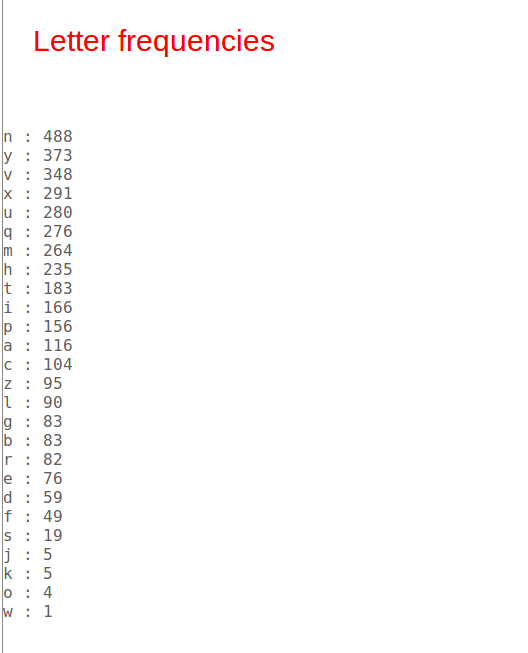
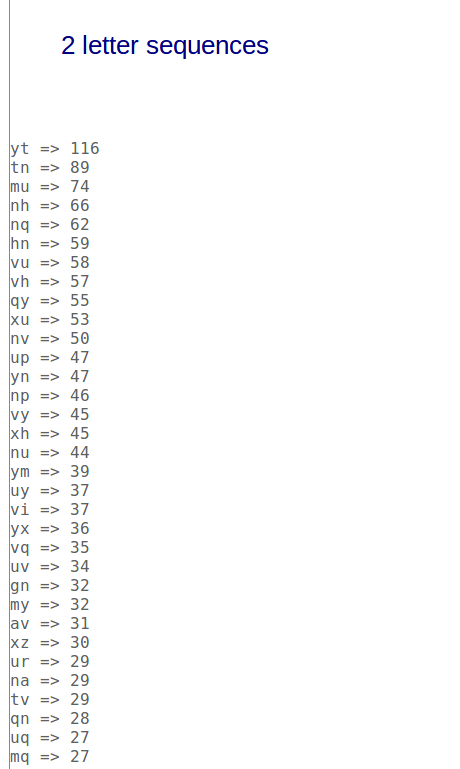
Lab-Report

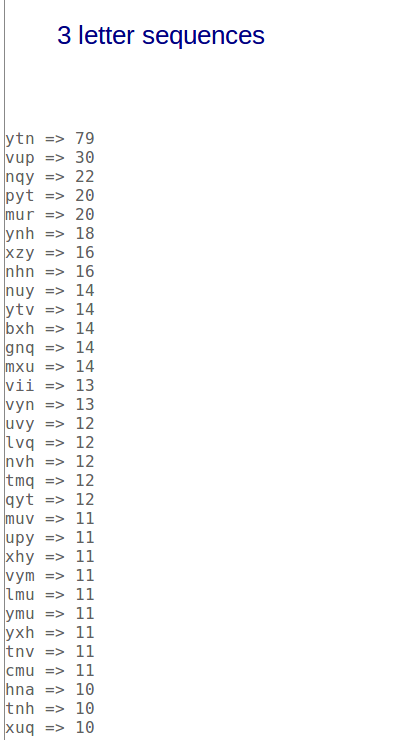
57118103 郭欣然

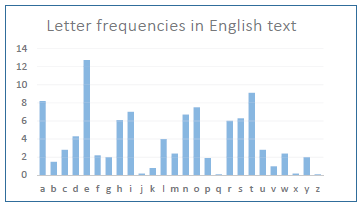
Task1

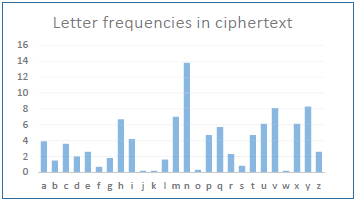
将密文复制到网站<http://www.richkni.co.uk/php/crypta/freq.php>

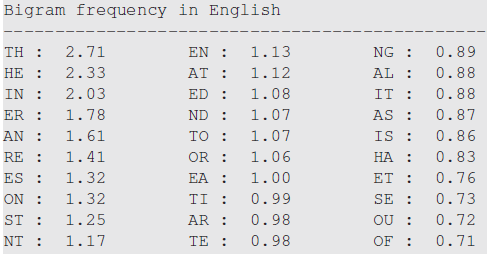
分析密文中字母出现的频率，如图展示了单字母、双字母和三个字母的频次

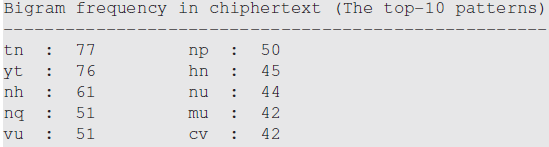


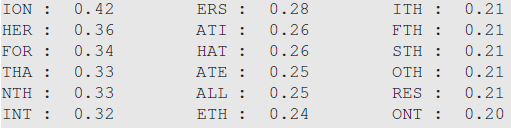
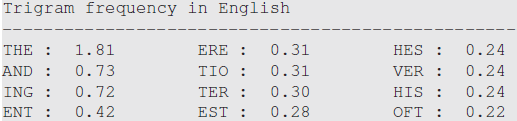


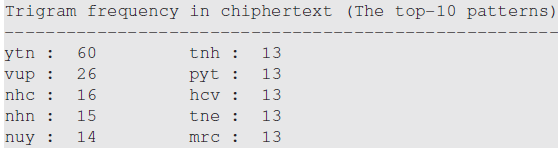
查询标准字母频率











根据单字母频率推测：

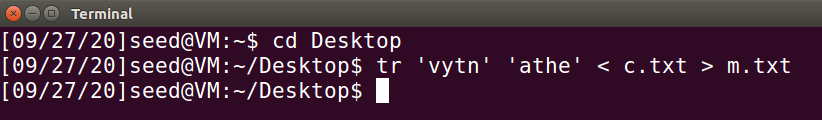
V——>a

根据双字母频率推测：

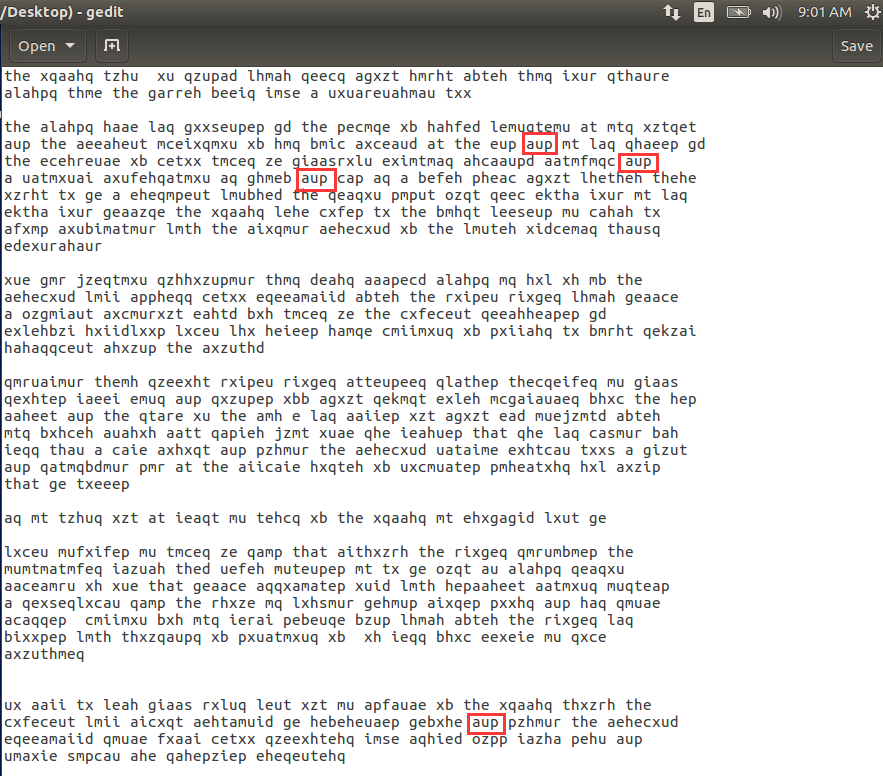
Yt——>th

tn——>he

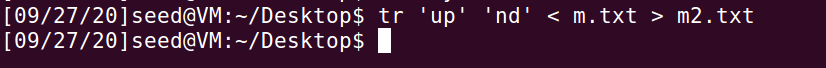
通过命令对txt文档中的v、y、t、n进行替换，结果如下图：

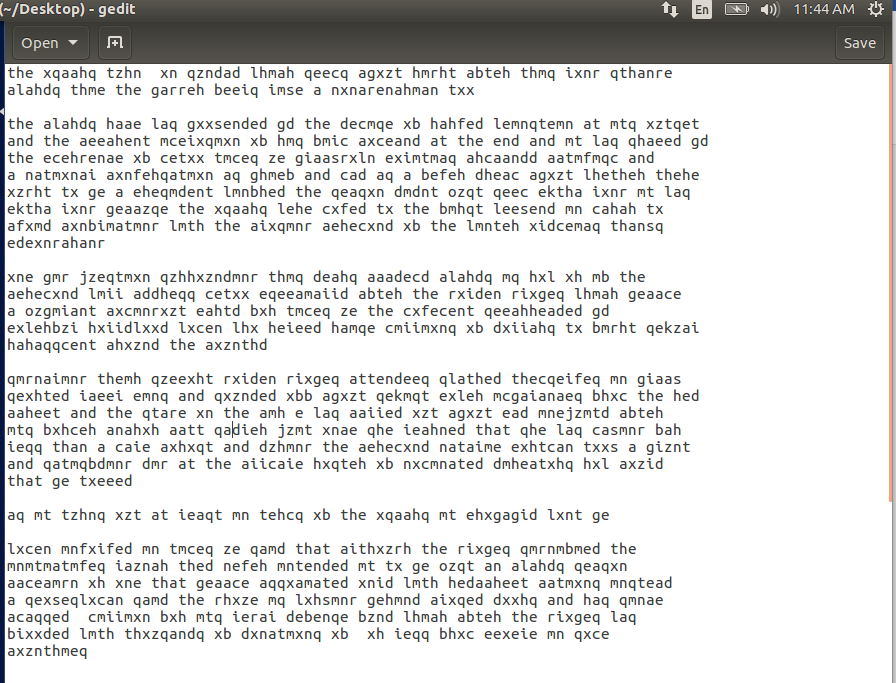


密文中发现许多三字母单词为aup，由于a已经替换过，因此猜测该单词是and，近一步将up替换为nd



vup——>and



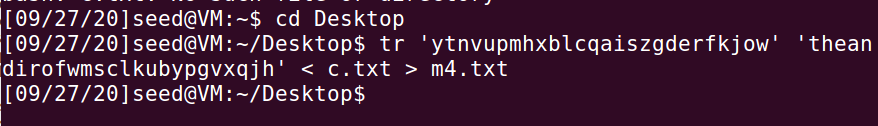


按照以上方法不断尝试进行调整，最终猜测出对应关系为：

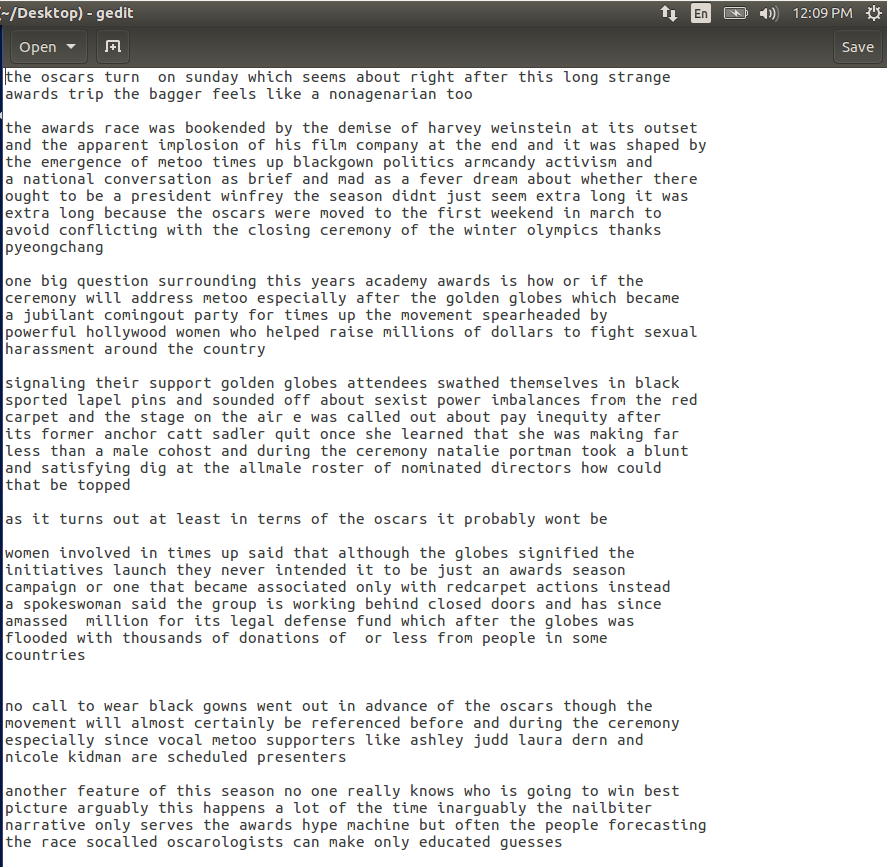
a->c b->f c>m d->y e->p f->v g->b h->r i->l

j->q k->x l->w m->i n->e o->j p->d q->s e->g

s->k t->h u->n v->a w->h x->o y->t z->u



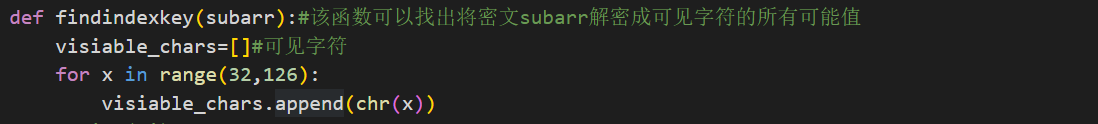
解密后的明文为：

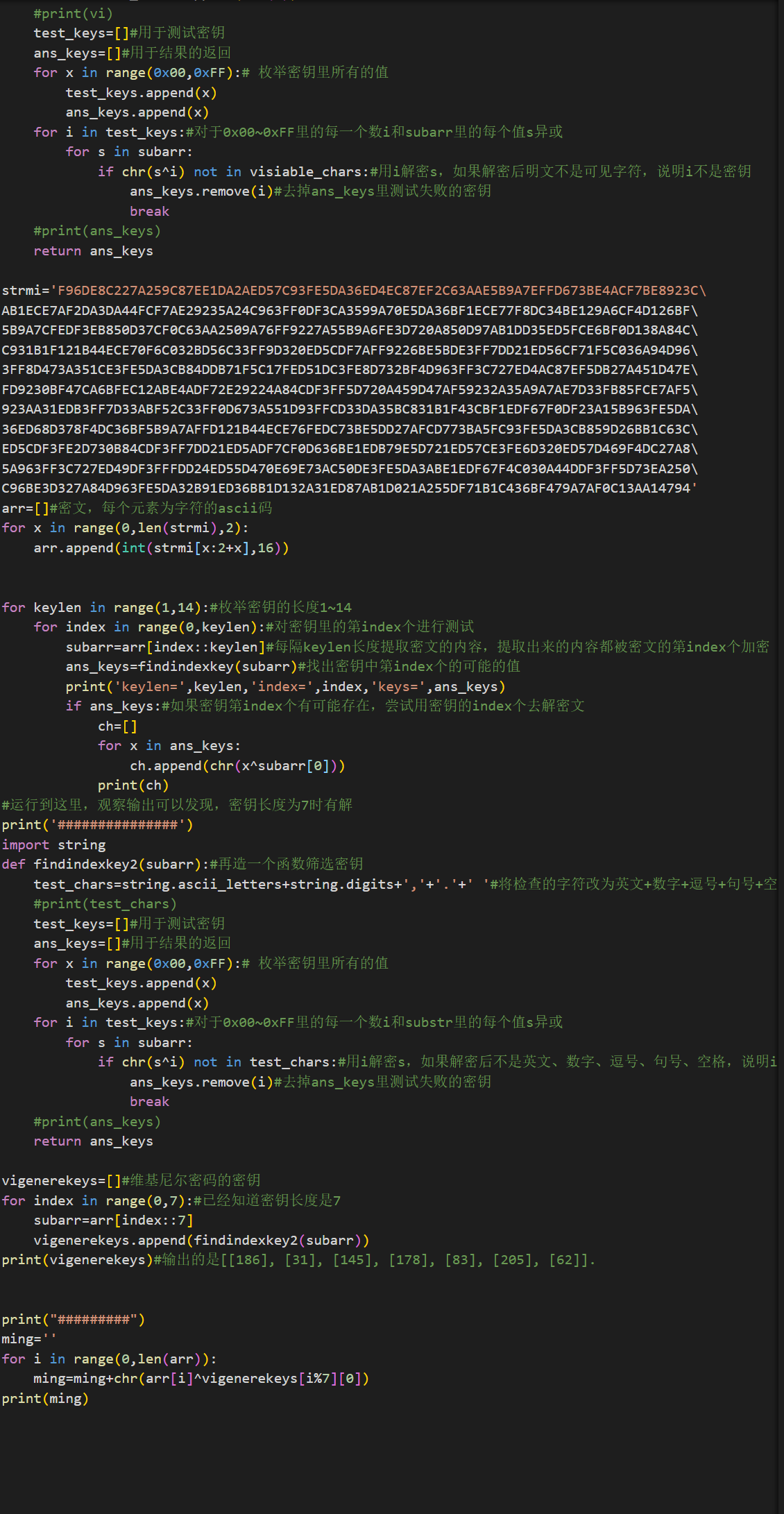


Task2：

1、破解维吉尼亚密码

编写如下代码进行解密：





最终得到的密钥为[186, 31, 145, 178, 83, 205, 62]；

解密得到得明文为：

Cryptography is the practice and study of techniques for, among other things, secure communication in the presence of attackers. Cryptography has been used for hundreds, if not thousands, of years, but traditional cryptosystems were designed and evaluated in a fairly ad hoc manner. For example, the Vigenere encryption scheme was thought to be secure for decades after it was invented, but we now know, and this exercise demonstrates, that it can be broken very easily.

2. 以下密文使用了重复的一次一密密码，请通过异或运算和ASCII码的计算规律破解原始消息。

首先逐个异或各段密文，得到的结果即为明文异或的结果，代码如下：

cipher = ['BB3A65F6F0034FA957F6A767699CE7FABA855AFB4F2B520AEAD612944A801E',

          'BA7F24F2A35357A05CB8A16762C5A6AAAC924AE6447F0608A3D11388569A1E',

          'A67261BBB30651BA5CF6BA297ED0E7B4E9894AA95E300247F0C0028F409A1E',

          'A57261F5F0004BA74CF4AA2979D9A6B7AC854DA95E305203EC8515954C9D0F',

          'BB3A70F3B91D48E84DF0AB702ECFEEB5BC8C5DA94C301E0BECD241954C831E',

          'A6726DE8F01A50E849EDBC6C7C9CF2B2A88E19FD423E0647ECCB04DD4C9D1E',

          'BC7570BBBF1D46E85AF9AA6C7A9CEFA9E9825CFD5E3A0047F7CD009305A71E'

          ]

char\_set = 'qwertyuiopsdfghjklzxcvbnm,. QWERTYUIOPASDFGHJKLZXCVBNM'

cipher\_ascii = []

for i in range(len(cipher)):

    cipher\_ascii.append(bytes.fromhex(cipher[i]))

keys = {}

for m in range(len(cipher\_ascii)):

    plain\_xor = []

    for j in range(len(cipher\_ascii)):

        plain\_xor.append([])

        for c in range(len(cipher\_ascii[j])):

            plain\_xor[j].append(cipher\_ascii[m][c] ^ cipher\_ascii[j][c])

    for i in range(len(plain\_xor[m])):

        space = False

        for j in range(1, len(plain\_xor)):

            if plain\_xor[j][i] > 64:

                space = True

                break

        if space:

            is\_space = True

            for k in range(len(plain\_xor)):

                if k == m:

                    continue

                if plain\_xor[k][i] < 64 and plain\_xor[k][i] != 0:   # 该位不是空格或其他标点

                    is\_space = False

                    break

            if is\_space:

                key = cipher\_ascii[m][i] ^ 32

                print("[+]key at {} is {}".format(i, key))

                keys[i] = key

key = []

for i in range(len(cipher\_ascii[0])):

    if keys.get(i):

        key.append(keys[i])

    else:

        key.append(0)

for c in range(len(cipher\_ascii)):

    plain = ''

    for i in range(len(cipher\_ascii[c])):

        plain += chr(cipher\_ascii[c][i] ^ key[i])

    print(plain)

输出结果如下，获取部分密钥以及破解了部分的明文

key at 1 is 26

key at 4 is 208

key at 13 is 188

key at 15 is 218

key at 22 is 114

key at 2 is 4

key at 5 is 115

key at 9 is 152

key at 14 is 134

key at 21 is 95

key at 24 is 131

key at 3 is 155

key at 11 is 9

key at 16 is 201

key at 19 is 137

key at 23 is 103

key at 4 is 208

key at 11 is 9

key at 14 is 134

key at 19 is 137

key at 22 is 114

key at 25 is 165

key at 1 is 26

key at 7 is 200

key at 12 is 14

key at 19 is 137

key at 26 is 97

key at 4 is 208

key at 7 is 200

key at 13 is 188

key at 18 is 57

key at 23 is 103

key at 27 is 253

key at 3 is 155

key at 7 is 200

key at 13 is 188

key at 16 is 201

key at 23 is 103

key at 28 is 37

» am pOaWn§ng a scrOt missio‑

ºe is Wh\ ¡nly pesoD to trus‑

¦he cuQr\nº plan s ^op secre‑

¥hen sKoLlª we met ^o do thi

» thinH Mh«y shoud Lollow hi‑

¦his iP Iu¼er tha tBat one i‑

¼ot onF Zaªet is et^er than §‑

通过不完全的明文猜测恢复密钥，得出密钥为：

key = [242, 26, 4, 155, 208, 115, 35, 200, 57, 152, 206, 9, 14, 188, 134, 218, 201, 224, 57, 137, 42, 95, 114, 103, 131,165, 97, 253, 37, 238, 48]

最终恢复出的明文为：

I am planning a secret mission.

He is the only person to trust.

The current plan is top secret.

When should we meet to do this?

I think they should follow him.

This is purer than that one is.

Not one cadet is better than I.