Cryptography___vigenere_cipher_encryption

Mostafa Amin-Naji

Simulation of HW1, Cryptography Course, Vigenère cipher encryption using letter frequency; Matlab Code

All of This Code was written by Mostafa Amin-Naji

For contact me: Mostafa.Amin.Naji@gmail.com

My other Website:

1. https://sites.google.com/site/mostafaaminnaji/
2. https://scholar.google.com/citations?user=z1gxuKcAAAAJ&hl=en
3. https://www.linkedin.com/in/mostafaaminnaji/

Our goal is encrypt the ciphered text.

Key Length: 7 Characters

alphabet = ['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z'];

English_Letter_Frequency = [0.0817, 0.0150, 0.0278, 0.0425, 0.1270, 0.0223, 0.0202, 0.0609, 0.0697, 0.0015, 0.0077, 0.0403, 0.0241, 0.0675, 0.0751, 0.0193, 0.0010, 0.0599, 0.0633, 0.0906, 0.0276, 0.0098, 0.0236, 0.0015, 0.0197, 0.0007];

Ciphered Text: loe lprtl ders-dpubmkutfv keyjrjhaiuu og s worfamhoahltju jivoes ohs lvrnmsazld cq seuu bblaiyaa bdiexai bjvutk fpmytkln taete zewwu atk utwk a sltbd jivoes vpsi ao toptio bfldeku cjhoex hlqzhbkas. bdiexai"t kfszlm pfsy ydiuuoej hlqzhbkas bxaex zewwyar dosvz, atk sxaacnls xwye oudjuhtkk bz oyizpnh loe rltuwy ol ahf uvrxlsqgudoug bdwhgieu au tnl cjhoexaeyl. sazlr, jf milaeff outkrfv hnj lihza, juoaofls zyiuzlmobs, jf oiy dosc worpgsswhoh, ionlnzld uzl tgiums yeiaa, b uyizpcbd joswoowut um tiw cimlnèsw jivoes. loe zyiuzlmobs dawhky, hpolvky, oodf pxvvjvld g wrpyyeyziww, yimpd, bfk pxldjuaahse tqztkt fpj zwoaciaug hltxwln ippiwy arwhbtlty. dhbl ps tvw lfvwt hs uzl voneoèjl cowhfj day vrjypngslz vlsiyicwk be nipnhn hhtuaztg iemdhsu pn iaz fomtfwu fomtz lorkl bpgr lg jigjh dks. sjy. niucao thtzpsus iersatg. oe hbiml bpuu tiw aahblb jlczh og lyizoenabs, hbt bvkej h rfhlazpnh "uvutaeskpgt" (hkfq) ao ydiuuo cowhfj hlvoacwas kcesq sezaes. ooexlat ssbkytj sud zyiuzlmobs vkld g miywk pgatfju ol zuckaizbtjgus, hllmszo"y zciwte slaol ahk waullrt vf tmiszptvlpotz cpmsd hl ebkple jhbfnej zinhsy hf sfdlczpnh s uec rez. clyy desw ayvpcbdsy ypnhdl wuydt gy snvru horgzet, cuocu tp tvtn waslpey pn bvcatje, pj argusnaatkk "ovl vf hhne" ssotn wjlo tnl mfkzaml. bfdsayv"s nwahuk timz rkxujjld yarpfn skjusaay lvr pfsy zoe lwf. ay pt jk yerhtjnlle latq ao ylcvjl a yoosl ree whssze, yhy cq h pxlvjgbs vyiwsae ivnwwysgaipf, iersatg"z seztfe day jookpdkyacdf muye twjuxl. gjdiexa vfjuas arjwk tu yeqspr zoe cjvkku cjhoex (jrfsaitn tiw cexuan-npgkuèrf uppnlr jf uitltfwu eonhuwln), hbt, og tazaes ooaz oe eak, tnl cjhoex dat kairs vvduexhbmw ao iyyqlhngsytaz. vkynbe"z wuyk, igdeblr, fnlnzbamdf lkk tp loe uue-uate vhd, b loeuyeuajarsy vfirkhkbtse ippiwy. it h cbwzax jiqzlr, khci dltzlr px ahk hlqzhbka it koilaee ssotn spel natbfj vf vsadwz; fuy eystprl, io s jakzas uppnlr px zhomt uzyek, h wpmsd hlcpel d, h dovdk bkjonw l, y cvumv ieivmf t hnj zo pf. ahk cihwuèrk jiqzlr ivntazty vf twcexhl dslsgy cjhoexz io klqalndw dizo djxmexlnu koila vbdbey.ao ffjrewt, b lhbrl og sspnhbflz cgu bf mzej, aeseld g aacmsa xlcus, cimlnèsw zqahrf, gy voneoèjl tgilf. aa cuusjkas um tiw hlvoacwa wxptuwu oaa txwute ziy lpmkz io vpfllrffa ruds, fsjh gspisiez zhjxaej jyddpcgslz lv tnl lfxa cutpbjld zv tiw wrkcipmz arwhbtlt, ivrswzpuudjfn tu ahf ldetay tae puzsjtse ihetsy cowhfjz. az kigxlrkut qgpnzz io loe kucsqwtovn qjvckzs, uzl cowhfj bskz a eamfkyeol hlvoacwa fxvm pfl ol ahf jvwy. ahf sspnhbfl bskk au whcn wojfa dkweovz ot h rfhlazpnh clycvre. whcn yox kaaxas xaah g rez dltzlr. uzl rktajfkex vf uzl rud hpdks zoe mwatkys b lv z (ou siamtkk osvlr). gstigbgn ahfjl axl txwute ziy cly xvwt koocu, ypm dirs oodf uyl at ehne rezk (kilmeswut gspisiezz) at loexl asw bnoxuf dltzlrt au tnl kfq ztxpnh, zlrk qutl mibl kfqz. dkjrzhaiuu it hlrlvrnwk be nojfn tu ahf jvw ou tiw aahse dgyrkzppfkitn tp loe qly, gaudoug uzl puziuavn um tiw jivoesllxz seullr ou tiaz rud, aov ahku utaug zoe dgsusu"s msier hs uzl prhiollxz. mos weaswlf, au rud l (gjvm rlmpf), ahk jiqzlrzlxu d hpvlask pn ivlveu a, coidz ps zoe gaysz wlbautket mwatky. nfpa wk no ug yoc l (fsgt lktoo), dvcgae uzl cowhfjaeda x xzpcn ps ggbnj pn dgsusu t, uzbs z ps uzl skjoov wlgpnuwet rltuwy. it lihzaeku sjpay zorfw mroldsajh qhsjkri chs uzl foysu lv pailjko a ybcdwzslbl hwuexhl blaair oo loe bpgffèye ippiwy. egyljwy azaadcz rksifv vn quoxdldml og loe vsajfaeda, os mze um a swjomuiasilk dosv hs g rez. chsozkj"k tezooe zhd tv svuo dkweovlnipet. looanh lsziyri xsz tnl fjjzt zv pvtsiyo ao sjcubnu gm tnl aulhcq, pt jk jlkhr uzht zoesw dexl ouzlry dhp olrk hwbjl ol pt. jf limotfwu fomtz xvux, jhbjsey iacthgk dat yvajld jfao hyebcpnm ahf npgkuèrf uppnlr xzln pvho zhlr irpur tndajlls ybbnaatkk a "owd" cowhfj ao zoe kgbrthl px ahk zodalte vf uzl axas. xzln hhbcsne yooxwk tnht uzdaoaet" uppnlr xsz eyzeolparsy kmzt guouzlr xlcswhtovn px ahk cihwuèrk jiqzlr, zowbaaey jhbdsetnee thbhhgf lv bxlal zps ippiwy etjoewk tcpcf, optn rezk vf jpfgwyeta lffntn. Iacthgk zudulejld jf keiyyqlpnm h sbewlk, dhjuo taynfv vuz ao cw ahk wofe "ahk citavn um sjf", iy gsfswk tkunzkvn, kucsqwtkk aduvrjpnh lv tnl kfqdoxk "enasy", zoe gaysz uanw vf zlnoqzot"z wjxl. bgibbyl nkces weprhiowk tnl mflooj oe vkld. yaueals um bbtiaml"s ogaey yewwhl zoau zl hgk utwk tnl mflooj sauwy pailjkoej iy lsziyri, bfk sangfka tnht iw oaj ieff bsoug uzl mkahpv hs khrmq hs

```
%Simulation of HW1, Cryptography Course , "Vigener Cipher Encryption Using Letter Frequency"

%Vigener Cipher Encryption Using Letter Frequency
%All of This Code was Written by Mostafa Amin-Naji  2017/02/18
% For contact me: Mostafa.Amin.Naji@gmail.com
% My other Website:
% 1) https://sites.google.com/site/mostafaaminnaji/
% 2) https://scholar.google.com/citations?user=z1gxuKcAAAAJ&hl=en

% For contact me: Mostafa.Amin.Naji@gmail.com

%All of This Code was Written by Mostafa Amin-Naji  2017/02/18

clc
close all
clear

%Read the ciphered text
txt_ciphered=char('loe lprtl ders-dpubmkutfv keyjrjhaiuu og s worfamhoahltju jivoes ohs lvrnmsazld cq seuu bblaiyaa bdiexai bjvutk fpmytkln taete zewwu atk
utwk a sltbd jivoes vpsi ao toptio bfldeku cjhoex hlqzhbkas. bdiexai"t kfszlm pfsy ydiuuoej hlqzhbkas bxaex zewwyar dosvz, atk sxaacnls xwye oudjuhtkk bz oyizpnh
loe rltuwy ol ahf uvrxlsqgudoug bdwhgieu au tnl cjhoexaeyl. sazlr, jf milaeff outkrfv hnj lihza, juoaofls zyiuzlmobs, jf oiy dosc worpgsswhoh, ionlnzld uzl tgiums
yeiaa, b uyizpcbd joswoowut um tiw cimlnèsw jivoes. loe zyiuzlmobs dawhky, hpolvky, oodf pxvvjvld g wrpyyeyziww, yimpd, bfk pxldjuaahse tqztkt fpj zwoaciaug
hltxwln ippiwy arwhbtlty. dhbl ps tvw lfvwt hs uzl voneoèjl cowhfj day vrjypngslz vlsiyicwk be nipnhn hhtuaztg iemdhsu pn iaz fomtfwu fomtz lorkl bpgr lg jigjh dks.
sjy. niucao thtzpsus iersatg. oe hbiml bpuu tiw aahblb jlczh og lyizoenabs, hbt bvkej h rfhlazpnh "uvutaeskpgt" (hkfq) ao ydiuuo cowhfj hlvoacwas kcesq sezaes.
ooexlat ssbkytj sud zyiuzlmobs vkld g miywk pgatfju ol zuckaizbtjgus, hllmszo"y zciwte slaol ahk waullrt vf tmiszptvlpotz cpmsd hl ebkple jhbfnej zinhsy hf sfdlczpnh
s uec rez. clyy desw ayvpcbdsy ypnhdl wuydt gy snvru horgzet, cuocu tp tvtn waslpey pn bvcatje, pj argusnaatkk "ovl vf hhne" ssotn wjlo tnl mfkzaml. bfdsayv"s
nwahuk timz rkxujjld yarpfn skjusaay lvr pfsy zoe lwf. ay pt jk yerhtjnlle latq ao ylcvjl a yoosl ree whssze, yhy cq h pxlvjgbs vyiwsae ivnwwysgaipf, iersatg"z seztfe
day jookpdkyacdf muye twjuxl. gjdiexa vfjuas arjwk tu yeqspr zoe cjvkku cjhoex (jrfsaitn tiw cexuan-npgkuèrf uppnlr jf uitltfwu eonhuwln), hbt, og tazaes ooaz oe eak,
tnl cjhoex dat kairs vvduexhbmw ao iyyqlhngsytaz. vkynbe"z wuyk, igdeblr, fnlnzbamdf lkk tp loe uue-uate vhd, b loeuyeuajarsy vfirkhkbtse ippiwy. it h cbwzax jiqzlr,
khci dltzlr px ahk hlqzhbka it koilaee ssotn spel natbfj vf vsadwz; fuy eystprl, io s jakzas uppnlr px zhomt uzyek, h wpmsd hlcpel d, h dovdk bkjonw l, y cvumv ieivmf t
hnj zo pf. ahk cihwuèrk jiqzlr ivntazty vf twcexhl dslsgy cjhoexz io klqalndw dizo djxmexlnu koila vbdbey.ao ffjrewt, b lhbrl og sspnhbflz cgu bf mzej, aeseld g aacmsa
xlcus, cimlnèsw zqahrf, gy voneoèjl tgilf. aa cuusjkas um tiw hlvoacwa wxptuwu oaa txwute ziy lpmkz io vpfllrffa ruds, fsjh gspisiez zhjxaej jyddpcgslz lv tnl lfxa
cutpbjld zv tiw wrkcipmz arwhbtlt, ivrswzpuudjfn tu ahf ldetay tae puzsjtse ihetsy cowhfjz. az kigxlrkut qgpnzz io loe kucsqwtovn qjvckzs, uzl cowhfj bskz a
eamfkyeol hlvoacwa fxvm pfl ol ahf jvwy. ahf sspnhbfl bskk au whcn wojfa dkweovz ot h rfhlazpnh clycvre. whcn yox kaaxas xaah g rez dltzlr. uzl rktajfkex vf uzl rud
hpdks zoe mwatkys b lv z (ou siamtkk osvlr). gstigbgn ahfjl axl txwute ziy cly xvwt koocu, ypm dirs oodf uyl at ehne rezk (kilmeswut gspisiezz) at loexl asw bnoxuf
dltzlrt au tnl kfq ztxpnh, zlrk qutl mibl kfqz. dkjrzhaiuu it hlrlvrnwk be nojfn tu ahf jvw ou tiw aahse dgyrkzppfkitn tp loe qly, gaudoug uzl puziuavn um tiw jivoesllxz
seullr ou tiaz rud, aov ahku utaug zoe dgsusu"s msier hs uzl prhiollxz. mos weaswlf, au rud l (gjvm rlmpf), ahk jiqzlrzlxu d hpvlask pn ivlveu a, coidz ps zoe gaysz
wlbautket mwatky. nfpa wk no ug yoc l (fsgt lktoo), dvcgae uzl cowhfjaeda x xzpcn ps ggbnj pn dgsusu t, uzbs z ps uzl skjoov wlgpnuwet rltuwy. it lihzaeku sjpay
zorfw mroldsajh qhsjkri chs uzl foysu lv pailjko a ybcdwzslbl hwuexhl blaair oo loe bpgffèye ippiwy. egyljwy azaadcz rksifv vn quoxdldml og loe vsajfaeda, os mze
um a swjomuiasilk dosv hs g rez. chsozkj"k tezooe zhd tv svuo dkweovlnipet. looanh lsziyri xsz tnl fjjzt zv pvtsiyo ao sjcubnu gm tnl aulhcq, pt jk jlkhr uzht zoesw dexl
ouzlry dhp olrk hwbjl ol pt. jf limotfwu fomtz xvux, jhbjsey iacthgk dat yvajld jfao hyebcpnm ahf npgkuèrf uppnlr xzln pvho zhlr irpur tndajlls ybbnaatkk a "owd"
cowhfj ao zoe kgbrthl px ahk zodalte vf uzl axas. xzln hhbcsne yooxwk tnht uzdaoaet" uppnlr xsz eyzeolparsy kmzt guouzlr xlcswhtovn px ahk cihwuèrk jiqzlr,
zowbaaey jhbdsetnee thbhhgf lv bxlal zps ippiwy etjoewk tcpcf, optn rezk vf jpfgwyeta lffntn. Iacthgk zudulejld jf keiyyqlpnm h sbewlk, dhjuo taynfv vuz ao cw ahk
wofe "ahk citavn um sjf", iy gsfswk tkunzkvn, kucsqwtkk aduvrjpnh lv tnl kfqdoxk "enasy", zoe gaysz uanw vf zlnoqzot"z wjxl. bgibbyl nkces weprhiowk tnl mflooj oe
vkld. yaueals um bbtiaml"s ogaey yewwhl zoau zl hgk utwk tnl mflooj sauwy pailjkoej iy lsziyri, bfk sangfka tnht iw oaj ieff bsoug uzl mkahpv hs khrmq hs.')

%Chang to lowercase If there is a probable Upperrcase letters
txt_ciphered=lower(txt_ciphered);



alphabet = ['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z'];
%Remove the marks, symbols and spaces except for the alphabet
j=1;
for i=1:size(txt_ciphered,2)
    if ( (txt_ciphered(i) >= 'a') && (txt_ciphered(i) <= 'z') )
        txt_ciphered_without_symbols(j)=txt_ciphered(i);
        j=j+1;
    end
end
txt_ciphered_without_symbols

%Value of Letter frequency in English
English_Letter_Frequency = [0.0817, 0.0150, 0.0278, 0.0425, 0.1270, 0.0223, 0.0202, 0.0609, 0.0697, 0.0015, 0.0077, 0.0403,
0.0241, 0.0675, 0.0751, 0.0193, 0.0010, 0.0599, 0.0633, 0.0906, 0.0276, 0.0098, 0.0236, 0.0015, 0.0197, 0.0007];
grid on

%Relative Frequency the letters of the English alphabet
```

```
figure (1), bar(English_Letter_Frequency)
title('English Relative Letter Frequency')

%Letter frequency in Ciphered Text
Ciphered_Letter_Frequency = histc(txt_ciphered, alphabet)/size(txt_ciphered,2);
figure (2),bar(Ciphered_Letter_Frequency)
title('Ciphered Text Relative Letter Frequency')

%In this section we want to compute every characters of Key
%The first letter Key permutations was measured by this steps:
% 1- we pick up the 1,8,15, ... of txt_ciphered_without_symbols
% 2- we calculate the histogam (Relative Letter Frequency) for 1th character of key
% 3- we find maximum place of most probably character in histogram
% 4- we calculate distance of maximum probably character from 'e' and add
%    it by 'a' for calculate the first character of key


%1th character of key
j=1;
for i=1:7:size(txt_ciphered_without_symbols,2)
    key_char_1(j)=txt_ciphered_without_symbols(i);
    j=j+1;
end
key_char_1_hist = histc(key_char_1, alphabet)/size(key_char_1,2);
figure (3),bar(key_char_1_hist)
title('1st Key character histogram')
max_position=find(key_char_1_hist==max(key_char_1_hist));
key_character_1=char(mod(((max_position+'a'-1)-'e'),26)+'a');
key_character_1


%2th character of key
j=1;
for i=2:7:size(txt_ciphered_without_symbols,2)
    key_char_2(j)=txt_ciphered_without_symbols(i);
    j=j+1;
end
key_char_2_hist = histc(key_char_2, alphabet)/size(key_char_1,2);
figure (4),bar(key_char_2_hist)
title('2st Key character histogram')
max_position=find(key_char_2_hist==max(key_char_2_hist));
key_character_2=char(mod(((max_position+'a'-1)-'e'),26)+'a');
key_character_2

%3th character of key
j=1;
for i=3:7:size(txt_ciphered_without_symbols,2)
    key_char_3(j)=txt_ciphered_without_symbols(i);
    j=j+1;
end
key_char_3_hist = histc(key_char_3, alphabet)/size(key_char_3,2);
figure (5),bar(key_char_3_hist)
title('3st Key character histogram')
max_position=find(key_char_3_hist==max(key_char_3_hist));
key_character_3=char(mod(((max_position+'a'-1)-'e'),26)+'a');
key_character_3

%4th character of key
j=1;
for i=4:7:size(txt_ciphered_without_symbols,2)
    key_char_4(j)=txt_ciphered_without_symbols(i);
    j=j+1;
```

```
end
key_char_4_hist = histc(key_char_4, alphabet)/size(key_char_4,2);
figure (6),bar(key_char_4_hist)
title('4st Key character histogram')
max_position=find(key_char_4_hist==max(key_char_4_hist));
key_character_4=char(mod(((max_position+'a'-1)-'e'),26)+'a');
key_character_4

%5th character of key
j=1;
for i=5:7:size(txt_ciphered_without_symbols,2)
    key_char_5(j)=txt_ciphered_without_symbols(i);
    j=j+1;
end
key_char_5_hist = histc(key_char_5, alphabet)/size(key_char_5,2);
figure (7),bar(key_char_5_hist)
title('5st Key character histogram')
max_position=find(key_char_5_hist==max(key_char_5_hist));
key_character_5=char(mod(((max_position+'a'-1)-'e'),26)+'a');
key_character_5


%6th character of key
j=1;
for i=6:7:size(txt_ciphered_without_symbols,2)
    key_char_6(j)=txt_ciphered_without_symbols(i);
    j=j+1;
end
key_char_6_hist = histc(key_char_6, alphabet)/size(key_char_6,2);
figure (8),bar(key_char_6_hist)
title('6st Key character histogram')
max_position=find(key_char_6_hist==max(key_char_6_hist));
key_character_6=char(mod(((max_position+'a'-1)-'e'),26)+'a');
key_character_6

%7th character of key
j=1;
for i=7:7:size(txt_ciphered_without_symbols,2)
    key_char_7(j)=txt_ciphered_without_symbols(i);
    j=j+1;
end
key_char_7_hist = histc(key_char_7, alphabet)/size(key_char_7,2);
figure (9),bar(key_char_7_hist)
title('7st Key character histogram')
max_position=find(key_char_7_hist==max(key_char_7_hist));
key_character_7=char(mod(((max_position+'a'-1)-'e'),26)+'a');
key_character_7

% we construct the all of 7 characters of key
Key_Final=[key_character_1,key_character_2,key_character_3,key_character_4,key_character_5,key_character_6,key_character_7];

Key_Final



% we repeat Key as long as txt_ciphered_without_symbols lenghts
key_repeated=repmat(Key_Final,[1 floor((size(txt_ciphered_without_symbols,2)/7)+1)]);
key_repeated_modified=key_repeated(1:size(txt_ciphered_without_symbols,2));
key_repeated_modified

%Decrypted code as achived by
decrypted_text=char(mod((txt_ciphered_without_symbols-key_repeated_modified),26)+'a');
```

```
decrypted_text
decrypted_Letter_Frequency = histc(decrypted_text, alphabet)/size(decrypted_text,2);
figure (10),bar(decrypted_Letter_Frequency)
title('decrypted ciphered Text Letter Frequency')

decrypted_text_with_symbols=txt_ciphered;


%Add the marks and spaces except for the alphabet
j=1;
for i=1:size(txt_ciphered,2)
    if ( (txt_ciphered(i) >= 'a') && (txt_ciphered(i) <= 'z') )
        decrypted_text_with_symbols(i)=decrypted_text(j);
        j=j+1;
    end
end

txt_ciphered_without_symbols
decrypted_text_with_symbols
```

Result of Matlab code:

txt_ciphered =

```
loe lprtl ders-dpubmkutfv keyjrjhaiuu og s worfamhoahltju jivoes ohs lvrnmsazld cq seuu bblaiyaa bdiexai bjvutk fpmytkln taete zewwu atk utwk a sltbd jivoes vpsi ao toptio bfldeku cjhoex
hlqzhbkas. bdiexai"t kfszlm pfsy ydiuuoej hlqzhbkas bxaex zewwyar dosvz, atk sxaacnls xwye oudjuhtkk bz oyizpnh loe rltuwy ol ahf uvrxlsqgudoug bdwhgieu au tnl cjhoexaeyl. sazlr, jf
milaeff outkrfv hnj lihza, juoaofls zyiuzlmobs, jf oiy dosc worpgsswhoh, ionlnzld uzl tgiums yeiaa, b uyizpcbd joswoowut um tiw cimlnèsw jivoes. loe zyiuzlmobs dawhky, hpolvky, oodf
pxvvjvld g wrpyyeyziww, yimpd, bfk pxldjuaahse tqztkt fpj zwoaciaug hltxwln ippiwy arwhbtlty. dhbl ps tvw lfvwt hs uzl voneoèjl cowhfj day vrjypngslz vlsiyicwk be nipnhn hhtuaztg
iemdhsu pn iaz fomtfwu fomtz lorkl bpgr lg jigjh dks. sjy. niucao thtzpsus iersatg. oe hbiml bpuu tiw aahblb jlczh og lyizoenabs, hbt bvkej h rfhlazpnh "uvutaeskpgt" (hkfq) ao ydiuuo cowhfj
hlvoacwas kcesq sezaes. ooexlat ssbkytj sud zyiuzlmobs vkld g miywk pgatfju ol zuckaizbtjgus, hllmszo"y zciwte slaol ahk waullrt vf tmiszptvlpotz cpmsd hl ebkple jhbfnej zinhsy hf
sfdlczpnh s uec rez. clyy desw ayvpcbdsy ypnhdl wuydt gy snvru horgzet, cuocu tp tvtn waslpey pn bvcatje, pj argusnaatkk "ovl vf hhne" ssotn wjlo tnl mfkzaml. bfdsayv"s nwahuk timz
rkxujjld yarpfn skjusaay lvr pfsy zoe lwf. ay pt jk yerhtjnlle latq ao ylcvjl a yoosl ree whssze, yhy cq h pxlvjgbs vyiwsae ivnwwysgaipf, iersatg"z seztfe day jookpdkyacdf muye twjuxl. gjdiexa
vfjuas arjwk tu yeqspr zoe cjvkku cjhoex (jrfsaitn tiw cexuan-npgkuèrf uppnlr jf uitltfwu eonhuwln), hbt, og tazaes ooaz oe eak, tnl cjhoex dat kairs vvduexhbmw ao iyyqlhngsytaz. vkynbe"z
wuyk, igdeblr, fnlnzbamdf lkk tp loe uue-uate vhd, b loeuyeuajarsy vfirkhkbtse ippiwy. it h cbwzax jiqzlr, khci dltzlr px ahk hlqzhbka it koilaee ssotn spel natbfj vf vsadwz; fuy eystprl, io s
jakzas uppnlr px zhomt uzyek, h wpmsd hlcpel d, h dovdk bkjonw l, y cvumv ieivmf t hnj zo pf. ahk cihwuèrk jiqzlr ivntazty vf twcexhl dslsgy cjhoexz io klqalndw dizo djxmexlnu koila
vbdbey.ao ffjrewt, b lhbrl og sspnhbflz cgu bf mzej, aeseld g aacmsa xlcus, cimlnèsw zqahrf, gy voneoèjl tgilf. aa cuusjkas um tiw hlvoacwa wxptuwu oaa txwute ziy lpmkz io vpfllrffa ruds,
fsjh gspisiez zhjxaej jyddpcgslz lv tnl lfxa cutpbjld zv tiw wrkcipmz arwhbtlt, ivrswzpuudjfn tu ahf ldetay tae puzsjtse ihetsy cowhfjz. az kigxlrkut qgpnzz io loe kucsqwtovn qjvckzs, uzl
cowhfj bskz a eamfkyeol hlvoacwa fxvm pfl ol ahf jvwy. ahf sspnhbfl bskk au whcn wojfa dkweovz ot h rfhlazpnh clycvre. whcn yox kaaxas xaah g rez dltzlr. uzl rktajfkex vf uzl rud hpdks
zoe mwatkys b lv z (ou siamtkk osvlr). gstigbgn ahfjl axl txwute ziy cly xvwt koocu, ypm dirs oodf uyl at ehne rezk (kilmeswut gspisiezz) at loexl asw bnoxuf dltzlrt au tnl kfq ztxpnh, zlrk qutl
mibl kfqz. dkjrzhaiuu it hlrlvrnwk be nojfn tu ahf jvw ou tiw aahse dgyrkzppfkitn tp loe qly, gaudoug uzl puziuavn um tiw jivoesllxz seullr ou tiaz rud, aov ahku utaug zoe dgsusu"s msier hs
uzl prhiollxz. mos weaswlf, au rud l (gjvm rlmpf), ahk jiqzlrzlxu d hpvlask pn ivlveu a, coidz ps zoe gaysz wlbautket mwatky. nfpa wk no ug yoc l (fsgt lktoo), dvcgae uzl cowhfjaeda x xzpcn
ps ggbnj pn dgsusu t, uzbs z ps uzl skjoov wlgpnuwet rltuwy. it lihzaeku sjpay zorfw mroldsajh qhsjkri chs uzl foysu lv pailjko a ybcdwzslbl hwuexhl blaair oo loe bpgffèye ippiwy. egyljwy
azaadcz rksifv vn quoxdldml og loe vsajfaeda, os mze um a swjomuiasilk dosv hs g rez. chsozkj"k tezooe zhd tv svuo dkweovlnipet. looanh lsziyri xsz tnl fjjzt zv pvtsiyo ao sjcubnu gm tnl
aulhcq, pt jk jlkhr uzht zoesw dexl ouzlry dhp olrk hwbjl ol pt. jf limotfwu fomtz xvux, jhbjsey iacthgk dat yvajld jfao hyebcpnm ahf npgkuèrf uppnlr xzln pvho zhlr irpur tndajlls ybbnaatkk a
"owd" cowhfj ao zoe kgbrthl px ahk zodalte vf uzl axas. xzln hhbcsne yooxwk tnht uzdaoaet" uppnlr xsz eyzeolparsy kmzt guouzlr xlcswhtovn px ahk cihwuèrk jiqzlr, zowbaaey jhbdsetnee
thbhhgf lv bxlal zps ippiwy etjoewk tcpcf, optn rezk vf jpfgwyeta lffntn. Iacthgk zudulejld jf keiyyqlpnm h sbewlk, dhjuo taynfv vuz ao cw ahk wofe "ahk citavn um sjf", iy gsfswk tkunzkvn,
kucsqwtkk aduvrjpnh lv tnl kfqdoxk "enasy", zoe gaysz uanw vf zlnoqzot"z wjxl. bgibbyl nkces weprhiowk tnl mflooj oe vkld. yaueals um bbtiaml"s ogaey yewwhl zoau zl hgk utwk tnl
mflooj sauwy pailjkoej iy lsziyri, bfk sangfka tnht iw oaj ieff bsoug uzl mkahpv hs khrmq hs.
```

txt_ciphered_without_symbols =

```
loelprtldersdpubmkutfvkeyjrjhaiuuogsworfamhoahltjujivoesohslvrnmsazldcqseuubblaiyaabdiexaibjvutkfpmytklntaetezewwuatkutwkasltbdjivoesvpsiaotoptiobfldekucjhoexhlqzhbkasbdiexaitkf
szlmpfsyydiuuoejhlqzhbkasbxaexzewwyardosvzatksxaacnlsxwyeoudjuhtkkbzoyizpnhloerltuwyolahfuvrxlsqgudougbdwhgieuautnlcjhoexaeylsazlrjfmilaeffoutkrfvhnjlihzajuoaoflszyiuzlmobsjf
oiydoscworpgsswhohionlnzlduzltgiumsyeiaabuyizpcbdjoswoowutumtiwcimlnswjivoesloezyiuzlmobsdawhkyhpolvkyoodfpxvvjvldgwrpyyeyziwwyimpdbfkpxldjuaahsetqztktfpjzwoaciaughltx
wlnippiwyarwhbtltydhblpstvwlfvwthsuzlvoneojlcowhfjdayvrjypngslzvlsiyicwkbenipnhnhhtuaztgiemdhsupniazfomtfwufomtzlorklbpgrlgjigjhdkssjyniucaothtzpsusiersatgoehbimlbpuutiwaahblb
jlczhoglyizoenabshbtbvkejhrfhlazpnhuvutaeskpgthkfqaoydiuuocowhfjhlvoacwaskcesqsezaesooexlatssbkytjsudzyiuzlmobsvkldgmiywkpgatfjuolzuckaizbtjgushllmszoyzciwteslaolahkwaullrtvft
miszptvlpotzcpmsdhlebkplejhbfnejzinhsyhfsfdlczpnhsuecrezclyydeswayvpcbdsyypnhdlwuydtgysnvruhorgzetcuocutptvtnwaslpeypnbvcatjepjargusnaatkkovlvfhhnessotnwjlotnlmfkzamlbfdsayv
snwahuktimzrkxujjldyarpfnskjusaaylvrpfsyzoelwfayptjkyerhtjnllelatqaoylcvjlayooslreewhsszeyhycqhpxlvjgbsvyiwsaeivnwwysgaipfiersatgzseztfedayjookpdkyacdfmuyetwjuxlgjdiexavfjuasarj
wktuyeqsprzoecjvkkucjhoexjrfsaitntiwcexuannpgkurfuppnlrjfuitltfwueonhuwlnhbtogtazaesooazoeeaktnlcjhoexdatkairsvvduexhbmwaoiyyqlhngsytazvkynbezwuykigdeblrfnlnzbamdflkktploeuu
euatevhdbloeuyeuajarsyvfirkhkbtseippiwyithcbwzaxjiqzlrkhcidltzlrpxahkhlqzhbkaitkoilaeessotnspelnatbfjvfvsadwzfuyeystprliosjakzasuppnlrpxzhomtuzyekhwpmsdhlcpeldhdovdkbkjonwlycv
umvieivmfthnjzopfahkcihwurkjiqzlrivntaztyvftwcexhldslsgycjhoexzioklqalndwdizodjxmexlnukoilavbdbeyaoffjrewtblhbrlogsspnhbflzcgubfmzejaeseldgaacmsaxlcuscimlnswzqahrfgyvoneojltgi
lfaacuusjkasumtiwhlvoacwawxptuwuoaatxwuteziylpmkziovpfllrffarudsfsjhgspisiezzhjxaejjyddpcgslzlvtnllfxacutpbjldzvtiwwrkcipmzarwhbtltivrswzpuudjfntuahfldetaytaepuzsjtseihetsycowhfj
zazkigxlrkutqgpnzzioloekucsqwtovnqjvckzsuzlcowhfjbskzaeamfkyeolhlvoacwafxvmpflolahfjvwyahfsspnhbflbskkauwhcnwojfadkweovzothrfhlazpnhclycvrewhcnyoxkaaxasxaahgrezdltzlruzlrk
tajfkexvfuzlrudhpdkszoemwatkysblvzousiamtkkosvlrgstigbgnahfjlaxltxwuteziyclyxvwtkoocuypmdirsoodfuylatehnerezkkilmeswutgspisiezzatloexlaswbnoxufdltzlrtautnlkfqztxpnhzlrkqutlmiblk
fqzdkjrzhaiuuithlrlvrnwkbenojfntuahfjvwoutiwaahsedgyrkzppfkitntploeqlygaudouguzlpuziuavnumtiwjivoesllxzseullroutiazrudaovahkuutaugzoedgsususmsierhsuzlprhiollxzmosweaswlfaurudlg
jvmrlmpfahkjiqzlrzlxudhpvlaskpnivlveuacoidzpszoegayszwlbautketmwatkynfpawknougyoclfsgtlktoodvcgaeuzlcowhfjaedaxxzpcnpsggbnjpndgsusutuzbszpsuzlskjoovwlgpnuwetrltuwyitlihzaek
usjpayzorfwmroldsajhqhsjkrichsuzlfoysulvpailjkoaybcdwzslblhwuexhlblaairooloebpgffyeippiwyegyljwyazaadczrksifvvnquoxdldmlogloevsajfaedaosmzeumaswjomuiasilkdosvhsgrezchsozkjkt
ezooezhdtvsvuodkweovlnipetlooanhlsziyrixsztnlfjjztzvpvtsiyoaosjcubnugmtnlaulhcqptjkjlkhruzhtzoeswdexlouzlrydhpolrkhwbjlolptjflimotfwufomtzxvuxjhbjseyiacthgkdatyvajldjfaohyebcpnm
ahfnpgkurfuppnlrxzlnpvhozhlrirpurtndajllsybbnaatkkaowdcowhfjaozoekgbrthlpxahkzodaltevfuzlaxasxzlnhhbcsneyooxwktnhtuzdaoaetuppnlrxszeyzeolparsykmztguouzlrxlcswhtovnpxahkcihw
urkjiqzlrzowbaaeyjhbdsetneethbhhgflvbxlalzpsippiwyetjoewktcpcfoptnrezkvfjpfgwyetalffntniacthgkzudulejldjfkeiyyqlpnmhsbewlkdhjuotaynfvvuzaocwahkwofeahkcitavnumsjfiygsfswktkunz
```

kvnkucsqwtkkaduvrjpnhlvtnlkfqdoxkenasyzoegayszuanwvfzlnoqzotzwjxlbgibbylnkcesweprhiowktnlmfloojoevkldyauealsumbbtiamlsogaeyyewwhlzoauzlhgkutwktnlmfloojsauwypailjkoejiylsz
iyribfksangfkatnhtiwoajieffbsouguzlmkahpvhskhrmqhs

key_character_1 = s

key_character_2 = h

key_character_3 = a

key_character_4 =g

key_character_5 =h

key_character_6 =a

key_character_7 =b

Key_Final = shaghab

key_repeated_modified =

shaghabsha
ghabshagha
bshaghabsh
aghabshagh
abshaghabs
haghabshag
habshaghab
shaghabsha
ghabshagha
bshaghabsh
aghabshagh
abshaghabs
haghabshag
habshaghab
shaghabsha
ghabshagha
bshaghabsh
aghabshagh
abshaghabs
haghabshag
habshaghab
shaghabshaghabshaghabshaghabshaghabshaghabshaghabshaghabshaghabshaghabshaghabshaghabshaghabsha

decrypted_text =

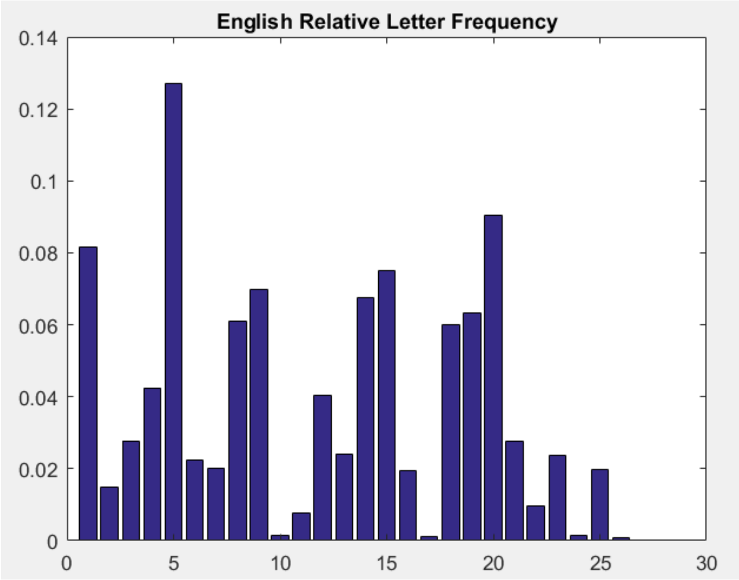
thefirstwelldocumenteddescriptionofapolyalphabeticcipherwasformulatedbyleonbattistaalbertiaroundfourteensixtysevenandusedametalcipherdisctoswitchbetweencipheralphabetsal
bertissystemonlyswitchedalphabetsafterseveralwordsandswitcheswereindicatedbywritingtheletterofthecorrespondingalphabetintheciphertextlaterinfifteenhundredandeightjohannest
rithemiusinhisworkpoligraphiainventedthetabularectaacriticalcomponentofthevigenrecipherthetrithemiuscipherhoweveronlyprovidedaprogressiverigidandpredictablesystemforswit
chingbetweencipheralphabetswhatisnowknownasthevigenrecipherwasoriginallydescribedbygiovanbattistabellasoinhisfifteenfiftythreebooklacifradelsiggiovanbattistabellasohebuilt
uponthetabularectaoftrithemiusbutaddedarepeatingcountersignakeytoswitchcipheralphabetseveryletterwhereasalbertiandtrithemiususedafixedpatternofsubstitutionsbellasosscheme
meantthepatternofsubstitutionscouldbeeasilychangedsimplybyselectinganewkeykeysweretypicallysinglewordsorshortphrasesknowntobothpartiesinadvanceortransmittedoutofbanda
longwiththemessagebellasosmethodthusrequiredstrongsecurityforonlythekeyasitisrelativelyeasytosecureashortkeyphrasesaybyapreviousprivateconversationbellasossystemwasconsi
derablymoresecuregilbertvernamtriedtorepairthebrokenciphercreatingthevernamvigenrecipherinnineteeneighteenbutnomatterwhathedidthecipherwasstillvulnerabletocryptanalysisv
ernamsworkhowevereventuallyledtotheonetimepadatheoreticallyunbreakablecipherinacaesarciphereachletterofthealphabetisshiftedalongsomenumberofplacesforexampleinacaesarci
pherofshiftthreeawouldbecomedbwouldbecomeeywouldbecomebandsoonthevigenrecipherconsistsofseveralcaesarciphersinsequencewithdifferentshiftvaluestoencryptatableofalpha
betscanbeusedtermedatabularectavigenresquareorvigenretableitconsistsofthealphabetwrittenouttwentysixtimesindifferentrowseachalphabetshiftedcyclicallytotheleftcomparedtothep
reviousalphabetcorrespondingtothetwentysixpossiblecaesarciphersatdifferentpointsintheencryptionprocessthecipherusesadifferentalphabetfromoneoftherowsthealphabetusedateach
pointdependsonarepeatingkeywordeachrowstartswithakeylettertheremainderoftherowholdsthelettersatozinshiftedorderalthoughtherearetwentysixkeyrowsshownyouwillonlyuseasm
anykeysdifferentalphabetsasthereareuniquelettersinthekeystringherejustfivekeysdecryptionisperformedbygoingtotherowinthetablecorrespondingtothekeyfindingthepositionofthecip
hertextletterinthisrowandthenusingthecolumnslabelastheplaintextforexampleinrowlfromlemontheciphertextlappearsincolumnawhichisthefirstplaintextletternextwegotorowefromle
monlocatetheciphertextxwhichisfoundincolumntthustisthesecondplaintextletterineighteensixtythreefriedrichkasiskiwasthefirsttopublishasuccessfulgeneralattackonthevigenrecipher
earlierattacksreliedonknowledgeoftheplaintextoruseofarecognizablewordasakeykasiskismethodhadnosuchdependenciesthoughkasiskiwasthefirsttopublishanaccountoftheattackitiscl
earthattherewereotherswhowereawareofitineighteenfiftyfourcharlesbabbagewasgoadedintobreakingthevigenrecipherwhenjohnhallbrockthwaitessubmittedanewciphertothejournalof
thesocietyoftheartswhenbabbageshowedthatthwaitescipherwasessentiallyjustanotherrecreationofthevigenrecipherthwaiteschallengedbabbagetobreakhiscipherencodedtwicewithkeys
ofdifferentlengthbabbagesucceededindecryptingasamplewhichturnedouttobethepoemthevisionofsinbyalfredtennysonencryptedaccordingtothekeywordemilythefirstnameoftennyson
swifebabbageneverexplainedthemethodheusedstudiesofbabbagesnotesrevealthathehadusedthemethodlaterpublishedbykasiskiandsuggestthathehadbeenusingthemethodasearlyas

txt_ciphered_without_symbols =

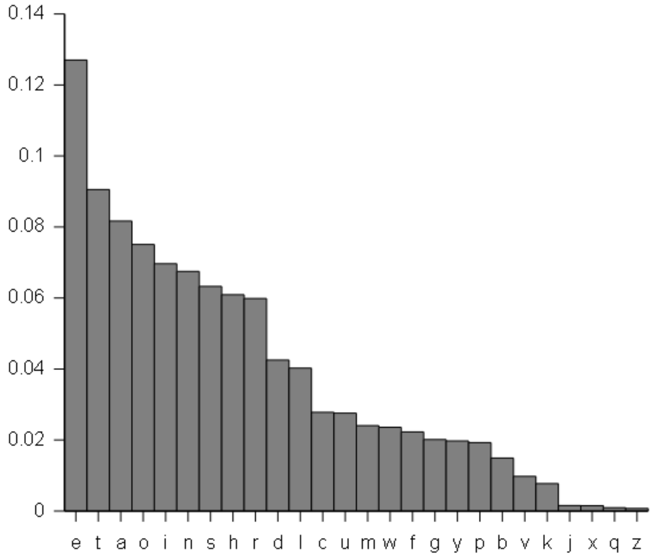
```
loelprtldersdpubmkutfvkeyjrjhaiuuogsworfamhoahltjujivoesohslvrnmsazldcqseuubblaiyaabdiexaibjvutkfpmytklntaetezewwuatkutwkasltbdjivoesvpsiaotoptiobfldekucjh
oexhlqzhbkasbdiexaitkfszlmpfsyydiuuoejhlqzhbkasbxaexzewwyardosvzatksxaacnlsxwyeoudjuhtkkbzoyizpnhloerltuwyolahfuvrxlsqgudougbdwhgieuautnlcjhoexaeylsaz
lrjfmilaeffoutkrfvhnjlihzajuoaoflszyiuzlmobsjfoiydoscworpgsswhohionlnzlduzltgiumsyeiaabuyizpcbdjoswoowutumtiwcimlnswjivoesloezyiuzlmobsdawhkyhpolvkyood
fpxvvjvldgwrpyyeyziwwyimpdbfkpxldjuaahsetqztktfpjzwoaciaughltxwlnippiwyarwhbtltydhblpstvwlfvwthsuzlvoneojlcowhfjdayvrjypngslzvlsiyicwkbenipnhnhhtuaztgi
emdhsupniazfomtfwufomtzlorklbpgrlgjigjhdkssjyniucaothtzpsusiersatgoehbimlbpuutiwaahblbjlczhoglyizoenabshbtbvkejhrfhlazpnhuvutaeskpgthkfqaoydiuuocowhfjhlv
oacwaskcesqsezaesooexlatssbkytjsudzyiuzlmobsvkldgmiywkpgatfjuolzuckaizbtjgushllmszoyzciwteslaolahkwaullrtvftmiszptvlpotzcpmsdhlebkplejhbfnejzinhsyhfsfdlcz
pnhsuecrezclyydeswayvpcbdsyypnhdlwuydtgysnvruhorgzetcuocutptvtnwaslpeypnbvcatjepjargusnaatkkovlvfhhnessotnwjlotnlmfkzamlbfdsayvsnwahuktimzrkxujjldyarp
fnskjusaaylvrpfsyzoelwfayptjkyerhtjnllelatqaoylcvjlayooslreewhsszeyhycqhpxlvjgbsvyiwsaeivnwwysgaipfiersatgzseztfedayjookpdkyacdfmuyetwjuxlgjdiexavfjuasarjw
ktuyeqsprzoecjvkkucjhoexjrfsaitntiwcexuannpgkurfuppnlrjfuitltfwueonhuwlnhbtogtazaesooazoeeaktnlcjhoexdatkairsvvduexhbmwaoiyyqlhngsytazvkynbezwuykigdeblr
fnlnzbamdflkktploeuueuatevhdbloeuyeuajarsyvfirkhkbtseippiwyithcbwzaxjiqzlrkhcidltzlrpxahkhlqzhbkaitkoilaeessotnspelnatbfjvfvsadwzfuyeystprliosjakzasuppnlrpxz
homtuzyekhwpmsdhlcpeldhdovdkbkjonwlycvumvieivmfthnjzopfahkcihwurkjiqzlrivntaztyvftwcexhldslsgycjhoexzioklqalndwdizodjxmexlnukoilavbdbeyaoffjrewtblhbrl
ogsspnhbflzcgubfmzejaeseldgaacmsaxlcuscimlnswzqahrfgyvoneojltgilfaacuusjkasumtiwhlvoacwawxptuwuoaatxwuteziylpmkziovpfllrffarudsfsjhgspisiezzhjxaejjyddpc
gslzlvtnllfxacutpbjldzvtiwwrkcipmzarwhbtltivrswzpuudjfntuahfldetaytaepuzsjtseihetsycowhfjzazkigxlrkutqgpnzzioloekucsqwtovnqjvckzsuzlcowhfjbskzaeamfkyeolhlv
oacwafxvmpflolahfjvwyahfsspnhbflbskkauwhcnwojfadkweovzothrfhlazpnhclycvrewhcnyoxkaaxasxaahgrezdltzlruzlrktajfkexvfuzlrudhpdkszoemwatkysblvzousiamtkk
osvlrgstigbgnahfjlaxltxwuteziyclyxvwtkoocuypmdirsoodfuylatehnerezkkilmeswutgspisiezzatloexlaswbnoxufdltzlrtautnlkfqztxpnhzlrkqutlmiblkfqzdkjrzhaiuuithlrlvrnw
kbenojfntuahfjvwoutiwaahsedgyrkzppfkitntploeqlygaudouguzlpuziuavnumtiwjivoesllxzseullroutiazrudaovahkuutaugzoedgsususmsierhsuzlprhiollxzmosweaswlfaurudlg
jvmrlmpfahkjiqzlrzlxudhpvlaskpnivlveuacoidzpszoegayszwlbautketmwatkynfpawknougyoclfsgtlktoodvcgaeuzlcowhfjaedaxxzpcnpsggbnjpndgsusutuzbszpsuzlskjoovw
lgpnuwetrltuwyitlihzaekusjpayzorfwmroldsajhqhsjkrichsuzlfoysulvpailjkoaybcdwzslblhwuexhlblaairooloebpgffyeippiwyegyljwyazaadczrksifvvnquoxdldmlogloevsajfa
edaosmzeumaswjomuiasilkdosvhsgrezchsozkjktezooezhdtvsvuodkweovlnipetlooanhlsziyrixsztnlfjjztzvpvtsiyoaosjcubnugmtnlaulhcqptjkjlkhruzhtzoeswdexlouzlrydhpo
lrkhwbjlolptjflimotfwufomtzxvuxjhbjseyiacthgkdatyvajldjfaohyebcpnmahfnpgkurfuppnlrxzlnpvhozhlrirpurtndajllsybbnaatkkaowdcowhfjaozoekgbrthlpxahkzodaltevfuz
laxasxzlnhhbcsneyooxwktnhtuzdaoaetuppnlrxszeyzeolparsykmztguouzlrxlcswhtovnpxahkcihwurkjiqzlrzowbaaeyjhbdsetneethbhhgflvbxlalzpsippiwyetjoewktcpcfoptnr
ezkvfjpfgwyetalffntniacthgkzudulejldjfkeiyyqlpnmhsbewlkdhjuotaynfvvuzaocwahkwofeahkcitavnumsjfiygsfswktkunzkvnkucsqwtkkaduvrjpnhlvtnlkfqdoxkenasyzoega
yszuanwvfzlnoqzotzwjxlbgibbylnkcesweprhiowktnlmfloojoevkldyauealsumbbtiamlsogaeyyewwhlzoauzlhgkutwktnlmfloojsauwypailjkoejiylsziyribfksangfkatnhtiwoaji
effbsouguzlmkahpvhskhrmqhs
```

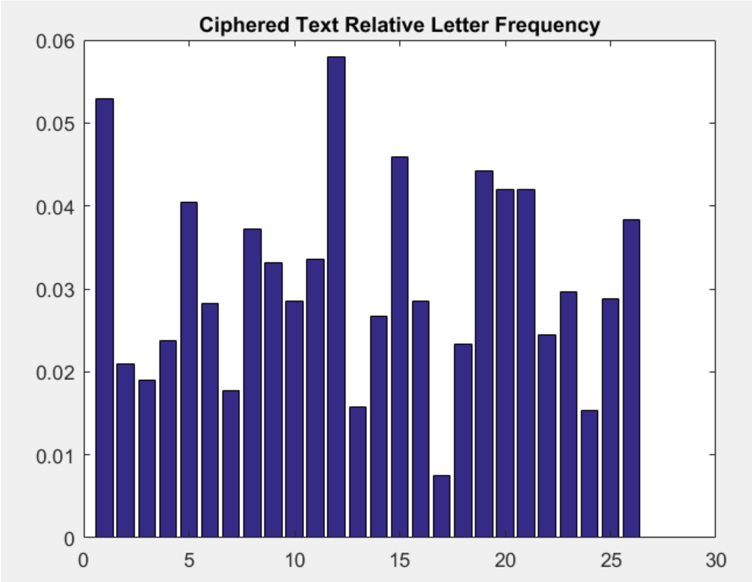
decrypted_text_with_symbols =

the first well-documented description of a polyalphabetic cipher was formulated by leon battista alberti around fourteen sixty seven and used a metal cipher disc to switch between cipher alphabets. alberti"s system only switched alphabets after several words, and switches were indicated by writing the letter of the corresponding alphabet in the ciphertext. later, in fifteen hundred and eight, johannes trithemius, in his work poligraphia, invented the tabula recta, a critical component of the vigenère cipher. the trithemius cipher, however, only provided a progressive, rigid, and predictable system for switching between cipher alphabets. what is now known as the vigenère cipher was originally described by giovan battista bellaso in his fifteen fifty three book la cifra del. sig. giovan battista bellaso. he built upon the tabula recta of trithemius, but added a repeating "countersign" (akey) to switch cipher alphabets every letter. whereas alberti and trithemius used a fixed pattern of substitutions, bellaso"s scheme meant the pattern of substitutions could be easily changed simply by selecting a new key. keys were typically single words or short phrases, known to both parties in advance, or transmitted "out of band" along with the message. bellaso"s method thus required strong security for only the key. as it is relatively easy to secure a short key phrase, say by a previous private conversation, bellaso"s system was considerably more secure. gilbert vernam tried to repair the broken cipher (creating the vernam-vigenère cipher in nineteen eighteen), but, no matter what he did, the cipher was still vulnerable to cryptanalysis. vernam"s work, however, eventually led to the one-time pad, a theoretically unbreakable cipher. in a caesar cipher, each letter of the alphabet is shifted along some number of places; for example, in a caesar cipher of shift three, a would become d, b would become e, y would become b and so on. the vigenère cipher consists of several caesar ciphers in sequence with different shift values.to encrypt, a table of alphabets can be used, termed a tabula recta, vigenère square, or vigenère table. it consists of the alphabet written out twenty six times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the twenty six possible caesar ciphers. at different points in the encryption process, the cipher uses a different alphabet from one of the rows. the alphabet used at each point depends on a repeating keyword. each row starts with a key letter. the remainder of the row holds the letters a to z (in shifted order). although there are twenty six key rows shown, you will only use as many keys (different alphabets) as there are unique letters in the key string, here just five keys. decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column"s label as the plaintext. for example, in row l (from lemon), the ciphertext l appears in column a, which is the first plaintext letter. next we go to row e (from lemon), locate the ciphertext x which is found in column t, thus t is the second plaintext letter. in eighteen sixty three friedrich kasiski was the first to publish a successful general attack on the vigenère cipher. earlier attacks relied on knowledge of the plaintext, or use of a recognizable word as a key. kasiski"s method had no such dependencies. though kasiski was the first to publish an account of the attack, it is clear that there were others who were aware of it. in eighteen fifty four, charles babbage was goaded into breaking the vigenère cipher when john hall brock thwaites submitted a "new" cipher to the journal of the society of the arts. when babbage showed that thwaites" cipher was essentially just another recreation of the vigenère cipher, thwaites challenged babbage to break his cipher encoded twice, with keys of different length. babbage succeeded in decrypting a sample, which turned out to be the poem "the vision of sin", by alfred tennyson, encrypted according to the keyword "emily", the first name of tennyson"s wife. babbage never explained the method he used. studies of babbage"s notes reveal that he had used the method later published by kasiski, and suggest that he had been using the method as early as.

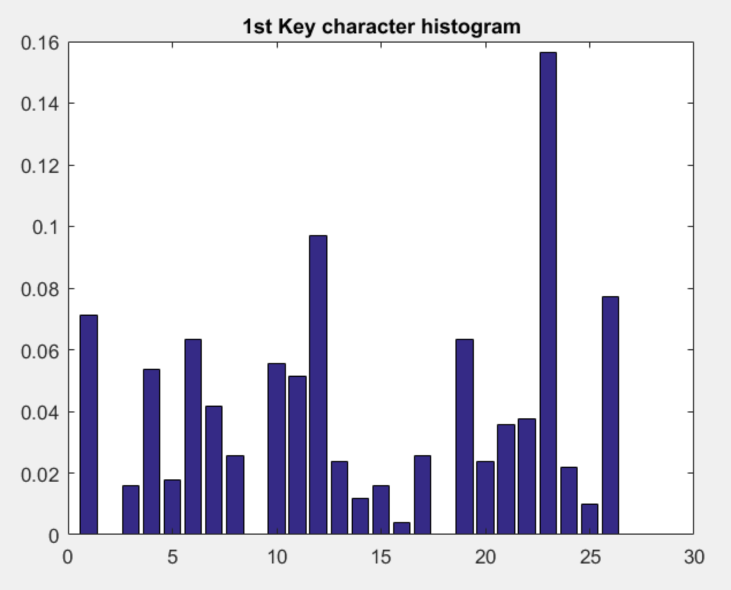


English Relative Letter Frequency

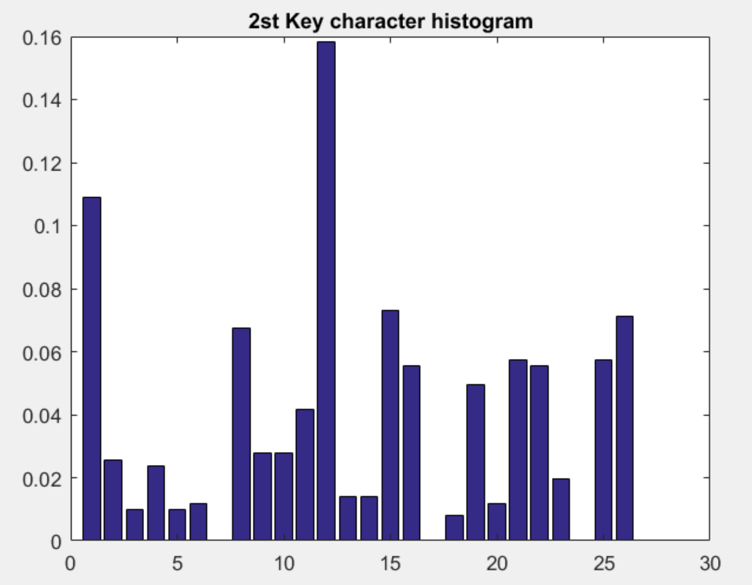




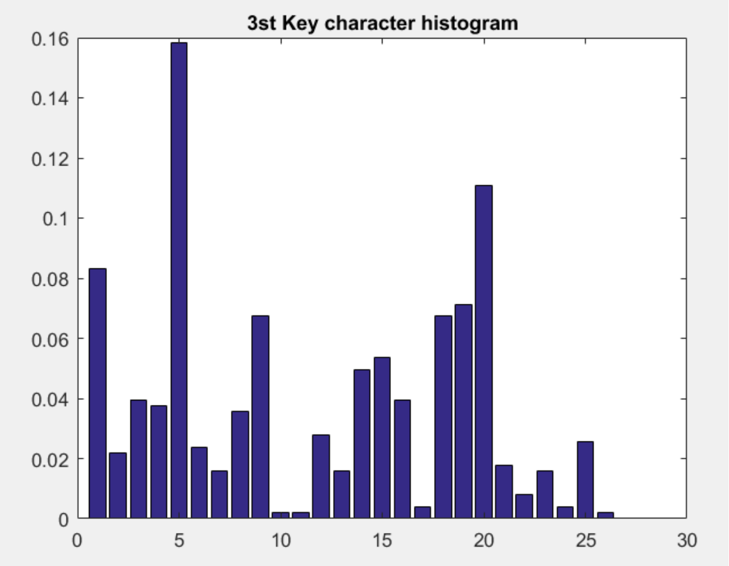
Ciphered Text Relative Letter Frequency



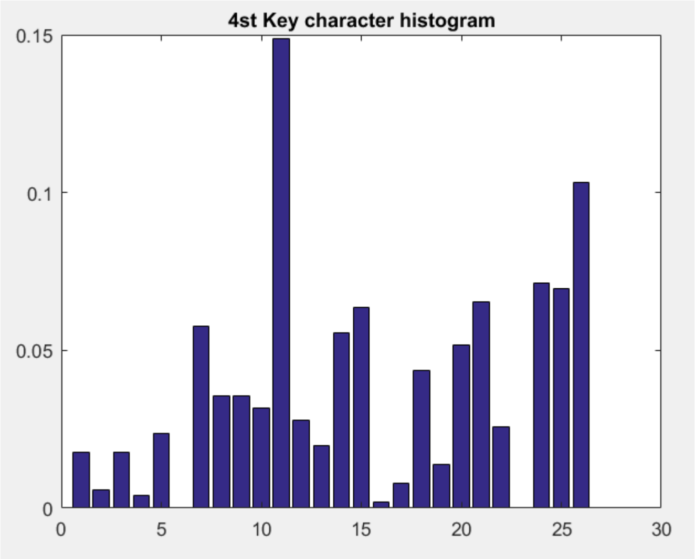
1st Key character histogram

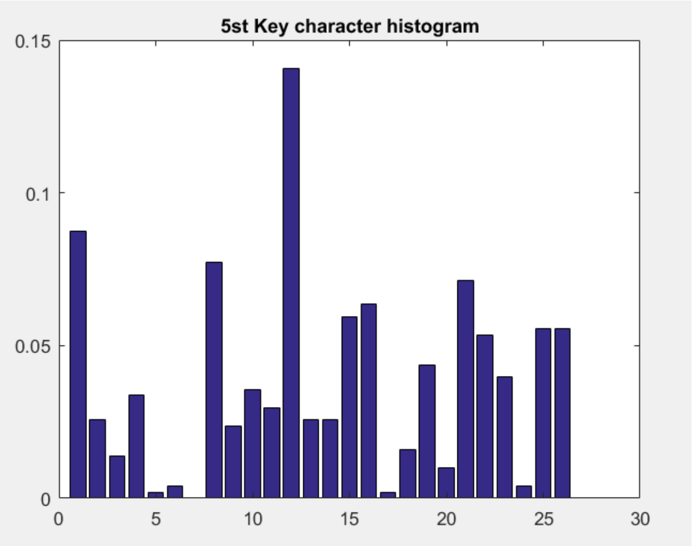


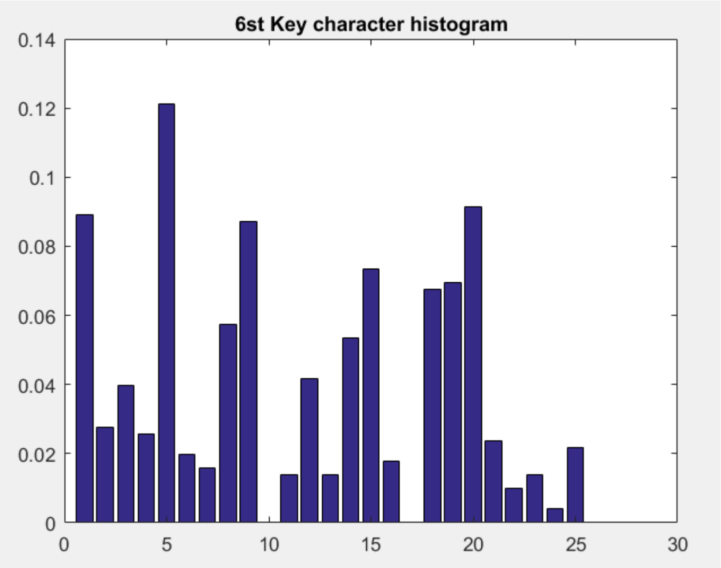
2st Key character histogram

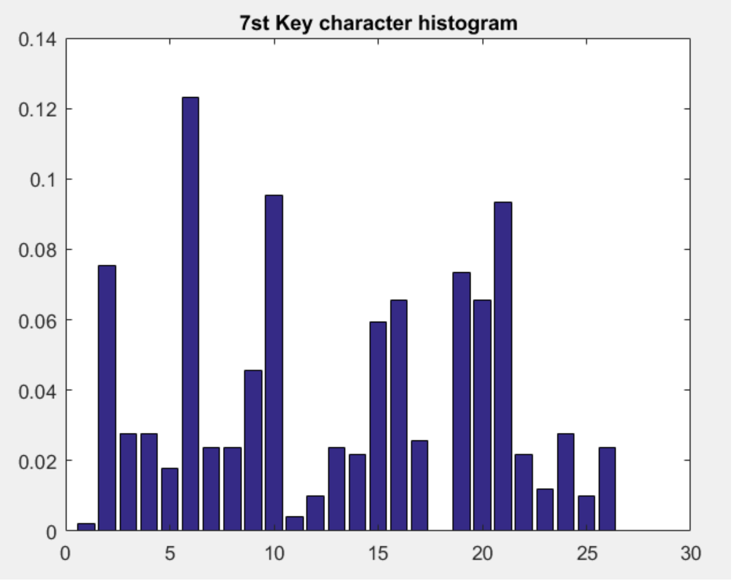


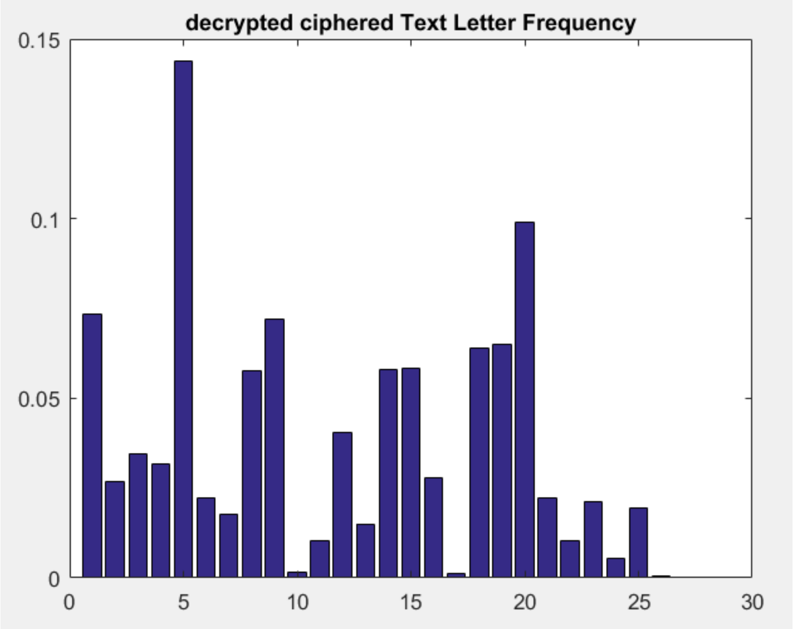
3st Key character histogram


4st Key character histogram


5st Key character histogram


6st Key character histogram


7st Key character histogram


decrypted ciphered Text Letter Frequency