Example of breaking a substitution cipher

```
IFYPX SBSAY SLEXA BQYIF ZXFYQ GXZGF
IYPGF YEZGB PZXKF LBQBS FXITF ZZFIY
PQXSL WQZBP ZXKXI YEBZN IFYPX SBSAI
FMFIP ZXYIY SAFXM SYZWI YEZGX WAGZH
IXQFP PFPBS ZGFFC FINLY NVXIE LEXAB
QBPGX VVFXW AGZZX ZGBSR BMXTD FQZBC
FZIWZ GBPXW IAXYE YSLZG FFCFI NLYNV
XIELB PCFIN PFELX KQXSQ FISFL VBZGX
TDFQZ BCFZI WZGEX ABQBP ZGFPQ BFSQF
XMZGF DWPZB MBQYZ BXSXM QXSQE WPBXS
PVFGY CFIFY QGFLT NSYZW IYEIF YPXSB
SAKNH XBSZG FIFBP ZGYZM XIPWQ GSYZW
IYEIF YPXSB SAZXX QQWIQ XSPQB XWPSF
PPBPS XZSFQ FPPYI NZGFC FINIF YPXSV
FSFFL EXABQ YZYEE BPTFQ YWPFK XPZIF
YPXSB SABPS XZQXS PQBXW PYZYE EXXXX
```

(Most or all of the XXXX at the end is probably padding.)

Most frequent letters

F	54	11.34%	(three doubles)
X	48	10.08%	(one double)
Z	41	8.61%	(two doubles)
P	38	7.98%	(three doubles)
B	36	7.56%	
S	35	7.35%	
Y	35	7.35%	
I	33	6.93%	
Q	28	5.88%	(one double)
G	22	4.62%	
E	18	3.78%	(two doubles)
W	16	3.36%	
A	13	2.73%	
L	12	2.52%	
N	10	2.10%	
C	7	1.47%	
M	7	1.47%	
V	7	1.47%	(one double)
K	5	1.05%	
T	5	1.05%	
DHRJOU	6	1.26%	(freqs 321000)

Common digrams and trigrams

BP	10
BS	9
FI	10
FY	9
GF	9
IF	10
XS	13
YE	8
YP	8
ZG	14

BSA	5
CFI	5
FYP	6
IFY	7
PXS	6
QXS	5
SBS	5
XSB	5
YPX	6
ZGF	7

Case 1: Try `F` = `e`.

```
IeYPX SBSAY SLEXA BQYIe ZXeYQ GXZGe
IYPGe YEZGB PZXKe LBQBS eXITe ZZeIY
PQXSL WQZBP ZXKXI YEBZN IeYPX SBSAI
eMeIP ZXYIY SAeXM SYZWI YEZGX WAGZH
IXQeP PePBS ZGeeC eINLY NVXIE LEXAB
QBPGX VVeXW AGZZX ZGBSR BMXTD eQZBC
eZIWZ GBPXW IAXYE YSLZG eeCeI NLYNV
XIELB PCeIN PeELX KQXSQ eISeL VBZGX
TDeQZ BCeZI WZGEX ABQBP ZGePQ BeSQe
XMZGe DWPZB MBQYZ BXSXM QXSQE WPBXS
PVeGY CeIeY QGeLT NSYZW IYEIe YPXSB
SAKNH XBSZG eIeBP ZGYZM XIPWQ GSYZW
IYEIe YPXSB SAZXX QQWIQ XSPQB XWPSe
PPBPS XZSeQ ePPYI NZGeC eINIe YPXSV
eSeeL EXABQ YZYEE BPTeQ YWPeK XPZIe
YPXSB SABPS XZQXS PQBXW PYZYE EXXXX
```

Case 1.1: Try $\mathtt{X} = \mathtt{t}$.

```
IeYPt SBSAY SLEtA BQYIe ZteYQ GtZGe
IYPGe YEZGB PZtKe LBQBS etITe ZZeIY
PQtSL WQZBP ZtKtI YEBZN IeYPt SBSAI
eMeIP ZtYIY SAetM SYZWI YEZGt WAGZH
ItQeP PePBS ZGeeC eINLY NVtIE LEtAB
QBPGt VVetW AGZZt ZGBSR BMtTD eQZBC
eZIWZ GBPtW IAtYE YSLZG eeCeI NLYNV
tIELB PCeIN PeELt KQtSQ eISeL VBZGt
TDeQZ BCeZI WZGEt ABQBP ZGePQ BeSQe
tMZGe DWPZB MBQYZ BtStM QtSQE WPBtS
PVeGY CeIeY QGeLT NSYZW IYEIe YPtSB
SAKNH tBSZG eIeBP ZGYZM tIPWQ GSYZW
IYEIe YPtSB SAZtt QQWIQ tSPQB tWPSe
PPBPS tZSeQ ePPYI NZGeC eINIe YPtSV
eSeeL EtABQ YZYEE BPTeQ YWPeK tPZIe
YPtSB SABPS tZQtS PQBtW PYZYE Etttt
```

There are only two occurrences of `t*e`, one as `tKe` and the other as `tQe`. It is unlikely there will be only one ‘the’ in this text so, if $\mathtt{F} = \mathtt{e}$, then probably $\mathtt{X} \neq \mathtt{t}$.

Case 1.2: Try Z = t.

```
IeYPX SBSAY SLEXA BQYIe tXeYQ GXtGe
IYPGe YEtGB PtXKe LBQBS eXITe tteIY
PQXSL WQtBP tXKXI YEBtN IeYPX SBSAI
eMeIP tXYIY SAeXM SYtWI YEtGX WAGtH
IXQeP PePBS tGeeC eINLY NVXIE LEXAB
QBPGX VVeXW AGttX tGBSR BMXTD eQtBC
etIWt GBPXW IAXYE YSLtG eeCeI NLYNV
XIELB PCeIN PeELX KQXSQ eISeL VBtGX
TDeQt BCetI WtGEX ABQBP tGePQ BeSQe
XMtGe DWPtB MBQYt BXSXM QXSQE WPBXS
PVeGY CeIeY QGeLT NSYtW IYEIe YPXSB
SAKNH XBStG eIeBP tGYtM XIPWQ GSYtW
IYEIe YPXSB SAtXX QQWIQ XSPQB XWPSe
PPBPS XtSeQ ePPYI NtGeC eINIe YPXSV
eSeeL EXABQ YtYEE BPTeQ YWPeK XPtIe
YPXSB SABPS XtQXS PQBXW PYtYE EXXXX
```

There are lots (7) occurrences of tGe.

Try $\mathtt{G} = \mathtt{h}$.

```
IeYPX SBSAY SLEXA BQYIe tXeYQ hXthe
IYPhe YEthB PtXKe LBQBS eXITe tteIY
PQXSL WQtBP tXKXI YEBtN IeYPX SBSAI
eMeIP tXYIY SAeXM SYtWI YEthX WAhtH
IXQeP PePBS theeC eINLY NVXIE LEXAB
QBPhX VVeXW AhttX thBSR BMXTD eQtBC
etIWt hBPXW IAXYE YSLth eeCeI NLYNV
XIELB PCeIN PeELX KQXSQ eISeL VBthX
TDeQt BCetI WthEX ABQBP thePQ BeSQe
XMthe DWPtB MBQYt BXSXM QXSQE WPBXS
PVehY CeIeY QheLT NSYtW IYEIe YPXSB
SAKNH XBSth eIeBP thYtM XIPWQ hSYtW
IYEIe YPXSB SAtXX QQWIQ XSPQB XWPSe
PPBPS XtSeQ ePPYI NtheC eINIe YPXSV
eSeeL EXABQ YtYEE BPTeQ YWPeK XPtIe
YPXSB SABPS XtQXS PQBXW PYtYE EXXXX
```

The sequence **`httXth`** strongly suggests that `X` is a vowel (or `y`). Letter frequencies suggest that $\mathtt{X} \in \{\mathtt{a}, \mathtt{i}, \mathtt{o}\}$. Since there is one `XX`, it is perhaps most likely that `X` is `o`.

Try $\mathtt{X} = \mathtt{o}$.

```
IeYPo SBSAY SLEoA BQYIe toeYQ hothe
IYPhe YEthB PtoKe LBQBS eoITe tteIY
PQoSL WQtBP toKoI YEBtN IeYPo SBSAI
eMeIP toYIY SAeoM SYtWI YEtho WAhtH
IoQeP PePBS theeC eINLY NVoIE LEoAB
QBPho VVeoW Ahtto thBSR BMoTD eQtBC
etIWt hBPoW IAoYE YSLth eeCeI NLYNV
oIELB PCeIN PeELo KQoSQ eISeL VBtho
TDeQt BCetI WthEo ABQBP thePQ BeSQe
oMthe DWPtB MBQYt BoSoM QoSQE WPBoS
PVehY CeIeY QheLT NSYtW IYEIe YPoSB
SAKNH oBSth eIeBP thYtM oIPWQ hSYtW
IYEIe YPoSB SAtoo QQWIQ oSPQB oWPSe
PPBPS otSeQ ePPYI NtheC eINIe YPoSV
eSeeL EoABQ YtYEE BPTeQ YWPeK oPtIe
YPoSB SABPS otQoS PQBoW PYtYE Eoooo
```

`oWAhtto` is a sequence. This looks a bit like '…ought to…', so try $\mathtt{W} = \mathtt{u}$ and $\mathtt{A} = \mathtt{g}$.

Substitute `W` = `u` and `A` = `g`.

```
IeYPo SBSgY SLEog BQYIe toeYQ hothe
IYPhe YEthB PtoKe LBQBS eoITe tteIY
PQoSL uQtBP toKoI YEBtN IeYPo SBSgI
eMeIP toYIY SgeoM SYtuI YEtho ughtH
IoQeP PePBS theeC eINLY NVoIE LEogB
QBPho VVeou ghtto thBSR BMoTD eQtBC
etIut hBPou IgoYE YSLth eeCeI NLYNV
oIELB PCeIN PeELo KQoSQ eISeL VBtho
TDeQt BCetI uthEo gBQBP thePQ BeSQe
oMthe DuPtB MBQYt BoSoM QoSQE uPBoS
PVehY CeIeY QheLT NSYtu IYEIe YPoSB
SgKNH oBSth eIeBP thYtM oIPuQ hSYtu
IYEIe YPoSB Sgtoo QQuIQ oSPQB ouPSe
PPBPS otSeQ ePPYI NtheC eINIe YPoSV
eSeeL EogBQ YtYEE BPTeQ YuPeK oPtIe
YPoSB SgBPS otQoS PQBou PYtYE Eoooo
```

`hoVVeoughtto` is a sequence. This looks like ‘how we ought to . . . ’, so try `V` = `w`.

```
IeYPo SBSgY SLEog BQYIe toeYQ hothe
IYPhe YEthB PtoKe LBQBS eoITe tteIY
PQoSL uQtBP toKoI YEBtN IeYPo SBSgI
eMeIP toYIY SgeoM SYtuI YEtho ughtH
IoQeP PePBS theeC eINLY NwoIE LEogB
QBPho wweou ghtto thBSR BMoTD eQtBC
etIut hBPou IgoYE YSLth eeCeI NLYNw
oIELB PCeIN PeELo KQoSQ eISeL wBtho
TDeQt BCetI uthEo gBQBP thePQ BeSQe
oMthe DuPtB MBQYt BoSoM QoSQE uPBoS
PwehY CeIeY QheLT NSYtu IYEIe YPoSB
SgKNH oBSth eIeBP thYtM oIPuQ hSYtu
IYEIe YPoSB Sgtoo QQuIQ oSPQB ouPSe
PPBPS otSeQ ePPYI NtheC eINIe YPoSw
eSeeL EogBQ YtYEE BPTeQ YuPeK oPtIe
YPoSB SgBPS otQoS PQBou PYtYE Eoooo
```

Letter frequencies suggest that both `P` and `B` are in $\{\mathtt{a}, \mathtt{i}, \mathtt{n}, \mathtt{r}, \mathtt{s}\}$. The sequence `ePPeP` strongly suggests that `P` is a consonant, and then from the sequence `thBPt` it is unlikely that `B` is also a consonant. The sequences `BouP` make it unlikely that `B` is `a`.

So try `B` = `i`.

```
IeYPo SiSgY SLEog iQYIe toeYQ hothe
IYPhe YEthi PtoKe LiQiS eoITe tteIY
PQoSL uQtiP toKoI YEitN IeYPo SiSgI
eMeIP toYIY SgeoM SYtuI YEtho ughtH
IoQeP PePiS theeC eINLY NwoIE LEogi
QiPho wweou ghtto thiSR iMoTD eQtiC
etIut hiPou IgoYE YSLth eeCeI NLYNw
oIELi PCeIN PeELo KQoSQ eISeL witho
TDeQt iCetI uthEo giQiP thePQ ieSQe
oMthe DuPti MiQYt ioSoM QoSQE uPioS
PwehY CeIeY QheLT NSYtu IYEIe YPoSi
SgKNH oiSth eIeiP thYtM oIPuQ hSYtu
IYEIe YPoSi Sgtoo QQuIQ oSPQi ouPSe
PPiPS otSeQ ePPYI NtheC eINIe YPoSw
eSeeL EogiQ YtYEE iPTeQ YuPeK oPtIe
YPoSi SgiPS otQoS PQiou PYtYE Eoooo
```

The five sequences `i*g` are all part of longer sequences `oSiSg` (followed by `Y`, `I`, `K`, `t` `i`). Since `S` is also common, and the one sequence `tio` is part of `tioS`, this makes it very likely that `S` = `n`.

Try `S` = `n`.

```
IeYPo ningY nLEog iQYIe toeYQ hothe
IYPhe YEthi PtoKe LiQin eoITe tteIY
PQonL uQtiP toKoI YEitN IeYPo ningI
eMeIP toYIY ngeoM nYtuI YEtho ughtH
IoQeP PePin theeC eINLY NwoIE LEogi
QiPho wweou ghtto thinR iMoTD eQtiC
etIut hiPou IgoYE YnLth eeCeI NLYNw
oIELi PCeIN PeELo KQonQ eIneL witho
TDeQt iCetI uthEo giQiP thePQ ienQe
oMthe DuPti MiQYt ionoM QonQE uPion
PwehY CeIeY QheLT NnYtu IYEIe YPoni
ngKNH ointh eIeiP thYtM oIPuQ hnYtu
IYEIe YPoni ngtoo QQuIQ onPQi ouPne
PPiPn otneQ ePPYI NtheC eINIe YPonw
eneeL EogiQ YtYEE iPTeQ YuPeK oPtIe
YPoni ngiPn otQon PQiou PYtYE Eoooo
```

The sequence `ogiQiPhowweoughtto` and the two sequences `QonPQiouP` suggest that `P` is `s` rather than `r`. (Even the sequence `iouP` gives that preference, though not as strongly, for `P`; there are words like ‘saviour’.)

Try P = s.

```
IeYso ningY nLEog iQYIe toeYQ hothe
IYshe YEthi stoKe LiQin eoITe tteIY
sQonL uQtis toKoI YEitN IeYso ningI
eMeIs toYIY ngeoM nYtuI YEtho ughtH
IoQes sesin theeC eINLY NwoIE LEogi
Qisho wweou ghtto thinR iMoTD eQtiC
etIut hisou IgoYE YnLth eeCeI NLYNw
oIELi sCeIN seELo KQonQ eIneL witho
TDeQt iCetI uthEo giQis thesQ ienQe
oMthe Dusti MiQYt ionoM QonQE usion
swehY CeIeY QheLT NnYtu IYEIe Ysoni
ngKNH ointh eIeis thYtM oIsuQ hnYtu
IYEIe Ysoni ngtoo QQuIQ onsQi ousne
ssisn otneQ essYI NtheC eINIe Ysonw
eneeL EogiQ YtYEE isTeQ YuseK ostIe
Ysoni ngisn otQon sQiou sYtYE Eoooo
```

The text (i ng)too QQuIQ onsQi ousne ssisn otneQ essYI N(the) suggests that Q = c, and that the whole phrase is ‘(ing) to occur consciousness is not necessary (the)’.

So try Q = c, Y = a, I = r and N = y.

```
reaso ninga nLEog icare toeac hothe
rashe aEthi stoKe Licin eorTe ttera
sconL uctis toKor aEity reaso ningr
eMers toara ngeoM natur aEtho ughtH
roces sesin theeC eryLa yworE LEogi
cisho wweou ghtto thinR iMoTD ectiC
etrut hisou rgoaE anLth eeCer yLayw
orELi sCery seELo Kconc erneL witho
TDect iCetr uthEo gicis thesc ience
oMthe Dusti Micat ionoM concE usion
sweha Cerea cheLT ynatu raEre asoni
ngKyH ointh ereis thatM orsuc hnatu
raEre asoni ngtoo ccurc onsci ousne
ssisn otnec essar ytheC eryre asonw
eneeL Eogic ataEE isTec auseK ostre
asoni ngisn otcon sciou sataE Eoooo
```

Now begin to finish off. The message seems to commence 'reasoning anL Eogic are to each other as heaEth is to KeLicine . . . ', suggesting that L = d, E = l and K = m, Note that EE occurs twice in the text.

Take L = d, E = l and K = m.

```
reaso ninga ndlog icare toeac hothe
rashe althi stome dicin eorTe ttera
scond uctis tomor ality reaso ningr
eMers toara ngeoM natur altho ughtH
roces sesin theeC eryda yworl dlogi
cisho wweou ghtto thinR iMoTD ectiC
etrut hisou rgoal andth eeCer ydayw
orldi sCery seldo mconc erned witho
TDect iCetr uthlo gicis thesc ience
oMthe Dusti Micat ionoM concl usion
sweha Cerea chedT ynatu ralre asoni
ngmyH ointh ereis thatM orsuc hnatu
ralre asoni ngtoo ccurc onsci ousne
ssisn otnec essar ytheC eryre asonw
eneed logic atall isTec ausem ostre
asoni ngisn otcon sciou satal loooo
```

Fill in the remaining blanks. This is now fairly easy.

Take `C` = `v`, `H` = `p`, `M` = `f`, `R` = `k`, `D` = `j` and `T` = `b`.

```
reaso ninga ndlog icare toeac hothe rashe
althi stome dicin eorbe ttera scond uctis
tomor ality reaso ningr efers toara ngeof
natur altho ughtp roces sesin theev eryda
yworl dlogi cisho wweou ghtto think ifobj
ectiv etrut hisou rgoal andth eever ydayw
orldi svery seldo mconc erned witho bject
ivetr uthlo gicis thesc ience ofthe justi
ficat ionof concl usion sweha verea chedb
ynatu ralre asoni ngmyp ointh ereis thatf
orsuc hnatu ralre asoni ngtoo ccurc onsci
ousne ssisn otnec essar ythev eryre asonw
eneed logic atall isbec ausem ostre asoni
ngisn otcon sciou satal loooo
```

Reasoning and logic are to each other as health is to medicine, or better, as conduct is to morality. Reasoning refers to a range of natural thought processes in the everyday world. Logic is how we ought to think if objective truth is our goal, and the everyday world is very seldom concerned with objective truth. Logic is the science of the justification of conclusions we have reached by natural reasoning. My point here is that for such natural reasoning to occur consciousness is not necessary. The very reason we need logic at all is because most reasoning is not conscious at all!