

**ciphertext**

```

opkjcpcsrqtkhespzxxsjmuinieiovvryaaqaecjn:
ystxnemmbyzrvvvjopwxzinqjibxzjdmjfsxniz:
vjidqdfzzymlyeieljidqdfzzaspwxcbnihesp:
zxxsjmuinbnijiehjzutsvrxdvmwmwkihaujhar:
vzvqqsgfqhwtroqvsabnijycrzzgfwpzxtxuxsr:
kmvtxmgorxopkxwqvsaxafzmt eoquroruxcmicp:
iirjbkwwwjyzqtavmtlopkzipeimihmzmkcvxvi:
ovvhnwllxkeiiqmxwwsewvzkmriexdnoirmwoiwc:
rhlzwdvlsfqrxdwtmgtiinmtxshfrgggwowlqhi:
xcqsdtgmzirikedyefirzvqreppvjmwsvxvijsp:
ziiwrumxizirmexcmkrrrffxzxiowvrjbkxveki:
qmtmtxyihmzlhcfjvbezqoyenvuxpivrpbopwdv:
hjzgrsbppjqzwqvztoqyrcxtymzkrhppadlkpme:
medtgfzifropkmbxvvimzedskiiboezzlpimxep:
mcmognegfviiqjibxzjdmjydhxrzazswxvqnivt:
seimioordvvzdawwwjyzaujqcsimvuxswrvzto:
whiumijuprrvadvl sfqrxdwtgcrkedvkhwrklzc:
vhoxvadtretdvemqtmhec mxqfirgfpjzkhhi oxr:
pkvsegtgqieppvxcmzeppvpdazwogmiicsfsvzr:
mmjavmtlxwxvswgsilyxcxyixwsqcrmygvkvofz:
pdboigeehzfvsgyiinkbizmjxvkuqdmceoqurcj:
jxvvjefhzdzlteaijjzbyzrvvvjopwxzinithe:
xyimqtjcvdeoqurgitymqzcsbgsncxig

```

Use the `coinc` function supplied with the book to compute  
Friedman's index of coincidence for several shifts of the ciphertext :

```

Do[Print[i, " ",
  coinc[ciphertext, i]], {i, 25}]

```

```

1 47
2 46
3 28
4 49

```

5 34  
 6 33  
 7 21  
 8 57  
 9 27  
 10 41  
 11 32  
 12 47  
 13 24  
 14 41  
 15 33  
 16 66  
 17 29  
 18 38  
 19 34  
 20 47  
 21 37  
 22 52  
 23 38  
 24 52  
 25 42

Shifts that are a multiple of 8 have higher indices so we guess that the key length is 8. Now look at a slice of the text, taking every 8th character :

**ct1 = choose[ciphertext, 8, 1]**

```

orznyjmvndzzizcznjdhzhaztvoaocjzomvngvdidd:
  nghgdvmpxczjqhvnpjjomddoiiioidznidzmzid:
  ddzdmxjrgcdimxixgdznavovzjvnmomn

```

Look at the frequencies of this slice. They should resemble normal English frequencies :

**frequency[ct1]**

```
{ {a, 2}, {b, 0}, {c, 4}, {d, 16},
  {e, 0}, {f, 0}, {g, 4}, {h, 4},
  {i, 10}, {j, 8}, {k, 0}, {l, 0},
  {m, 9}, {n, 10}, {o, 9}, {p, 2},
  {q, 2}, {r, 2}, {s, 0}, {t, 1}, {u, 0},
  {v, 9}, {w, 0}, {x, 4}, {y, 1}, {z, 15} }
```

The most common characters by far are d and z; if one of these is e, then the key is z or v. z is unlikely because if it were the key, then y would be very common in the plaintext, which is unlikely. So we guess the first letter of the key is v.

We can also use the dot products of the observed frequencies of the slice with shifts of the frequency vector for normal English :

**corr[vigvec[ciphertext, 8, 1]]**

```
{ 0.0352232, 0.0352589, 0.0344554, 0.0375268,
  0.0353304, 0.0376786, 0.0410893, 0.0367054,
  0.0433125, 0.0392589, 0.0449554, 0.037125,
  0.0383571, 0.0306071, 0.0349554, 0.0388482,
  0.0353929, 0.0413304, 0.0330893,
  0.0309375, 0.0373214, 0.0702054,
  0.0397768, 0.0283661, 0.0288929, 0.055 }
```

**Max[%]**

```
0.0702054
```

The biggest dot product occurs for a shift of 21, which again says the first letter of the key is v.

Define a function to do this automatically :

```
key[i_] :=
  Position[corr[vigvec[ciphertext, 8, i]],
    Max[corr[vigvec[ciphertext, 8, i]]] - 1
```

And use it to find the full key :

```
Do[Print[key[i]], {i, 8}]
```

```
{ {21} }
```

```
{ {8} }
```

```
{ {6} }
```

```
{ {4} }
```

```
{ {14} }
```

```
{ {4} }
```

```
{ {17} }
```

```
{ {4} }
```

The key is "vigenere" and the plaintext is :

```
In[104]:=  
vigenere[ciphertext, -{21, 8, 6, 4, 14, 4, 17, 4}]
```

```
Out[104]=  
thefollowingtableprovidesayearendssummaryofsoftwarevulnerabilitiesidentifiedbetweendec:  
embersixthanddecembertwelfththetableprovidesthevendoroperatingsystemsoftwarenameco:  
mmonnameofthevulnerabilitypotentialriskatthetimeofpublicationandthecybernotesissue:  
inwhichthevulnerabilityappearedsoftwareversionsareidentifiedifknownthisinformation:  
ispresentedonlyasasummarycompletedetailsareavailablefromthesourceindicatedintheend:  
notepleasenotethatevenifthemethodofattackhasnotbeenutilizedoranexploitscriptisnotc:  
urrentlywidelyavailableontheinternetapotentialvulnerabilityhasbeenidentifiedupdate:  
stoitemsappearinginpreviousissuesofcybernotesarelisteredboldnewinformationcontaine:  
dintheupdatewillappearinitalicizedcoloredtextwhereapplicablethetablelistsacvnumbe:  
rinredwhichcorrespondstothecommonvulnerabilitiesandexposurescvelistacomilationofs:  
tandardizednamesforvulnerabilitiesandotherinformationsecurityexposures
```