

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 bjuvutk fpmvutkl taete zewwu atk utwk a sltbd jivoes vpsi ao toptio bfldeku cjhoex hlqzhbkas. bdiexai"t kfszlm pfsy ydiuueoj 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 ziyuzlmobs, jf oiy dosc worpgsswhoh, ionlnzld uzl tgiuums yeiaa, b uyizpcbd joswoowut um tiw cimlnèsw jivoes. loe ziyuzlmobs dawhky, hpolvky, oodf pxvvjvld g wrpyyeyziww, yimpd, bfk pxldjuaahse tqztkf fpj zwoaciaug hltxwln ippiwy arwhbtltj. dhbl ps tww lfwut hs uzl voneoèjl cowhfj day vrjypngslz vlsiyicwk be nipnhn hhtuaztg iemdhshu pn iaz fomtfwu fomtz lorkl bpgg lg jigjh dks. sjy. niucau thtzpsus iersatg. oe hbiml bpau tiw aahblb jlczh og lyizoenabs, hbt bvkej h rfhlaizpnh "uvutaeskpqt" (hkfq) ao ydiuuo cowhfj hlvoacwas kcesq sezaes. ooexlat ssbkytj sud ziyuzlmobs vkld g miywk pgtfju ol zuckaizbtjgus, hlmszo"y zciwte slaol ahk wauillrt vf tmszptvlpotz cpmsd hl ebkple jhbfnej zinhsy hf sfdlczpnh s uec rez. clyy desw ayvpcbdshy ypnhdl wuydt gy snvru horgzet, cuocu tp tvtn waslpey pn bvcattje, pj argusnaatk "ovl vf hhne" ssotn wjlo tnl mfkzaml. bfdsayv"s nwahuk timz rkxujld yarpfn skjusaay lvr pfsy zoe lwf. ay pt jk yerhtjnle latq ao ylcvj a yoosl ree whssze, yhy cq h pxlvjgbs vyiwssae 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 vduexhbmw ao iyyqlhngsyta. vkynbe"z wuyk, igdeblr, fnlnzbamdf lkk tp loe uue-uate vhd, b loeuyeuajarsy vfirkhktse ippiwy. it h cbwzax

jiqzlr, khci dltzlr px ahk hlqzhhbka 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 vpflrffa ruds, fsjh gspisiez zhjxaej jyddpcgslz lv tnl lfxa cutpbjld zv tiw wrkcpimz arwhbtl, 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 jwvy. ahf sspnhbfl bskk au whcn wojfa dkweovz ot h rfhlaazpnh clycvre. whcn yox kaaxas xaah g rez dltzlr. uzl rktajfkex vf uzl rud hpdks zoe mwatlys b lv z (ou siamtkk osvrl). gstigbgn ahfjl axl txwute ziy cly xvwk koocu, ypm dirs oodf uyl at ehne rezk (kilmeswut gspisiezz) at loexl asw bnoxuf dltzlrt au tnl kfz ztxpnh, zlrk qutl mibl kfz. dkjrzhaiuu it hlrlvrnw be nojfn tu ahf jwv ou tiw aahse dgyrkzppfktn tp loe qly, gaudoug uzl puziuavn um tiw jivoesllxz seullr ou tiaz rud, aov ahku utaug zoe dgsusu"s msier hs uzl priollxz. mos weaswlf, au rud l (gjvm rlmpf), ahk jiqzlrzlxu d hplask 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 quoxldml og loe vsajfaeda, os mze um a swjomuiasilk dosv hs g rez. chsozkj"k tezoze zhd tv svuo dkweovlnipet. looanh lsziyri xsz tnl fjzt zv pvtiyo ao sjcubnu gm tnl aulhcq, pt jk jlkhr uzht zoesw dext ouzlyr dhp olrk hwbjl ol pt. jf limotfwu fomtz xvux, jhbjsey iacthgk dat yvajld jfao hyebcpnm ahf npgkuèrk uppnlr xzln pvho zhlr irpur tndajls ybbnaatkk a "owd" cowhfj ao zoe kgbtrhl px ahk zodalte vf uzl axas. xzln hhbscne yooxwk tnht uzdaoet" uppnlr xsz eyzeolparsy kmzt guouzlr xlcswhtovn px ahk cihwuèrk jiqzlr, zowbaaey jhbdsetnee thbhghf lv bxlal zps ippiwy etjoewk tcpcf, optn rezk vf jpfgyweta lfftn. iacthgk zudulejld jf keiyyqlpnm h sbewlk, dhjuo taynfv vuz ao cw ahk wofe "ahk citavn um sjf", iy gsfswk tkunzkn, kucsqwtkk aduvrjpnh lv tnl kfqdoxk "enasy", zoe gaysz uanw vf zlnozot"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 khmq 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 worfamhoahlrtju jivoes ohs lvrnmsazld cq seuu bblaiyaa bdiexai bjvutk fpmtytkln taete zewwu atk  
utwk a sltbd jivoes vpsi ao toptio bfldeku cjhoez hlqzhbkas. bdiexai"t kfszlm pfsy ydiuuej hlqzhbkas bxaex zewwyar dosvz, atk sxaacnls xwye oudjuhtkk bz oyizpnh  
loe rltuwy ol ahf uvrxlsqgdoud bdwhgieu au tnl cjhoeaeyl. sazlr, jf milaeff outkrfv hnj lihza, juoaofls zyiuzlmobs, jf oiy dosc worpgsswhoh, ionlnzld uzl tgiums  
yeiaa, b uyizpcbd joswooutw um tiw cimlnësw jivoes. loe zyiuzlmobs dawhky, hpolvky, oodf pxvrvjld g wrpyeyziww, yimpd, bfk pxldjuaahse tqztk fpj zwoaciaug  
hltxwln ippiwy arwhbtlty. dhlbl ps tvw lfvtw hs uzl voneoëjl cowhfj day vrjypngslz vlsiyicwk be nipnln hhtuaztg iemdhsh pn iaz fomtfwu fomtz lorkl bpgr lg jigjh dks.  
sjy. niucao thtzipus iersatg. oe hbiml bpui tiw aahblb jlczh og lyizoenabs, hbt bykej h rfhlapznh "uvutaeskpqt" (hkfq) ao ydiuuo cowhfj hlvoacwas kcesq sezaes.  
ooexlat ssbkytj sud zyiuzlmobs vkld g miywk pgtfju ol zuckaizbtjgus, hlmszo"y zciwte slaol ahk waullrt vf tmsizptvlpotz cpmsd hl ebkple jhbfnej zinhsy hf sfdleczpnh  
s uec rez. clyy desw ayvpcbdys ypnhdl wuydt gy snvru horgzet, cuocu tp tvtn waslpey pn bvcatje, pj argusnaatkk "ovl vf hhne" ssotn wjlo tnl mfkzaml. bñdsayv"s  
nwahuk timz rkujiild yarpfm skjusaay lvr pfsy zoe lwf. ay pt jk yerhtjnle latq ao ylevjl a yoosl ree whssze, yhy cq h pxlvjgbs vyiwae ivnw wysgaipf, iersatg"z seztfe  
day jookpdkyacd f muye twjuxl. gjdiexa vfjuas arjwk tu yeqspr zoe cjkku cjhoez (jrfsaitn tiw cexuan-npgkuërf uppnlr jf uitltfw eonhuwln), hbt, og tazaes ooaz oe eak,  
tnl cjhoez dat kairs vduexhbmw ao iyyqlhngsyta. vkyne"z wuyk, igdebl, fnlnzbamdf lkk tp loe uue-uate vhd, b loeuyeuajarsy vfirkhktse ippiwy. it h cbwzax jiqzlr,  
kheci 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 cvumy ieiwmf t  
hnj zo pf. ahk cihwuërk jiqzlr ivntazty vf twcexhl dslsgy cjhoez io klqalndw dzo dmxmexlnu koila vdbey.ao ffjrewt, b lhlrl og sspnhbflz cgu bf mzej. aeseld g aacmsa  
xlcus, cimlnësw zqahr, gy voneoëjl tgilf. aa cuusjkas um tiw hlvoacwa wxptuwu oaa txwute ziy lpmkz io vpfllrffa ruds, fsjh gspisiez zhjxaej jyddpcgslz lv tnl lfxa  
cutpbjld zv tiw wrkicpmz arwhbtl, ivrszwpudjfn tu ahf ldetay tae puzsjtse ihetsy cowhfjz. az kigxlrtkut qgpnz io loe kucsqtovn qjvckzs, uzl cowhfj bskz a  
eamfkyeol hlvoacwa fxvm pfl ol ahf jvw. ahf sspnhbfl bskk au when wofja dkweovz ot h rfhlapznh clycvre. when yox kaaxas xaah g rez dltzlr. uzl rktajfkex vf uzl rud  
hpdks zoe mwatkys b lv z (ou siamtck osvrl). gstigbgn ahfjl axl txwute ziy cly xvwt koocu, ypm dirs oodf uyl at ehne rezk (kilmeswut gspisiez) at loexl asw bnouf  
dltzlr at tnl kfq ztxpnh, zlrk qutl mibl kfz. dkjrzhaiuu it hlrlvmwk be nojfn tu ahf jvw ou tiw aahse dgyrkzppfkittn tp loe qly, gaudoug uzl puziavm um tiw jivoesllxz  
seullr ou tiaz rud, aov ahku utaug zoe dgsusu"s msier hs uzl phriollxz. mos weaswlf, au rud l (gjm rlmfp), ahk jiqzlrzlxu d hpvlask pn ivlveu a, coizd 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  
zorfwr mroldsajh qhsjkri chs uzl foysu lv pailjko a ybcdwzslb hwuexhl blaair oo loe bpgffeye ippiwy. egyljwy azaadcz rksifv vn quoxddml and loe vsajfaeda, os mze  
um a swjomuasiik dosv hs g rez. chsozjk"k tezoee zhd tv svuo dkweovlnipet. looanh lsziyri xsz tnl fjizt zv pvtisiyo ao sjcubnu gm tnl aulhcq, pt jk jlkhr uztz zoesw dext  
ouzlrj dhp ork hwbjl ol pt. jf limotfwu fomtz xvux, jhbsey iacthgk dat yvaid jfao hyebcpnm ahf npgkuërf uppnlr xzln pvho zhlr irpur tndajlls ybbnaatkk a "owd"  
cowhfj ao zoe kgbtrhl px ahk zodalte vf uzl axas. xzln hhbcsne yooxwk thnt uzdaoaet" uppnlr xsz eyzeolparsy kmzt guouzl xlcswhtovm px ahk cihwuërk jiqzlr,  
zowbaaej jhbdsetnee thbhgf lv bxlal zps ippiwy etjoewk tcepf, optn rezk vf jpfgwyaeta lffntn. iacthgk zudulejd jf keiyyqlpnm h sbewlk, dhjuo taynfv vuz ao cw ahk  
wofe "ahk citavn um sjf", iy gsfswk tkunzkn, kucsqwtkk aduvrjpn lv tnl kfqdoxk "enasy", zoe gaysz uanv 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 thnt iw oaj ieff bsoug uzl mkahpv hs khmrq hs.')
```

%Chang to lowercase If there is a probable Uppercase 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 Ciphred Text
```

```
Ciphred_Letter_Frequency = histc(txt_ciphred, alphabet)/size(txt_ciphred,2);
figure (2), bar(Ciphred_Letter_Frequency)
title('Ciphred 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_ciphred_without_symbols
% 2- we calculate the histogram (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_ciphred_without_symbols,2)
    key_char_1(j)=txt_ciphred_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_ciphred_without_symbols,2)
    key_char_2(j)=txt_ciphred_without_symbols(i);
    j=j+1;
end
key_char_2_hist = histc(key_char_2, alphabet)/size(key_char_2,2);
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_ciphred_without_symbols,2)
    key_char_3(j)=txt_ciphred_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_ciphred_without_symbols,2)
    key_char_4(j)=txt_ciphred_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_ciphared_without_symbols,2)
    key_char_5(j)=txt_ciphared_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_ciphared_without_symbols,2)
    key_char_6(j)=txt_ciphared_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_ciphared_without_symbols,2)
    key_char_7(j)=txt_ciphared_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_ciphared_without_symbols lengths
key_repeated=repmat(Key_Final,[1 floor((size(txt_ciphared_without_symbols,2)/7)+1)]);
key_repeated_modified=key_repeated(1:size(txt_ciphared_without_symbols,2));
key_repeated_modified

%Decrypted code as achived by
decrypted_text=char(mod((txt_ciphared_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-dpubmktutfv keyjrjhaiuu og s worfamhoahlju jivoes ohs lvrmsaszld cq seuu bblaiyaa bdiexai bjvutk fpmtykl n taete zewwu atk utwk a sltbd jivoes vpsi ao toptio bfldeku cjhoe x hqzhhbks. bdiexai"t kfszlm pfsy ydiuuoeh hlqzhbks bxaex zewwyar dosvz, atk sxaacnls xwy e oudjuhtkk bz oyizpnh loe rltuwy ol ahf uvrxlsqgdoug bdwhgieu au tnl cjhoe xae y l. sazlr, jf milaeff outkrfv hn j liha, juoaofls ziyuzlmobs, jf oiy dosc worpgsswhoh, ionlnzld uzl tgiuys yeiaa, b uyizpcbd joswoowut um tiw cimlnšw jivoes. loe ziyuzlmobs dawhky, hpolvky, oodf pxvvyjld g wrpyyeyziww, yimpd, bfk pxdljuaa hse tzqtk fpj zwoaciaug hltxwln ippiwy arwbhtlty. dhl ps twv lfvwt hs uzl voneoèjl cowh fj day vrjypngslz vlsiycwk be nipn hn htuaztg iemdh su pn iaz fomtfwu fomt z lorkl bpg r lg jigjh dks. sij. niuca o tht zpsus iersatg. oe hbiml bp u tiw aahblb jlczh og lyizoenabs, hbt bvkej h rfhlapzh "uvutaeskpgt" (hkfk) ao ydiuuo cowh fj hlvoacwas kcesq sezaes. ooexlat ssbkytj sud ziyuzlmobs vkld g miywk pgtatfu ol zuckaizbtjgus, hlmszo"y zciwte slaol ahk waulrt vf tmsizptvlpotz cpmsd hl ebkple jhbfn ej zinh sy hf sfdlc zpnhs s uec rez. clyy desw ayvpcbdsy ypnhd l wuydt gy snvr horgzet, cuocu pt tvtn waslpey pn bvcatje, pj argusnaatk "ovl vf hhne" ssotn wjlo tnl mfkzaml. b fdsayv"s n wahu k timz rku xijld yarpf n skjusaay lvr pfsy zoe lwf. ay pt jk yerhtjn l le latq ao ylc vjl a yoos l ree whssze, yhy cq h pxlvjgbs vyiw sae ivnwwysgaipf, iersatg"z seztfe day jookpdkyacdf muye twjuxl. gidie xa v fjuas arjwk tu yeqspr zoe cjkvku cjhoe x (jrfasaitn tiw cexuan-npgkuèrf uppnlr jf uiltfwu eonhuwln), hbt, og tazeas oaz oe eak, tnl cjhoe x dat kairs vvdue xhbm w ao iyyqlhngsy taz. vky nbe"z wuyk, igdebr, fnlnzbamd f lkk tp loe uue-uate vhd, b loe uyeuajarsy vfrkhkbtse 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 hlcpe l d, h dovdk bkjonw l, y cvumv ieivmf t hn j zo pf. ahk cihwuèrk jiqzlr ivntazty vf twexhl dslsgy cjhoe x io klqalndw dzo d jmxmexl nu koila vdbbey. ao ffjrewt, b lhlrl og sspnhbflz cgu bf mzej, aeseld g aacmsa xlcus, cimlnšw zqahr f, gy voneoèjl tgi l. aa cuusjkas um tiw hlvoacwa wxptuwu oaa txwute ziy lpmkz io vpfllrffa ruds, fsjh gspisiez zhjxae jyddpcgsz lv tnl lfxa cutpbjld zv tiw wrkcipmz arwbhtl, ivrszwpudjfn tu ahf ldetay tae puzsjtse ihetsy cowh fjz. az kigxlkut qgpnz io loe kucsqwtov n qjvckzs, uzl cowh fj bskz a eamfkyeol hlvoacwa fxvm pfl ol ahf jvw y. ahf sspnhbfl bskk au when wojfa dkweovz ot h rfhlapzh clycvre. when yox kaaxas xaah g rez dltzlr. uzl rktajfex vf uzl rud hpdks zoe mwatks b lv z (ou siamtk osv l r). gstighgn ahf j axl txwute ziy cly xvwt koo cu, ypm dirs oodf uyl at ehne rezk (kilmeswut gspisiezz) at loe x l asw bnouxf dltzlr au tnl kf q ztxpnh, zlrk qutl mibl kf qz. dkjrzhaiu it hlrlvrnw k be nojfn tu ahf jvw ou tiw aahse dgyrkzppfktn tp loe qly, gaudoug uzl puziav n um tiw jivoes llxz seullr ou tiaz rud, aov ahku utaug zoe dgsusu"s msier h uz l prhiolxz. mos weaswif, ao rud l (gijv rlmfp), ahk jiqzlrzlxu d hpvlask pn i vlveu a, coizd ps zoe gaysz wlbautket mwatky. nfpa wk no ug yoc l (fsqt lkto o), dvcgae uzl cowh fjaeda x xzpen ps ggbnj pn dgsusu t, uzbs z ps uzl skjoov wlgpnuwet rltuwy. it lihzaeku sjpay zorfw mroldsajh qhsjkri chs uzl foy su lv pailjko a ybcdwzslbl hwue xhl blaair oo loe bpgf fye ippiwy. egyljwy azaadcz rksifv vn quoxldml og loe vsajfaeda, os mze um a swjomuiasilk dosv hs g rez. chsozjk" k tezo oe zhd tv svuo dkweovlnipet. looan h lsziry xsz tnl fj jzt zv pvtisyo ao sjcubnu gm tnl aulhq, pt jk jlkhr uzht zoesw dex l ouzlyr dhp olrk hwbjl ol pt. jf limotfwu fomt z vxux, jhbsey iacthgk dat vya jld fja o hyebcpnm ahf npgkuèrf uppnlr xzln pvho zhlr irpur tndajlls ybbnaatk a "owd" cowh fj ao zoe kgrthl px ahk zodalte vf uzl axas. xzln hhbcsne yooxwk thnt uzdaoaet" uppnlr xsz eyzeolparsy kmzt guozlr xlcswhtov n px ahk cihwuèrk jiqzlr, zowbaaey jhbds etnee thbhghf lv bxlal zps ippiwy etjoewk tcepf, optn rezk vf jpfgyweta l fntn. lacthgk zudulejld jf keiyyqlpnm h sbewlk, dhjuo taynfv vuz ao cw ahk wofe "ahk citav n sjf", iy gsfswk tkunzkn, kucsqwtwk aduvrjpn h lv tnl kf qdoxk "enasy", zoe gaysz uanw vf zlnozot"z wjxl. bgibbyl nces wephriowk tnl mflooj oe vkld. yaueals um bbtiaml"s ogaey yewwhl zoau z l hgk utwk tnl mflooj sawuy pailjkoe j iy lsziry, bfk sangfka thnt iv oaj ieff bsoug uzl mkahpv hs khrmq hs.

```
txt_ciphered_without_symbols =
```

loe lprtl ders-dpubmktutfv keyjrjhaiuu og s worfamhoahlju jivoes ohs lvrmsaszld cq seuu bblaiyaa bdiexai bjvutk fpmtykl n taete zewwu atk utwk a sltbd jivoes vpsi ao toptio bfldeku cjhoe x hqzhhbks bdiexaitf szlmpfsy ydiuuoeh hlqzhbks bxaex zewwyar dosvz atk sxaacnls xwy e oudjuhtkk bz oyizpnh loe rltuwy ol ahf uvrxlsqgdoug bdwhgieu autnlcjhoe xae y l sazlrj f milaeff outkrfv hn j liha juoaofls ziyuzlmobs jf oiy dosc worpgsswhoh ionlnzld uzl tgiuys yeiaa bu yizpcbd joswoowut utmiw cimlnšw jivoes loe ziyuzlmobs dawhky hpolvky oodf pxvvyjld g wrpyyeyziww yimpd bfk pxdljuaa hse tzqtk fpj zwoaciaug hltxwln ippiwy arwbhtlty dhl ps twv lfvwt hs uzl voneoèjl cowh fj day vrjypngslz vlsiycwk be nipn hn htuaztg iemdh su pn iaz fomtfwu fomt z lorkl bpg r lg jigjh dks sij niuca o tht zpsus iersatg oe hbiml bp u tiw aahblb jlczh og lyizoenabs hbt bvkej h rfhlapzh "uvutaeskpgt" (hkfk) ao ydiuuo cowh fj hlvoacwas kcesq sezaes ooexlat ssbkytj sud ziyuzlmobs vkld g miywk pgtatfu ol zuckaizbtjgus hlmszo"y zciwte slaol ahk waulrt vf tmsizptvlpotz cpmsd hl ebkple jhbfn ej zinh sy hf sfdlc zpnhs s uec rez clyy desw ayvpcbdsy ypnhd l wuydt gy snvr horgzet cuocu pt tvtn waslpey pnbvcatje pj argusnaatk kovl fhhnesotn wjlotn mfkzaml b fdsayv snwahu k timz rku xijld yarpf n skjusaay lvr pfsy zoe lwf ay pt jk yerhtjn l le latq ao ylc vjl a yoos l ree whssze yhy cq h pxlvjgbs vyiw sae ivnwwysgaipf iersatg"z seztfe day jookpdkyacdf muye twjuxl gidie xa v fjuas arjwk tu yeqspr zoe cjkvku cjhoe x (jrfasaitn tiw cexuan-npgkuèrf uppnlr jf uiltfwu eonhuwln hbt og tazeas oaz oe eak tnl cjhoe x dat kairs vvdue xhbm wao iyyqlhngsy taz vky nbe z wuyk igdebr fnlnzbamd f lkk tp loe uue-uate vhd b loe uyeuajarsy vfrkhkbtse 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 hlcpe l d h dovdk bkjonw l y cvumv ieivmf t hn j zo pf ahk cihwuèrk jiqzlr ivntazty vf twexhl dslsgy cjhoe x io klqalndw dzo d jmxmexl nu koila vdbbey ao ffjrewt b lhlrl og sspnhbflz cgu bf mzej aeseld g aacmsa xlcus cimlnšw zqahr f gy voneoèjl tgi l aa cuusjkas um tiw hlvoacwa wxptuwu oaa txwute ziy lpmkz io vpfllrffa ruds fsjh gspisiez zhjxae jyddpcgsz lv tnl lfxa cutpbjld zv tiw wrkcipmz arwbhtl ivrszwpudjfn tu ahf ldetay tae puzsjtse ihetsy cowh fjz az kigxlkut qgpnz io loe kucsqwtov n qjvckzs uzl cowh fj bskz a eamfkyeol hlvoacwa fxvm pfl ol ahf jvw y ahf sspnhbfl bskk au when wojfa dkweovz ot h rfhlapzh clycvre when yox kaaxas xaah g rez dltzlr uzl rktajfex vf uzl rud hpdks zoe mwatks b lv z (ou siamtk osv l r) gstighgn ahf j axl txwute ziy cly xvwt koo cu ypm dirs oodf uyl at ehne rezk (kilmeswut gspisiezz) at loe x l asw bnouxf dltzlr au tnl kf q ztxpnh zlrk qutl mibl kf qz dkjrzhaiu it hlrlvrnw k be nojfn tu ahf jvw ou tiw aahse dgyrkzppfktn tp loe qly gaudoug uzl puziav n um tiw jivoes llxz seullr ou tiaz rud aov ahku utaug zoe dgsusu"s msier h uz l prhiolxz mos weaswif ao rud l (gijv rlmfp) ahk jiqzlrzlxu d hpvlask pn i vlveu a coizd ps zoe gaysz wlbautket mwatky nfpa wk no ug yoc l (fsqt lkto o) dvcgae uzl cowh fjaeda x xzpen ps ggbnj pn dgsusu t uzbs z ps uzl skjoov wlgpnuwet rltuwy it lihzaeku sjpay zorfw mroldsajh qhsjkri chs uzl foy su lv pailjko a ybcdwzslbl hwue xhl blaair oo loe bpgf fye ippiwy egyljwy azaadcz rksifv vn quoxldml og loe vsajfaeda os mze um a swjomuiasilk dosv hs g rez chsozjk" k tezo oe zhd tv svuo dkweovlnipet looan h lsziry xsz tnl fj jzt zv pvtisyo ao sjcubnu gm tnl aulhq pt jk jlkhr uzht zoesw dex l ouzlyr dhp olrk hwbjl ol pt jf limotfwu fomt z vxux jhbsey iacthgk dat vya jld fja o hyebcpnm ahf npgkuèrf uppnlr xzln pvho zhlr irpur tndajlls ybbnaatk a "owd" cowh fj ao zoe kgrthl px ahk zodalte vf uzl axas xzln hhbcsne yooxwk thnt uzdaoaet" uppnlr xsz eyzeolparsy kmzt guozlr xlcswhtov n px ahk cihwuèrk jiqzlr zowbaaey jhbds etnee thbhghf lv bxlal zps ippiwy etjoewk tcepf optn rezk vf jpfgyweta l fntn lacthgk zudulejld jf keiyyqlpnm h sbewlk dhjuo taynfv vuz ao cw ahk wofe "ahk citav n sjf" iy gsfswk tkunzkn kucsqwtwk aduvrjpn h lv tnl kf qdoxk "enasy" zoe gaysz uanw vf zlnozot"z wjxl bgibbyl nces wephriowk tnl mflooj oe vkld yaueals um bbtiaml"s ogaey yewwhl zoau z l hgk utwk tnl mflooj sawuy pailjkoe j iy lsziry bfk sangfka thnt iv oaj ieff bsoug uzl mkahpv hs khrmq hs

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. The system only switched alphabets after several words and switches were indicated by writing the letter of the corresponding alphabet in the cipher text later in fifteen hundred and eighty John Henry Playfair in his work on polygraphia invented the tabular recta a critical component of the Vigenere cipher. The trithemist cipher however only provided a progressive grid and predictable systems for writing between cipher alphabets what is now known as the Vigenere cipher was originally described by Giovan Battista Bellaso in his fifteen fifty three book *La cifra del siggio*. In Giovan Battista Bellaso's built upon the tabular recta of Playfair but added repeating countersigns to switch cipher alphabets every letter whereas Alberti and Trithemist 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 as by a previous private conversation. Bellaso's system was considerably more secure. Gilbert Vernam tried to repair the broken cipher by creating the Vernam Vigenere cipher in nineteen eighty eight but no matter what he did the cipher was still vulnerable to cryptanalysis. Vernam's work however eventually led to the one time pad that theoretically is unbreakable. Cipher in Caesar's cipher each letter of the alphabet is shifted along some number of places. For example in Caesar's cipher of shift three would become d would become g would become j and so on. The Vigenere cipher consists of several Caesar ciphers in sequence with different shifts. Vigenere's encryption table of alphabets can be used to read a tabular recta. Vigenere's square or Vigenere's table consists of the alphabet written out twenty six times in different rows. Each alphabet is 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 key word. Each row starts with a key letter. The remainder of the row holds the letters a-z in shifted order. Although there are twenty six key rows shown you will only use as many as key words. Different alphabets share a unique letter 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 cipher text letter in the row and then using the column label as the plaintext letter. For example in row f from the cipher text t appears in column m which is the first plaintext letter. Next we go to row c from the column c the cipher text x which is found in column t. Thus the second plaintext letter is t. The first three letters of the cipher text are t f r i e d r i c h k a s i s k i. This was the first to publish a successful general attack on the Vigenere 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 Vigenere cipher when John Hall Brockthwaites submitted a new cipher to the journal of the Society of Arts. When Babbage showed that his waite cipher was essentially just another recreation of the Vigenere cipher, the challenge to break Babbage's cipher encoded twice with keys of different lengths. Babbage succeeded in decrypting a sample which turned out to be the poem the vision of Sir Galahad by Alfred Tennyson encrypted according to the key word Emily. The first name of Tennyson's wife Babbage never explained the method. He used studies of Babbage's notes to reveal that he had used the method later published by Kasiski and suggested that he had been using the method as early as

txt_ciphred_without_symbols =

loelprtdersdpubmkutfvkeyjrhjhaiuogsworfamhoahljtjuivoesohslvrnmsazldcqseuubblaiyaabdiexaibjvutkfpmtyklntaetezewwuatkutwkasltbdjivoesvpsiaotoptiofbldkucjhoexhlqzhbkasbdiexaitkfszlmfpsydydiuoejhlqzhbkasbaexzewwyardosvzatkssaacnlsxwyeoudjuhtkbbzoyizpnhoerltuwylolahfuvrxlsgudougbdwhgieuauntlcjhoexaeylsazlrjfmilaeffoutkrfhnjlhazajuoaoflszyiuzlmobsjfoiydoscowpgrsswhohionlnzlduzltgiumsyieaabyizpcbdjoswoowutumiwcimlnswjivoesloezyiuzlmobsdawkhyhpolvkyyoodfpxvvjvldgwrpyyeyziwwyimpdbfkpxldjuaahsetqztktfjzwoaciaughltxwnlippiwyarwhbtltydhblpstvwlvfwthsuzlvoneojlcowhfdjdayvrjyppngslzslsiyicwkbenipnhhhhtuaztgiemdhstupniazfomtfwufomtzlorklbpgrlgjigjhdksjyniuaothtzipusiersatgoehbimlbpuutiwaahblbjlczhoglyizoenabshbtbvkejhrhflazpnhuvuatieskpgthkfqaoydiuocowhfhjlv oacwaskcesqsezaesooexlatssbkytsudzzyiuzlmobsvkldgmiiywkpgatfjuolzuckaizbtjgushllmszoyzciwteslaolahkwaullrtvftmiszptvlpotzcpmsdhlebkplejhbfnejzinhshyfsdclzpnhsuecrezclydeswayvpbcbsyypnhdwuydtgysnvruhorgzetcuocutptvtnwaslpeypnbvcatjepjargusnaatkkovlvfhnessotnwjlotnlmfkzamlbfdsayvsnwahuktimzrkxujldyarpfnskjusaaylvrfpsyzloefwayptjkyerhtjlnlletatqaoylcvjlayooslrcewhsszeyhyqchpxlvjgbsvyiwsaeivnwysgaipfiersatzseztfedayjookpdkyacdfmuyetwjuxljgdiexavfjuasarjwktuyeqsprzoecjvkkucjhoexjrfsaitntiwcexuannpgkurfupnlrjfuitltfwueonhuwlhnbtogetazaeosooazoeakncljhoexdatkairsvvduexbmwaoiyyqlhngsytazykynbezwykigdeblrfnlznzabmdflkktploeueueatevhdbleoueyuajarsyvfirkhktseippiwyithcbwzaxjiqzlrkhcidltzlrpxahklqzhbkaitkoilaessotnspelnatbfjvfvadwzfuyeystprliosjakzasupnlrpxz homtuzyekhwpmshlcpeldhdovdkbkjonwlycvumvievmfthnjzopfahkcihwurkjiqzlrivntaztyvftwcexhlslsgycjhoexzioklqalndwdizodjxmexlnukoilavdbdebayoffjrewtblhbrl ogsspnhbflzcgubfmzejaeseldgaacmsaxluscimlnswzqahrfgyvoneojltgilfaacuusjkasumtiwhlvoacwawxptuwuoaatxwuteziylpmkziopvflrrffarudsfjsjhgspisiezjhjxaejjyddpc gszlvtnllfxacutpbjldzvtiwrkcpmzarwhbtltrsvwpzpuudjntuahfldetaytaepuzsjtseihtsyacowhfhjzazkigxlrkutqgnzziolekucsqwtovnjvckzsuzlcowhfhjbskzaeamfkyeolhlv oacwafxvmpflolahfjvwyahfsspnhbflbskkauwhcnwojfadkweovzotrhrflazpnhclycvrwhcnxyokaaasxsaahgrezdltruzlrktajfkexvfuzlrudhpdkszoemwatkyblvzousiamtkk osvlrgstigbgnahfjlaxltxwuteziylyxvwtkooocypmdirsoodfuylatehnezezkilmeswtgspisiezatloexaswbnoxufdltrtautnlkfqtzpxnhzlrkqutlmiblkfqzdkjrzhaiuithlrvmw kbenojfntuahfjvwoutiwaahsedgyrkzppfkintploeqlygaudougzlpuziauvnumtiwjiwoesllxzseullroutiazrudaovahkuutaugzoedgsususmsierhsuzlprhiolxzmosweaswlfaurudlg jvmrlmpfahkjijqzlrzlxudhplvaskpnivlveuacoidzpszoegayszwbautketmwatkyfnfawknougyclofsgtlktoodvcgaeuzlcowhfhjaedaxxzpcnpsggbnjpdgsusutuzbszpsuzlskjoovw lgpnuwetrltuwytlihzakusjpayzorfwmroldsajhqhsjkrichsuzlfoysulvpailjkoaybcdwzslblhwuexhlblaaairooleobpgffyeippiwyegyljwyazaadczrksifvvnquoxdlmlogloevsajfa edaosmzmeumaswjomiaasilkdosvhsgrzechsozjkjtezooezhdtvsvuodkweovlnipetlooaanhsziyrixsztnlffjztzvpvtisyaoosjucubnugmtlnaulhccptqjklkhrzhtzoeswdexloulzrlydhpo lrkhwbjloltpljfilmotfwufomtzxvuxjhbjsyiaethgkdatyvajldjfaohyebcpnmahfngpkurfupnlrnxlnpvhzhzlrirpurtndajllsybbaatkaowdcowhfhjaozoeqgbrthlpxahkzodaltevfuz laxaszlnhbscsneyooxwktnthtuzdaoaetupnlrxszezolparsykmztguouzlrxlcswhtovnpxahkciihwurkjiqzlrzowbaeyjhdsetneethbhghflvbxlalzpsippiwyetjoeuwtkcpcfoptnr ezkvfjpfgwytalfntniacthgkzudulejldjfkciyqplnmhsbewlkdhjuotaynfvvuzaocwahkwofeahkcitavnumsjfjygsfswktkunzkvnkcusqwtkadvrjpnhlvtnlkfqdoxkenasyzoega yszuanwvfwlnoqzotzwxjlbgiibynlkesewephriowktnlmfloojoekvldyaualsumbbtiamsogaeyewwhlzoaulzhgkutwktnlmfloojsauwypailjkoeyjylsziyrbfksangfatnhtiwoaji effbsouguzlmkaphvhskhrmqhs

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.



