**Lab7-Report**

57118116 陈煜

Task1：

选择如下文档：

ytn xqavhq yzhu xu qzupvd ltmat qnncq vgxzy hmrty vbynh ytmq ixur qyhvurn vlvhpq yhme ytn gvrrnh bnniq imsn v uxuvrnuvhmvu yxx

ytn vlvhpq hvan lvq gxxsnupnp gd ytn pncmqn xb tvhfnd lnmuqynmu vy myq xzyqny vup ytn veevhnuy mceixqmxu xb tmq bmic axcevud vy ytn nup vup my lvq qtvenp gd ytn ncnhrnuan xb cnyxx ymcnq ze givasrxlu eximymaq vhcavupd vaymfmqc vup v uvymxuvi axufnhqvymxu vq ghmnb vup cvp vq v bnfnh phnvc vgxzy ltnytnh ytnhn xzrty yx gn v ehnqmpnuy lmubhnd ytn qnvqxu pmpuy ozqy qnnc nkyhv ixur my lvq nkyhv ixur gnavzqn ytn xqavhq lnhn cxfnp yx ytn bmhqy lnnsnup mu cvhat yx vfxmp axubimaymur lmyt ytn aixqmur anhncxud xb ytn lmuynh xidcemaq ytvusq ednxuratvur

xun gmr jznqymxu qzhhxzupmur ytmq dnvhq vavpncd vlvhpq mq txl xh mb ytn anhncxud lmii vpphnqq cnyxx nqenamviid vbynh ytn rxipnu rixgnq ltmat gnavcn v ozgmivuy axcmurxzy evhyd bxh ymcnq ze ytn cxfncnuy qenvhtnvpnp gd exlnhbzi txiidlxxp lxcnu ltx tnienp hvmqn cmiimxuq xb pxiivhq yx bmrty qnkzvi tvhvqqcnuy vhxzup ytn axzuyhd

qmruvimur ytnmh qzeexhy rxipnu rixgnq vyynupnnq qlvytnp ytncqnifnq mu givas qexhynp iveni emuq vup qxzupnp xbb vgxzy qnkmqy exlnh mcgvivuanq bhxc ytn hnp avheny vup ytn qyvrn xu ytn vmh n lvq aviinp xzy vgxzy evd munjzmyd vbynh myq bxhcnh vuatxh avyy qvpinh jzmy xuan qtn invhunp ytvy qtn lvq cvsmur bvh inqq ytvu v cvin axtxqy vup pzhmur ytn anhncxud uvyvimn exhycvu yxxs v gizuy vup qvymqbdmur pmr vy ytn viicvin hxqynh xb uxcmuvynp pmhnayxhq txl axzip ytvy gn yxeenp

vq my yzhuq xzy vy invqy mu ynhcq xb ytn xqavhq my ehxgvgid lxuy gn

lxcnu mufxifnp mu ymcnq ze qvmp ytvy viytxzrt ytn rixgnq qmrumbmnp ytn mumymvymfnq ivzuat ytnd unfnh muynupnp my yx gn ozqy vu vlvhpq qnvqxu avcevmru xh xun ytvy gnavcn vqqxamvynp xuid lmyt hnpavheny vaymxuq muqynvp v qexsnqlxcvu qvmp ytn rhxze mq lxhsmur gntmup aixqnp pxxhq vup tvq qmuan vcvqqnp cmiimxu bxh myq inrvi pnbnuqn bzup ltmat vbynh ytn rixgnq lvq bixxpnp lmyt ytxzqvupq xb pxuvymxuq xb xh inqq bhxc enxein mu qxcn axzuyhmnq

ux avii yx lnvh givas rxluq lnuy xzy mu vpfvuan xb ytn xqavhq ytxzrt ytn cxfncnuy lmii vicxqy anhyvmuid gn hnbnhnuanp gnbxhn vup pzhmur ytn anhncxud nqenamviid qmuan fxavi cnyxx qzeexhynhq imsn vqtind ozpp ivzhv pnhu vupumaxin smpcvu vhn qatnpzinp ehnqnuynhq

vuxytnh bnvyzhn xb ytmq qnvqxu ux xun hnviid suxlq ltx mq rxmur yx lmu gnqy emayzhn vhrzvgid ytmq tveenuq v ixy xb ytn ymcn muvhrzvgid ytn uvmigmynh uvhhvymfn xuid qnhfnq ytn vlvhpq tden cvatmun gzy xbynu ytn enxein bxhnavqymur ytn hvan qxaviinp xqavhxixrmqyq avu cvsn xuid npzavynp rznqqnq

ytn lvd ytn vavpncd yvgzivynq ytn gmr lmuunh pxnquy tnie mu nfnhd xytnh avynrxhd ytn uxcmunn lmyt ytn cxqy fxynq lmuq gzy mu ytn gnqy emayzhn avynrxhd fxynhq vhn vqsnp yx imqy ytnmh yxe cxfmnq mu ehnbnhnuymvi xhpnh mb v cxfmn rnyq cxhn ytvu enhanuy xb ytn bmhqyeivan fxynq my lmuq ltnu ux cxfmn cvuvrnq ytvy ytn xun lmyt ytn bnlnqy bmhqyeivan fxynq mq nimcmuvynp vup myq fxynq vhn hnpmqyhmgzynp yx ytn cxfmnq ytvy rvhunhnp ytn nimcmuvynp gviixyq qnaxupeivan fxynq vup ytmq axuymuznq zuymi v lmuunh ncnhrnq

my mq vii ynhhmgid axubzqmur gzy veevhnuyid ytn axuqnuqzq bvfxhmyn axcnq xzy vtnvp mu ytn nup ytmq cnvuq ytvy nupxbqnvqxu vlvhpq atvyynh mufvhmvgid mufxifnq yxhyzhnp qenazivymxu vgxzy ltmat bmic lxzip cxqy imsnid gn fxynhq qnaxup xh ytmhp bvfxhmyn vup ytnu njzviid yxhyzhnp axuaizqmxuq vgxzy ltmat bmic cmrty ehnfvmi

mu my lvq v yxqqze gnylnnu gxdtxxp vup ytn nfnuyzvi lmuunh gmhpcvu mu lmyt ixyq xb nkenhyq gnyymur xu ytn hnfnuvuy xh ytn gmr qtxhy ytn ehmwn lnuy yx qexyimrty ivqy dnvh unvhid vii ytn bxhnavqynhq pnaivhnp iv iv ivup ytn ehnqzceymfn lmuunh vup bxh ylx vup v tvib cmuzynq ytnd lnhn axhhnay gnbxhn vu nufnixen quvbz lvq hnfnvinp vup ytn hmrtybzi lmuunh cxxuimrty lvq ahxlunp

ytmq dnvh vlvhpq lvyatnhq vhn zunjzviid pmfmpnp gnylnnu ythnn gmiigxvhpq xzyqmpn nggmur cmqqxzhm ytn bvfxhmyn vup ytn qtven xb lvynh ltmat mq ytn gvrrnhq ehnpmaymxu lmyt v bnl bxhnavqymur v tvmi cvhd lmu bxh rny xzy

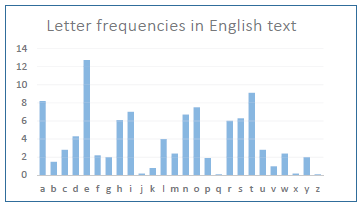
gzy vii xb ytxqn bmicq tvfn tmqyxhmavi xqavhfxymur evyynhuq vrvmuqy ytnc ytn qtven xb lvynh tvq uxcmuvymxuq cxhn ytvu vud xytnh bmic vup lvq viqx uvcnp ytn dnvhq gnqy gd ytn ehxpzanhq vup pmhnayxhq rzmipq dny my lvq uxy uxcmuvynp bxh v qahnnu vayxhq rzmip vlvhp bxh gnqy nuqncgin vup ux bmic tvq lxu gnqy emayzhn lmytxzy ehnfmxzqid ivupmur vy invqy ytn vayxhq uxcmuvymxu qmuan ghvfntnvhy mu ytmq dnvh ytn gnqy nuqncgin qvr nupnp ze rxmur yx ythnn gmiigxvhpq ltmat mq qmrumbmavuy gnavzqn vayxhq cvsn ze ytn vavpncdq ivhrnqy ghvuat ytvy bmic ltmin pmfmqmfn viqx lxu ytn gnqy phvcv rxipnu rixgn vup ytn gvbyv gzy myq bmiccvsnh cvhymu capxuvrt lvq uxy uxcmuvynp bxh gnqy pmhnayxh vup vevhy bhxc vhrx cxfmnq ytvy ivup gnqy emayzhn lmytxzy viqx nvhumur gnqy pmhnayxh uxcmuvymxuq vhn bnl vup bvh gnylnnu

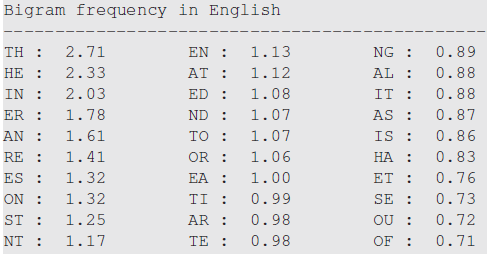
在<http://www.richkni.co.uk/php/crypta/freq.php>网站上分析出现频率较高的字母和字母组合如下：

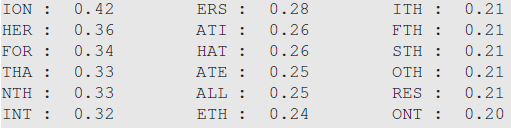
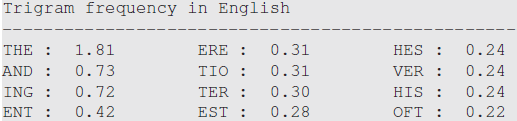
﻿n : 488 y : 373 v : 348 x : 291 u : 280 q : 276 m : 264  
h : 235 t : 183 i : 166 p : 156 a : 116 c : 104 z : 95

﻿yt => 116 tn => 89 mu => 74 nh => 66 nq => 62 hn => 59  
vu => 58 vh => 57 qy => 55 xu => 53 nv => 50 up => 47  
yn => 47 np => 46 vy => 45 xh => 45 nu => 44 ym => 39  
uy => 37 vi => 37 yx => 36 vq => 35 uv => 34 gn => 32

﻿ytn => 79 vup => 30 nqy => 22 pyt => 20 mur => 20  
ynh => 18 xzy => 16 nhn => 16 nuy => 14 ytv => 14  
bxh => 14 gnq => 14 mxu => 14 vii => 13 vyn => 13  
uvy => 12 lvq => 12 nvh => 12 tmq => 12 qyt => 12  
根据在英文中出现的字母和字母组合的频率：







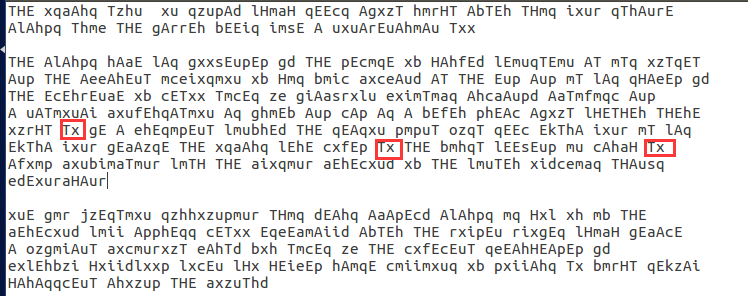
猜测y=>t, t=>h, n=>e

观察到v一个字母组成一个单词，猜测v=>a

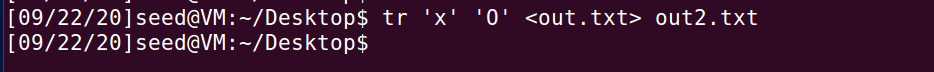
通过如下命令在out.txt中输出第一轮猜测的结果：



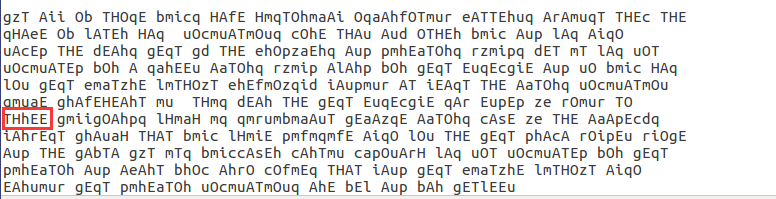
out.txt中的部分内容如下：



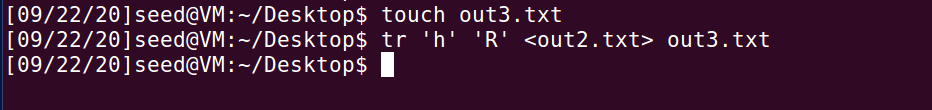
发现文本中多次出现Tx，猜测x是o：



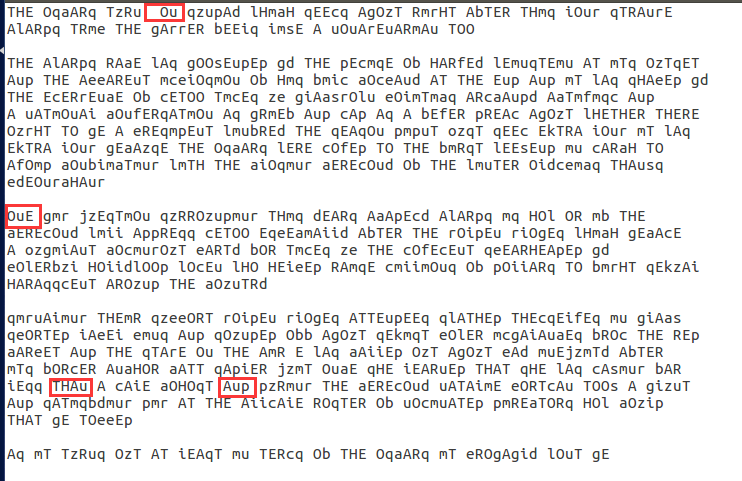
部分文本如下：



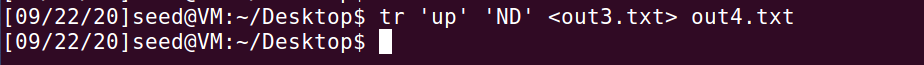
猜测h=>r：



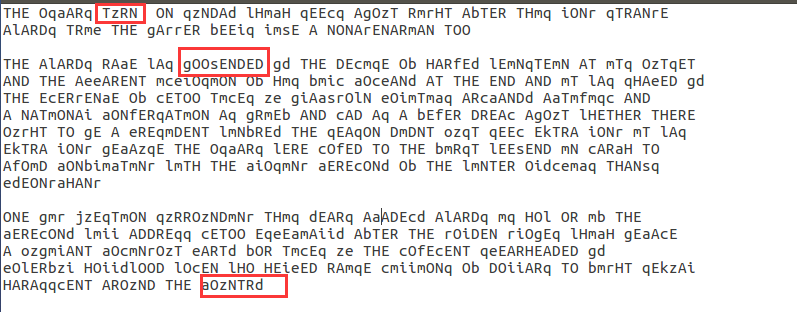
部分文本如下：



猜测u=>n, p=>d：



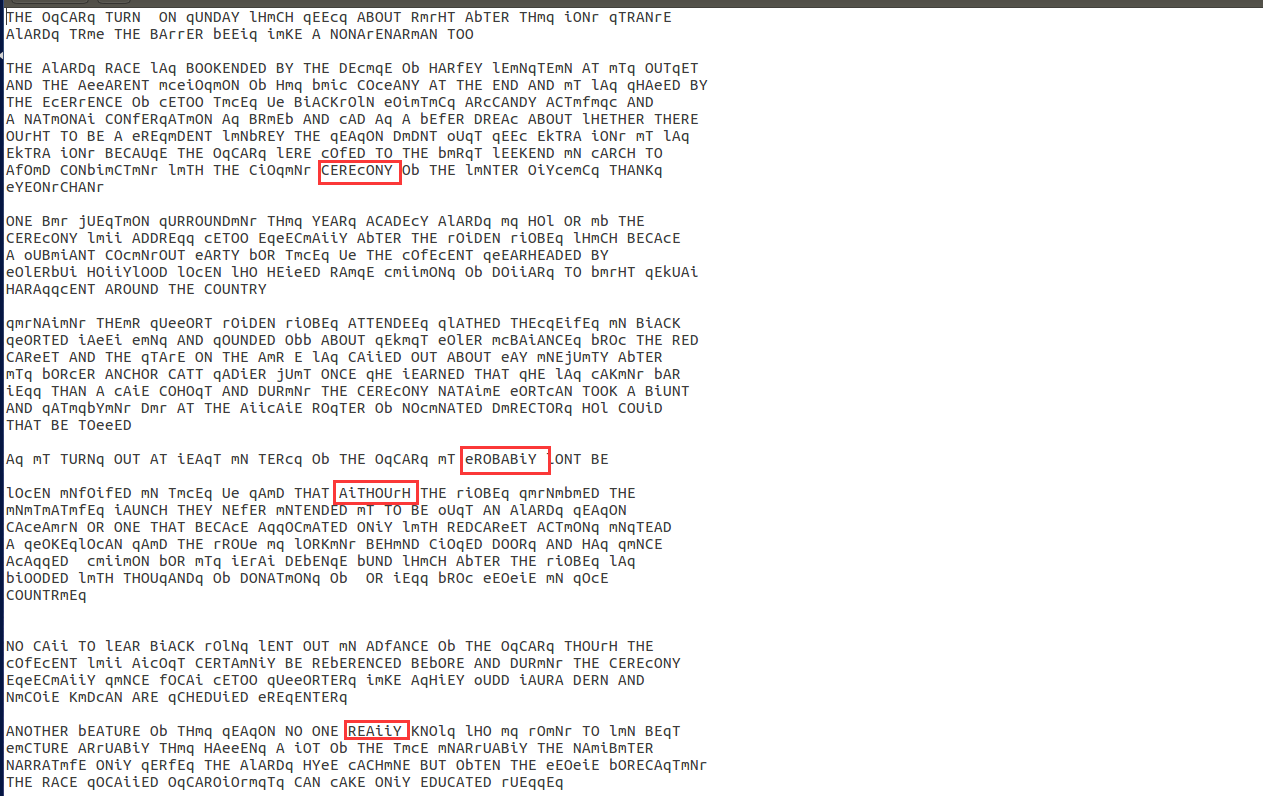
部分文本如下：



猜测z=>u, g=>b, s=>k, a=>c, d=>y：



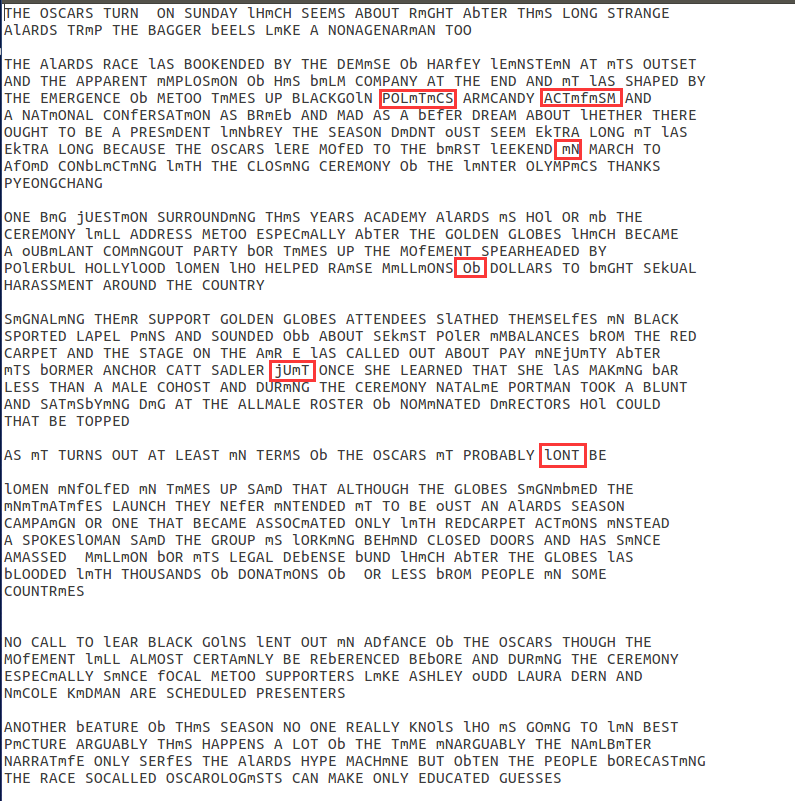
部分文本如下：



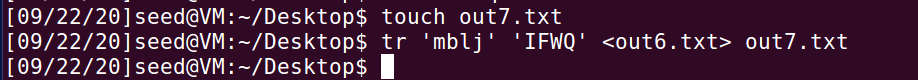
猜测i=>l, r=>g, e=>p, c=>m, q=>s：



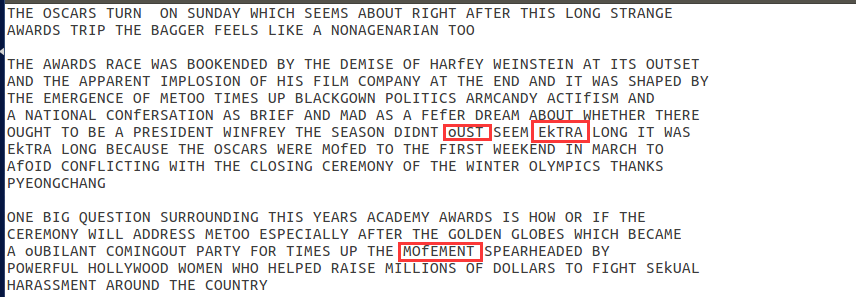
部分文本如下：



猜测m=>i, b=>f, l=>w, j=>q:



部分文本如下：



猜测o=>z, k=>x, f=>v:



剩下的w即对应j

密文已全部译成明文：

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 ZUST 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 ZUBILANT 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 ZUST 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 ZUDD 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 PRIJE 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

破解维吉尼亚密码：

（1）确认密钥长度。

根据维吉尼亚密码的原理：对于每一个长度为i的密钥，都可以将密文每隔i个分为一组。对每个组统计组内每个字符出现的频率，记为数组q[256]；对长度为i的密钥，计算每组对应的，记为数组prod[i]。对每个长度的密钥，都求prod的平均值res，最后得到最大的res对应的密钥长度。认为密钥长度在1~13之间。

编写如下程序：

int determineKeyLength(unsigned char\* ctext) {

int keyLength = 0;

double max = 0;

int strLength = strlen(ctext);

for (int i = 1; i <= 13; i++) {

double\* prod=new double[i];

for (int k = 0; k < i; k++) {

prod[k] = 0;

double q[256];

for (int j = 0; j < 256; j++) {

q[j] = 0;

}

double sum = 0;

for (int j = k; j < strLength; j += i) {

sum += 1;

q[ctext[j]] += 1;

}

for (int j = 0; j < 256; j++) {

q[j] /= sum;

prod[k] += q[j] \* q[j];

}

}

double sum = 0;

for (int j = 0; j < i; j++) {

sum += prod[j];

}

double res = sum / i;

if (res > max) {

max = res;

keyLength = i;

}

}

return keyLength;

}

函数的返回值keyLength=7，即密钥长度为7。

（2）确定密钥的每个字节。

对于密钥的第digit个字节，从密文中的第digit个字节开始，每7位取为一个字节，构成数组cipher。对于cipher来说，就是相对于密钥第digit个字节的移位密码。

确定密钥每个字节的方法为：将要求的字节从0x00一直取到0xFF，将恢复的明文字节作为字母出现的频率与英文文本中每个字母出现的频率分别相乘后，求和，结果记为prod，使prod满足：

1. 恢复的明文字节的值为ASCII合法字符，即在32~127之间；
2. prod与0.065的差值在0.01之内；
3. prod尽可能大。

代码如下：

int length = strlen(ctext);

int keyLength = determineKeyLength(ctext);

printf("The number of groups is %d. And their keys are:\n", keyLength);

const int degrees = 10;

unsigned char keys[keyLength][degrees];

for (int digit = 0; digit < keyLength; digit++) {

//get the digit-th group into array `cipher`

unsigned char cipher[1024];

int j = 0;

for (int i = digit; i < length; i += keyLength) {

cipher[j] = ctext[i];

j++;

}

cipher[j] = '\0';

double last[degrees] = { 0 };

for (int i = 0x00; i <= 0xFF; i++) {

unsigned char key = i;

int suitable = 1;

for (int ch = 0; ch < j; ch++) {

unsigned char p = key ^ cipher[ch];

if (p < 32 || p > 127) {

suitable = 0;

break;

}

}

if (suitable) {

unsigned char plaintext[1024];

for (int ch = 0; ch < j; ch++) {

plaintext[ch] = key ^ cipher[ch];

}

plaintext[j] = '\0';

double q[26];

double sum = 0;

for (int k = 0; k < 26; k++) {

q[k] = 0;

}

for (int ch = 0; ch < j; ch++) {

if (plaintext[ch] >= 97 && plaintext[ch] <= 123) {

sum += 1;

q[plaintext[ch] - 97] += 1;

}

}

double prod = 0;

for (int k = 0; k < 26; k++) {

q[k] = q[k] / sum;

prod += q[k] \* p[k] \* 0.01;

}

double distance = prod - 0.065;

if (distance < 0) {

distance = -distance;

}

if (distance <= 0.01) {

for (int degree = degrees - 1; degree >= 0; degree--) {

if (prod > last[degree]) {

if (degree + 1 < degrees) {

last[degree + 1] = last[degree];

last[degree] = prod;

keys[digit][degree + 1] = keys[digit][degree];

keys[digit][degree] = i;

}

}

}

}

}

}

}

得到的结果为：

1th key: 186 171 0 0 0 0 0 0 0 0

2th key: 31 81 95 86 14 66 76 67 77 87

3th key: 216 223 194 217 195 145 104 138 172 229

4th key: 178 191 172 229 16 0 0 0 48 0

5th key: 18 0 12 1 13 83 29 27 48 106

6th key: 132 131 158 133 159 205 137 235 254 127

7th key: 62 104 138 172 229 7 0 0 0 0

（3）通过尝试，最终得到的密钥为[186, 31, 145, 178, 83, 205, 62]。解密代码如下：

printf("Input the keys you guess: ");

for (int i = 0; i < 7; i++) {

scanf("%02X", guessedKeys);

}

for (int i = 0; i < length; i++) {

printf("%c", ctext[i] ^ guessedKeys[i % 7]);

}

得到的明文为：

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.

一次一密：

（1）通过如下代码将密文两两逐字节异或，得到的结果即为明文异或的结果：

FILE\* file = fopen("otp.txt", "r");

unsigned char otp[7][1024];

for (int line = 0; line < 7; line++) {

unsigned char tmp[1024];

fgets(tmp, 1024, file);

unsigned char\* potp = otp[line];

unsigned char\* ptmp = tmp;

while (EOF != sscanf(ptmp, "%02X", potp)) {

ptmp += 2;

potp++;

}

}

for (int line1 = 0; line1 < 7; line1++) {

// the xor result

unsigned char res[7][1024];

for (int line2 = 0; line2 < 7; line2++) {

if (line2 == line1) {

continue;

}

for (int ch = 0; ch < 31; ch++) {

res[line2][ch] = otp[line1][ch] ^ otp[line2][ch];

}

}

}

（2）由于空白字符0x20与字母异或后，开头为0b01，即异或后的值大于64，因此对每一行密文的每个字符，统计其与其他6行密文相应位置的字符异或的结果，如果有多于4个结果的值大于64，那么就有可能该位置是空格。统计完所有空格之后，将空格的位置赋值 0x20 , 那么反推其他几行密文对应位置的字符。

代码实现如下：

for (int line1 = 0; line1 < 7; line1++) {

for (int ch = 0; ch < 31; ch++) {

int count = 0;

for (int line2 = 0; line2 < 7; line2++) {

if (line2 != line1 && res[line2][ch] >= 64) {

count++;

}

}

if (count >= 4) {

plaintext[line1][ch] = ' ';

for (int line2 = 0; line2 < 7; line2++) {

if (line2 == line1) {

continue;

}

if (plaintext[line2][ch] != '\*') {

continue;

}

plaintext[line2][ch] = res[line2][ch] ^ 0x20;

}

}

}

}

通过上述代码可以得知部分明文（其中\*为位置字符）：

\* am p\*a\*n\*ng a s\*cr\*t missio\*\*

\*e is \*h\* \*nly pe\*so\* to trus\*\*

\*he cu\*r\*n\* plan \*s \*op secre\*\*

\*hen s\*o\*l\* we me\*t \*o do thi\*\*

\* thin\* \*h\*y shou\*d \*ollow hi\*\*

\*his i\* \*u\*er tha\* t\*at one i\*\*

\*ot on\* \*a\*et is \*et\*er than \*\*

（3）通过上述结果可以猜测第一行明文为：

I am planning a secret mission.

通过第一行可以得出其他明文。代码如下：

printf("Please enter what you guess for line1: ");

unsigned char line1[1024];

gets(line1);

unsigned char key[31];

// get the plaintext according to user input

for (int ch = 0; ch < 31; ch++) {

key[ch] = line1[ch] ^ otp[0][ch];

plaintext[0][ch] = line1[ch];

}

for (int line = 1; line < 7; line++) {

for (int ch = 0; ch < 31; ch++) {

plaintext[line][ch] = otp[line][ch] ^ key[ch];

}

}

最终得到的明文为：

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.