo:g has
s0e been snchta favouri`e? -U0d wraw, uhen 5m I to
 0ish you qoyk″  ″That Cs hxU0tl˜ tfe suest=on whi
c0 I expecoedtyou to asA. L X0dy s gmaeinat=on is
v0ry rapid  i  jumps frEm ldY0rasio` tm lov1, from
0x79695071626a392679544a5621595740352e294c5c246a2a783d416c34604f6a5d2b233d6b2b5e23534b24546b55742b464a
Press any key to continue . . .
```



```
#没办法的办法了_法解秘钥
import libnum
m="v0ry rapid  i  jumps frEm ldY0rasio` tm lov1, from"
m="very rapid  i  jumps from ldY0rasio` to love, from"
m="very rapid; it jumps from admiration to love, from"
c=0x0f0c220842185856103071764482d772a4043593f7c421845151d200859093d0b29424c534b5f31033f245231477512592927
cipher=hex(c^libnum.s2n(m))
print(cipher)
0x79695071626a392679544a5621595740352e294c5c246a2a783d416c34604f6a5d2b233d6b2b5e23534b24546b55742b464a
```

代码：**click_here**