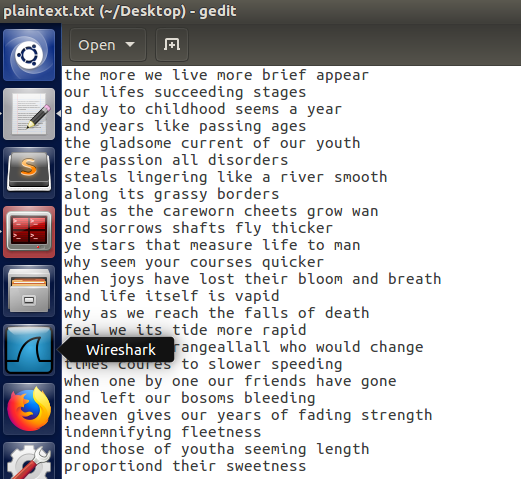
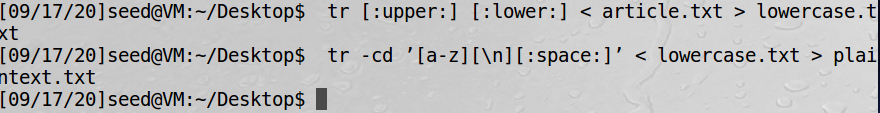
Secret-Key Encryption Lab

57118138 李嘉怡

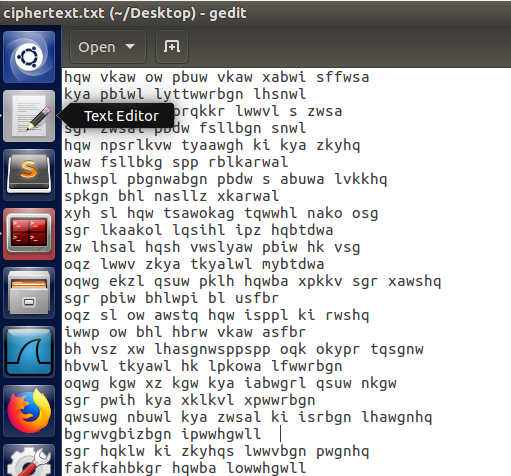
实验1：（task1之后的内容我也提前做了~）

Task 1: Frequency Analysis

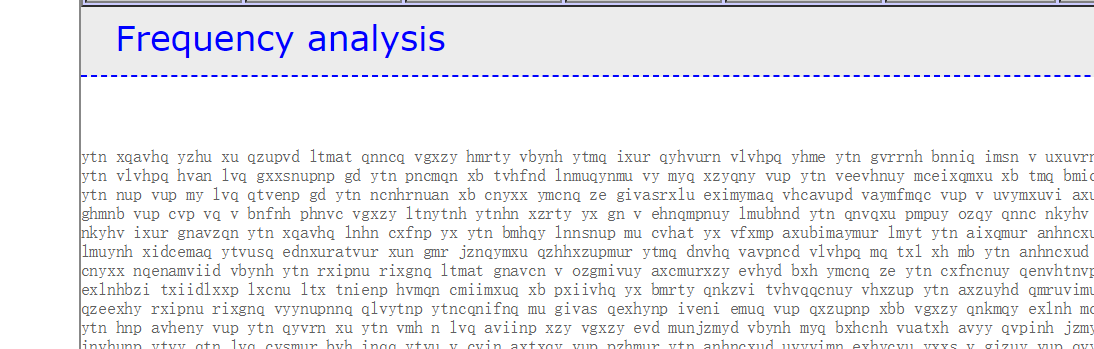
1.按指令对准备好的文章article做简化，生成plain.txt。

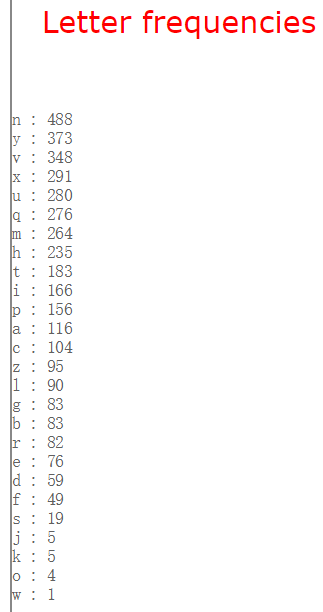


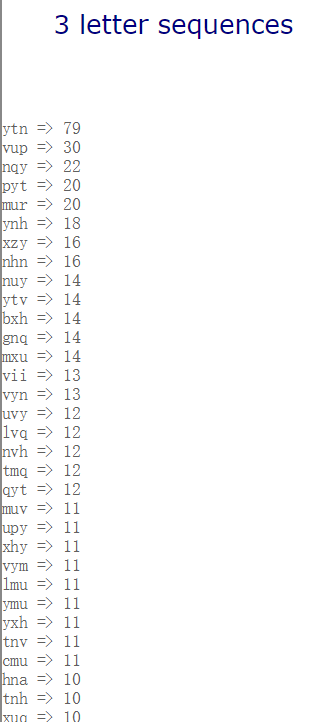
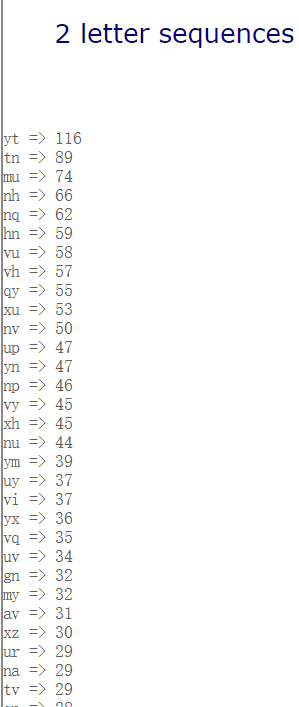
1. 用python和tr指令对简化后的文章进行加密。



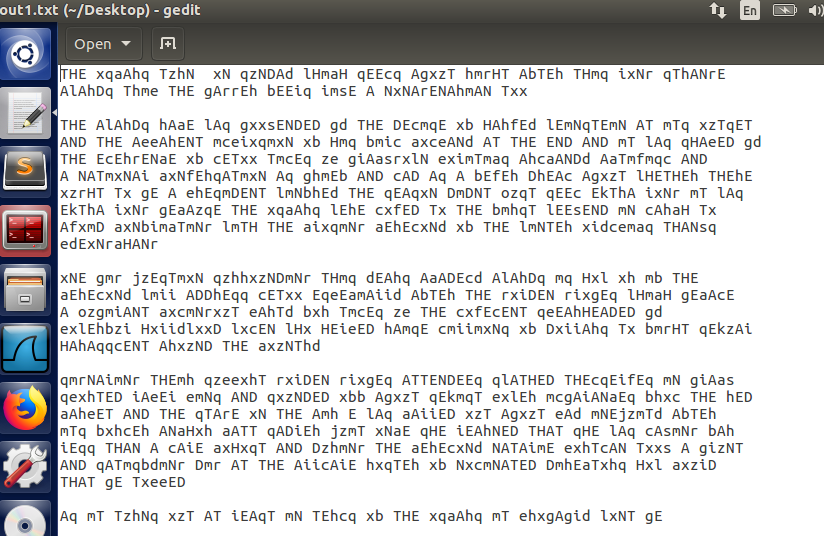
3.使用频率分析解析所给的密文ciphertet.txt。可以对照各个字母在明文文章中出现的一般频率，结合文章中的空格，还原每个单词，来分析每个密文字母对应哪个明文字母，从而得到加密密钥。







首先，根据双字母和三字母出现的频率，找到对应关系ytn->the， vup->and，替换这两组，得到out1.txt。



Timesc

of times

c

thanks

c

its

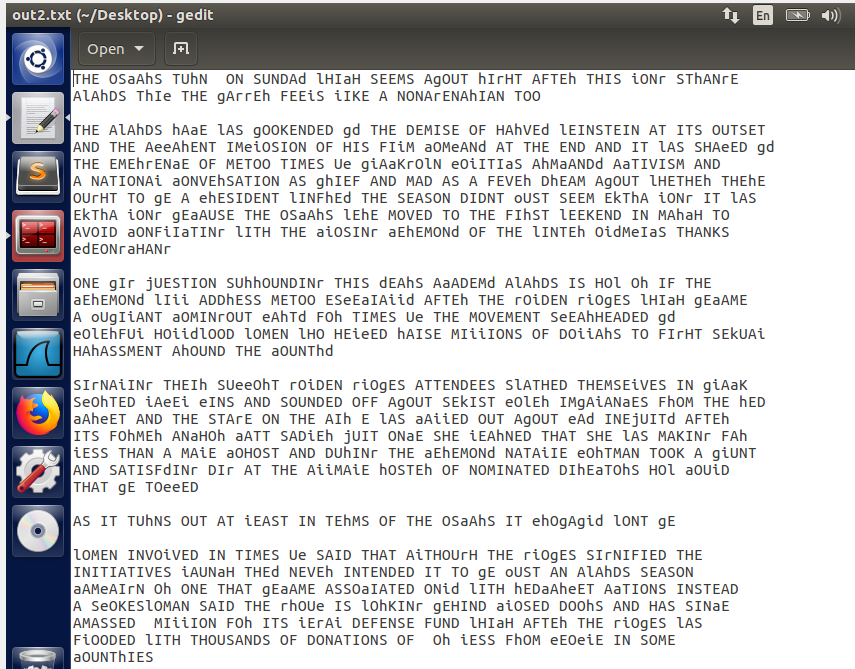
c

out

avoid

c

在新的文档中，结合已经替换的字母和单词的拼写，发现x->o，m->i，f->v，z->u，q->s，s->k，b->f，c->m，替换这些字母，得到out2.txt。



right

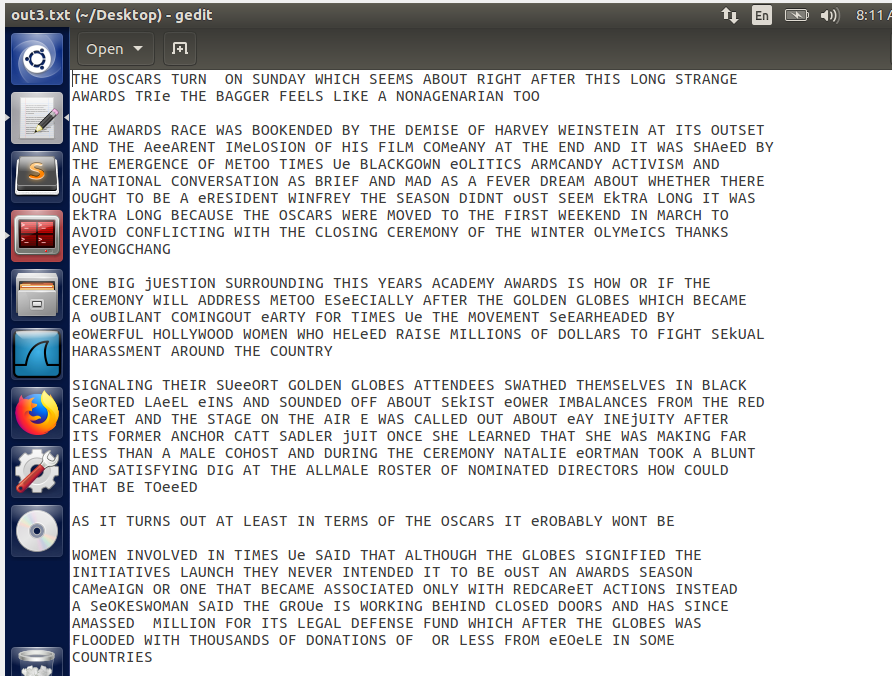
sunday which

wont be

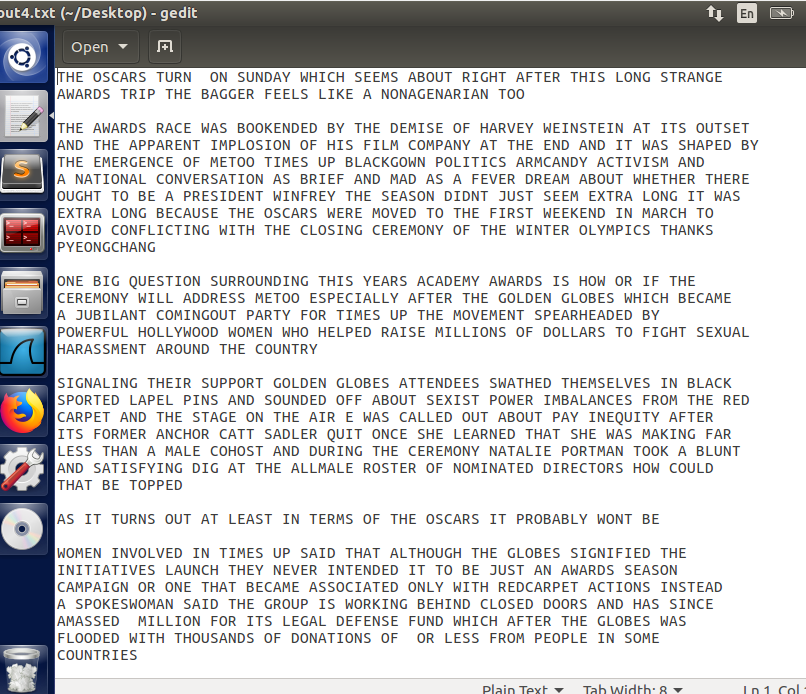
women

turns

从这里面可以看出，h->r，g->b，l->w，i->l，a->c，d->y，r->g，替换这些字母，得到out3.txt



可以看出剩余的：e->p，j->q，k->x，o->j，w->z，由此得到明文：



明文：

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

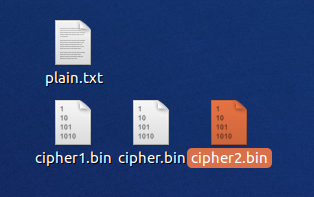
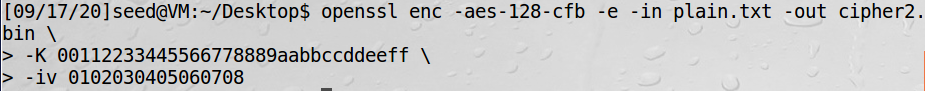
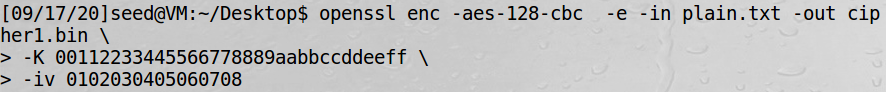
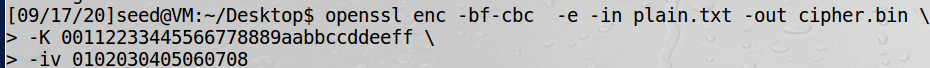
la land the presumptive winner and for two and a half minutes they were

correct before an envelope snafu was revealed and the rightful winner

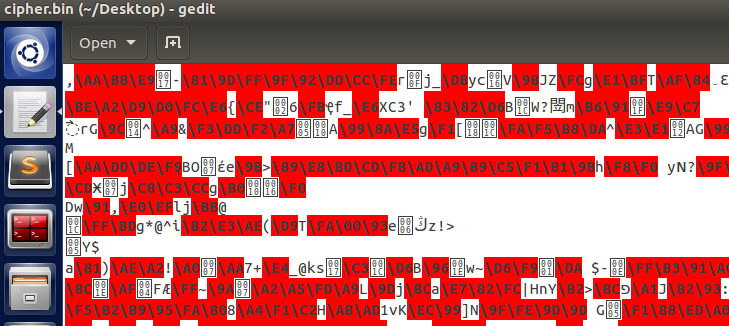
moonlight was crowned

Task 2: Encryption using Different Ciphers and Modes

1. 分别用三种算法对plain.txt加密，分别得到一个加密结果文件。

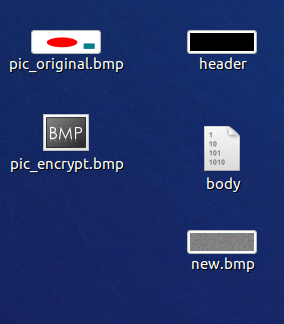
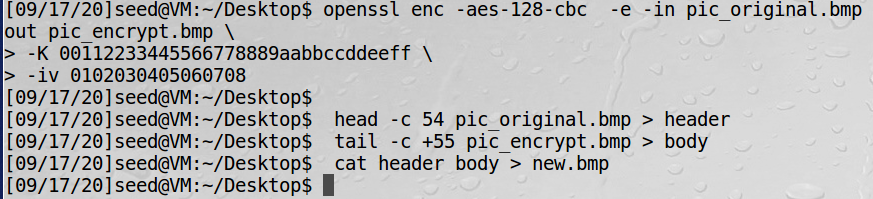


2.可以看到，不通加密方法的到的密文是不同的。

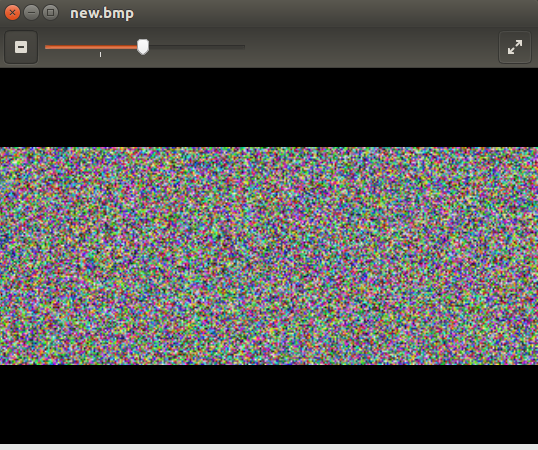


Task 3: Encryption Mode – ECB vs. CBC

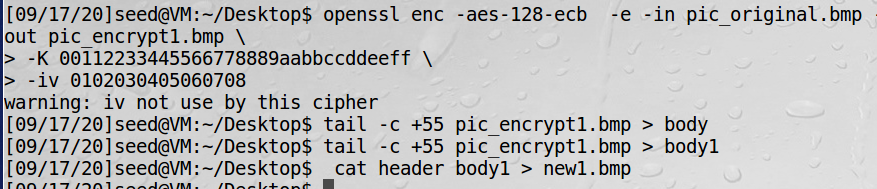
1.用cbc方式对原始图片加密后，将两个图片头尾拼接生成新的图片new.bmp：



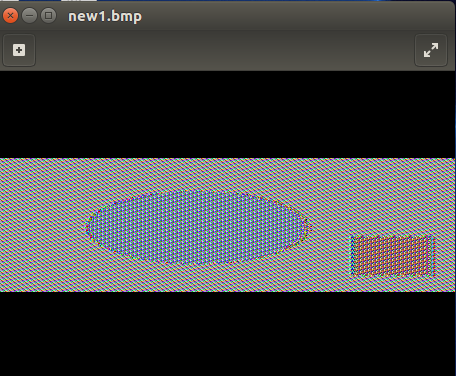
使用图片查看程序显示加密的图片，加密后的图片像素点被打乱了，基本颜色还是来源于原图片的红色，绿色和白色，但是无法找出原图片中的有用信息。



1. 用ecb方式对原始图片加密后，将两个图片头尾拼接生成新的图片new1.bmp：

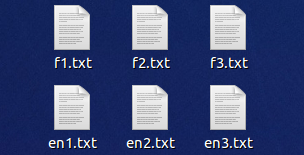
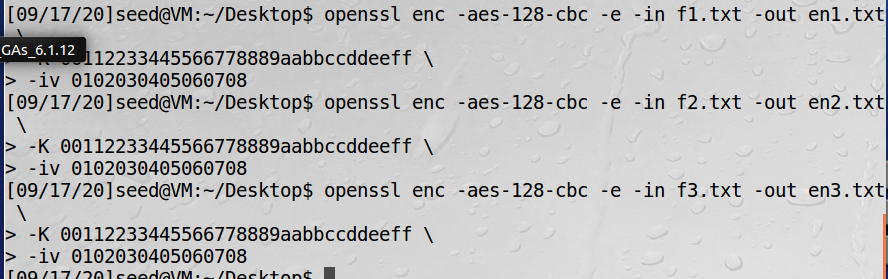
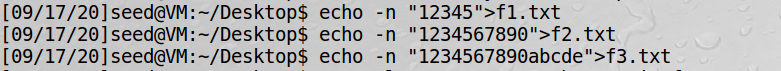


发现用此种方式加密，加密后的图片形状与原图基本相同，只是像素点颜色有所变化。

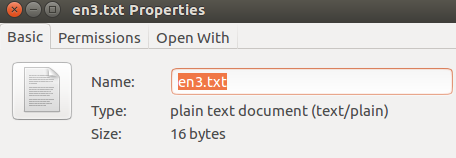
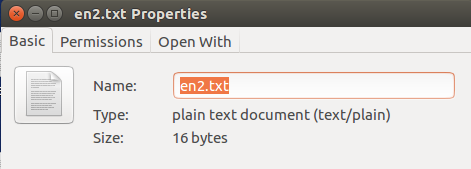
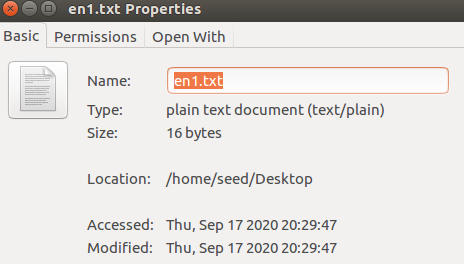


Task 4: Padding

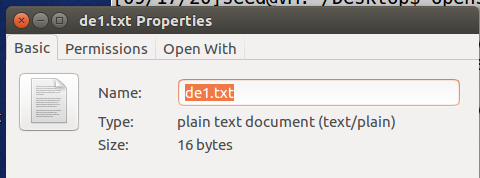
1.创建3个文件，分别为5/10/15字节，并分别对这三个文件进行cbc加密。



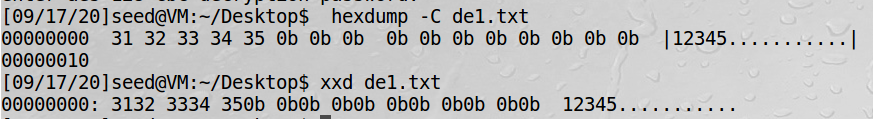
2.分别查看这个三个文件的大小，发现均为16字节，可知都进行了填充。



1. 查看解密数据，查看填充时用了哪些数据。解密文件与加密文件一样大，包含填充数据。



使用十六进制工具来显示内容，可以看到填充数据。



Task 5: Error Propagation – Corrupted Cipher Text

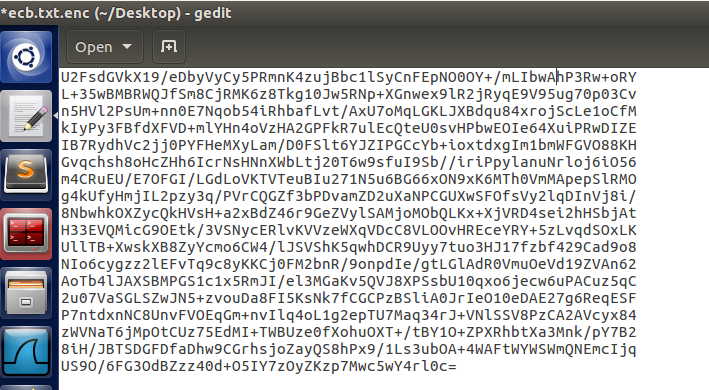
ECB：单个密文分组中有一个或多个比特错误只会影响该分组的解密结果。

CBC：密文分组中一个单比特错误会影响到该分组和它的下一个分组的解密，不会影响之后的。

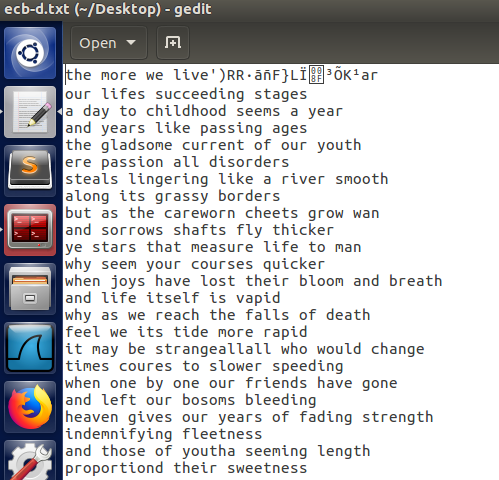
OFB：有一个或多个比特错误的任一密文字符仅会影响该字符的解密，密文的某比特位置出错将导致还原明文的相应位置也出错。

CFB：一个或多个比特错误出现在任一个r比特的密文分组中会影响该分组和后续 n/r（向上取整）个密文分组的解密。

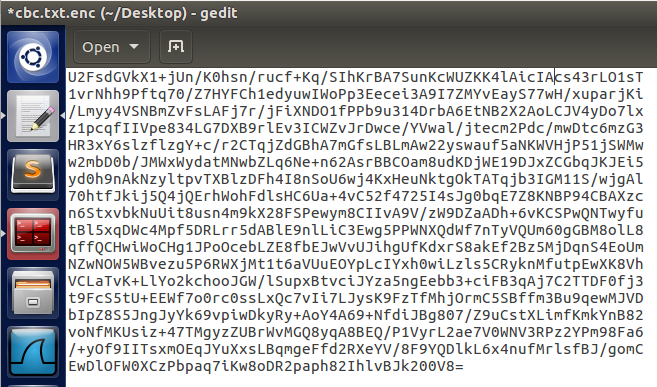
1. 对plain.txt执行ecb加密，生成加密文件ecb.txt.enc，修改第55个字母为‘A’：



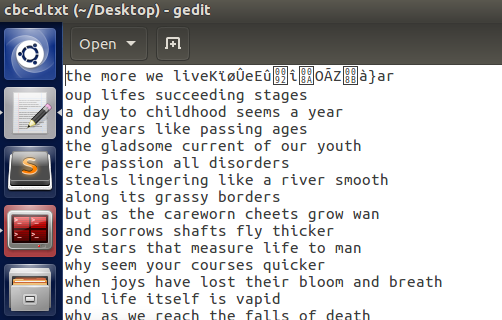
解密后生成ecb\_d.txt，发现只有该分组没能正确解密，后面的不受影响。



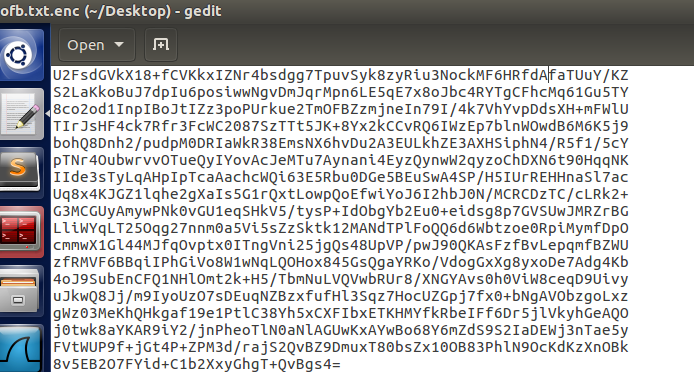
1. 对plain.txt执行cbc加密，生成加密文件cbc.txt.enc，修改第55个字母为‘A’：



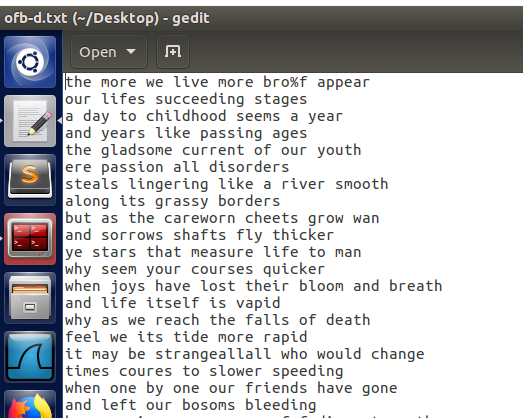
解密后生成cbc\_d.txt，发现只有该分组以及下一个分组没能正确解密，后面的不受影响。



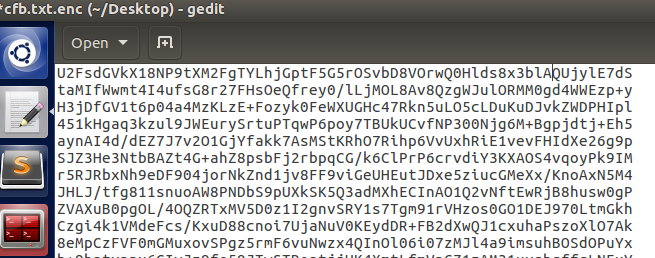
1. 对plain.txt执行ofb加密，生成加密文件ofb.txt.enc，修改第55个字母为‘A’：



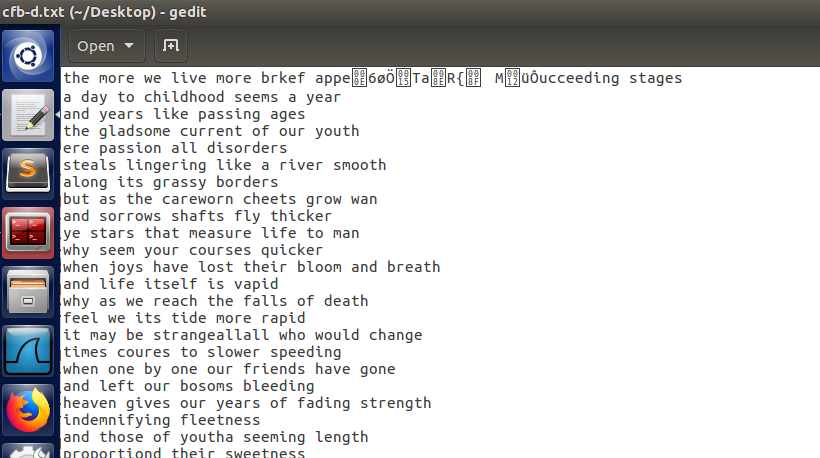
解密后生成ofb\_d.txt，发现只有该对应位置的字符没能正确解密，不影响整个分组，也不影响后面所有的。

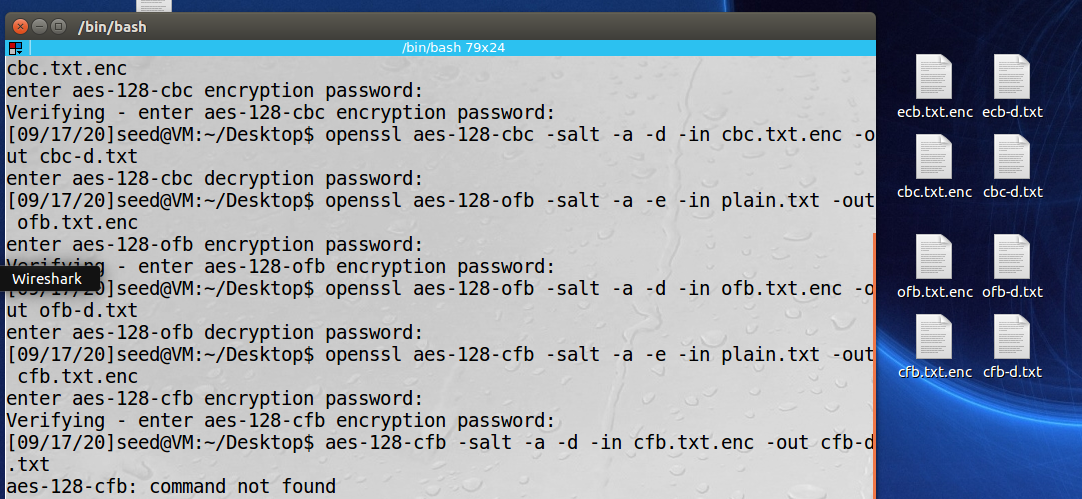


1. 对plain.txt执行cfb加密，生成加密文件cfb.txt.enc，修改第55个字母为‘A’：



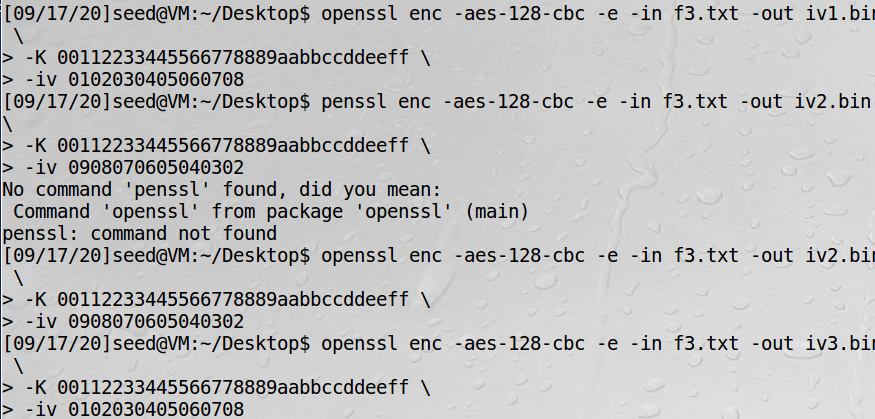
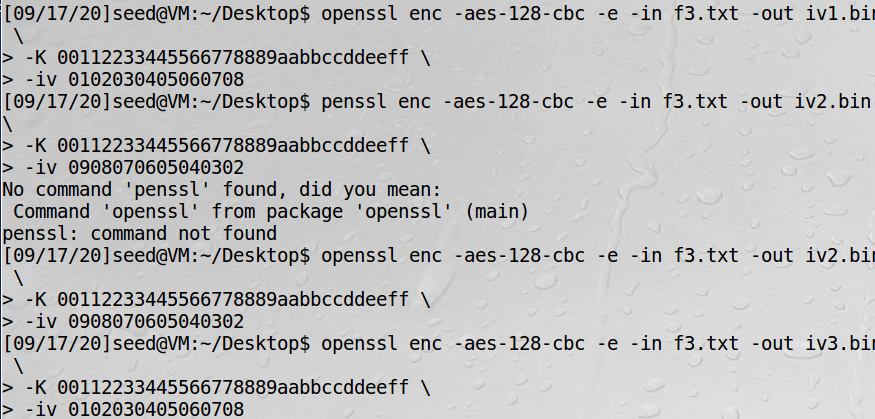
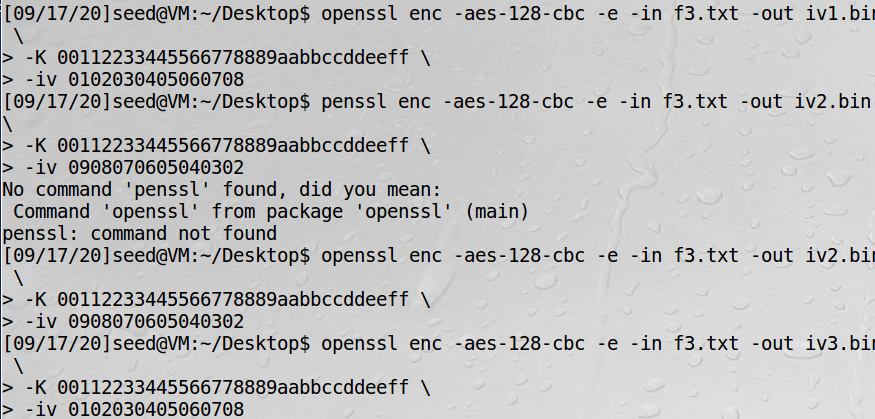
解密后生成cfb\_d.txt，发现后面多个分组（n/r向上取整）的内容改变了。





Task 6: Initial Vector (IV) and Common Mistakes

1. 分别用相同iv加密得到iv1.bin、iv3.bin，不同iv加密得到iv1.bin、iv2.bin。



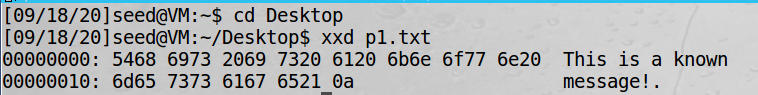
发现相同iv能产生相同密文，不同iv会产生不同密文。因此在解密的时候，只有密钥和iv都相同时，密文才能解密出同样的明文。因此iv需要是唯一的。



1. ofb是用iv和密钥生成密钥流，密钥流不断作为新的iv与后面的密钥生成后面的密钥流。因此如果iv和密钥都相同，则密钥流一定相同。而密文是明文与密钥流异或得到，如果已知一组明文和密文，可以用明文和密文异或得到密钥流，然后再用密钥流与另一组密文异或，解密出它对应的明文。即**P2(hex)=P1(hex)⊕C1⊕C2**。



将P1显示为十六进制形式：



用5468 6973 2069 7320 6120 6b6e 6f77 6e20 6d65 7373 6167 6521异或

a469 b1c5 02c1 cab9 6696 5e50 4254 38e1 bb1b 5f90 37a4 c159异或

bf73 bcd3 5092 99d5 66c3 5b5d 4503 37e1 bb17 5f90 3faf c159 （转为二进制形式做），

得到**P2(hex)= 7f72 6465 723a 304c 6175 6e93 6820 6120 6d69 7373 696c c159**.

1. cbc模式下，对于第一个明文分组，初始iv和明文异或后经密钥加密得到密文，解密时密文再经过密钥的相同作用（由于是对称密钥）后与iv异或得到明文。

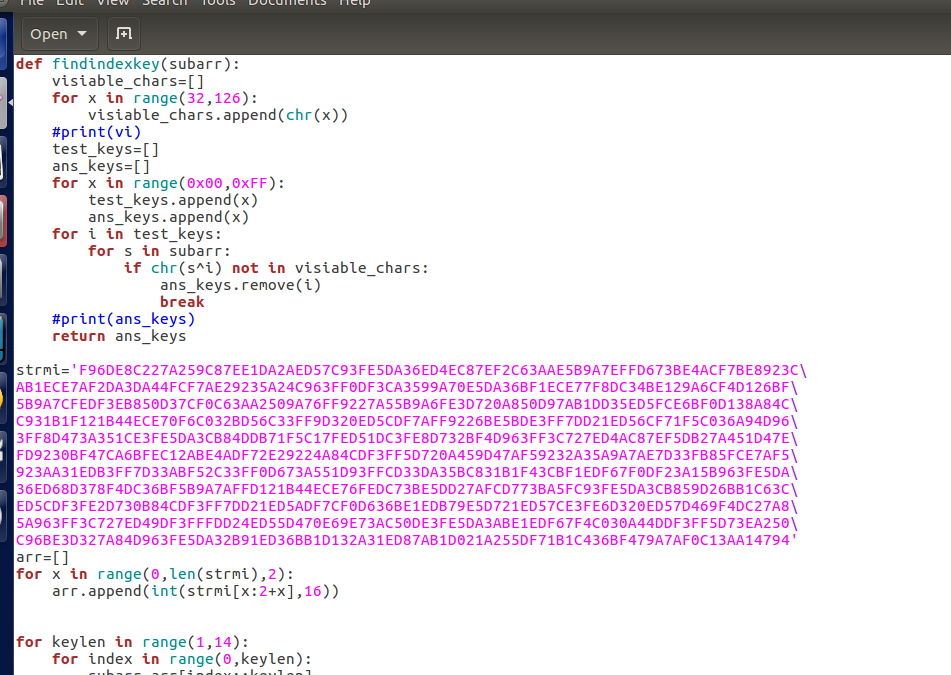
因此可以利用P2，预测后的iv和密文得到aes的密钥，然后用C1经密钥作用后再与前一个iv异或，从而得到P1明文。

实验2：

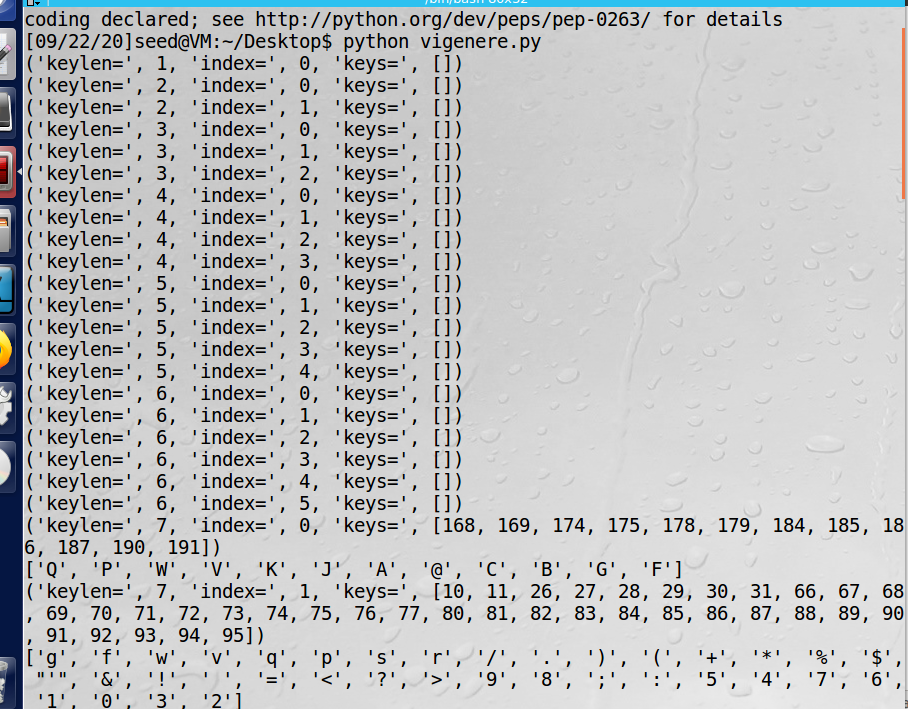
1. 破解Vigenere密码

假设加密者使用的密钥为vigenerekey，长度为keylen，密文为字符串arr，那么字符串subarr0=arr[0]+arr[keylen]+arr[keylen\*2]……是被vigenerekey[0]解密的内容。依次类推，subarr1=arr[1]+arr[1+keylen]+arr[1+keylen\*2]……是被vigenerekey[1]解密的内容，subarr2=arr[2]+arr[2+keylen]+arr[2+keylen\*2]……是被vigenerekey[2]解密的内容，……按照这种分割方法，可以把密文arr分割成keylen份，每份都被密钥vigenerekey的同一位解密。对每个vigenerekey[index]，穷举vigenerekey[index]的值（范围是0x00~0xFF），并与对应的subarr里的内容解码，找到能将该subarr所有内容解为可见字符的所有可能值。

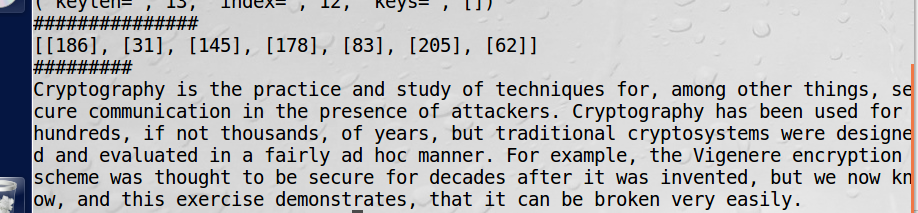
代码如下：





运行程序，可以看出，keylen=7时有结果。

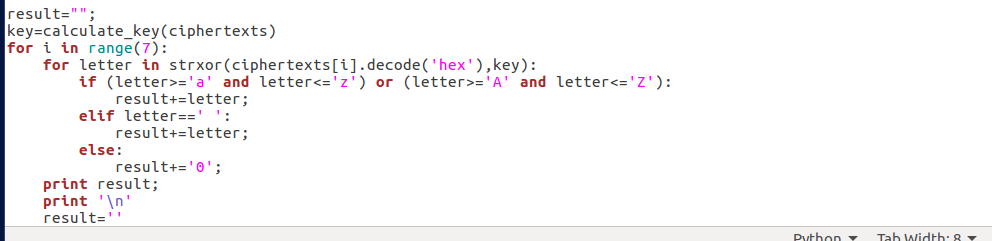
缩小一下范围，假设明文只有字母、数字、空格、逗号和句号，再进行穷举。得到唯一的密钥:[[186],[31],[145],[178],][83],[205],[62]]。用这个密钥解密，并显示明文：



1. 破解一次一密密码

空格space的ASCII码二进制形式为0010 0000，大写字母A～Z的ASCII码二进制形式为01000001～01011010，小写字母a～z的ASCII码二进制形式为 01100001～01111010。因此可以用space和字母做xor操作，对字母进行大小写切换，而两个字母做xor操作，结果将不在字母范围内。又由于将两个密文做xor操作相当于将两个密文对应的明文做xor操作，如果结果中某个位置出现字母，则说明这两个明文的其中一个在该位置可能为空格。故对7个密文分别做两两xor操作，然后通过结果判断不同明文中可能存在空格的位置，然后将对应位置上的密文和space做xor操作，就可得到对应位置的密钥信息，当获取足够多的密钥信息后，即可对目标密文进行解密。

代码如下：



程序运行结果如下，解出了输入的明文：

