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 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%
Y 35	7.35%
S 35	7.35%
I 33	6.93%
Q 23	4.83% (one double)

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 $X = t$

```
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 $F = e$, then probably $X \neq t$.

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 $G = h$

```
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
```

Letter frequencies suggest that $X \in \{a, o\}$. Since there is one XX, it is perhaps more likely that X is o than a.

Try X=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
```

oW Ahtto is a sequence. This looks like

'...ought to...' so try $W = u$ 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
```

ho VVeou ghtto 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 $P \in \{a, i, s\}$. Since eP PeP is a sequence it is unlikely that $P \in \{a, i\}$.

Try $P = s$.

```
IeYso SBSgY SLEog BQYIe toeYQ hothe
IYshe YEthB stoKe LBQBS eoITe tteIY
sQoSL uQtBs toKoI YEBtN IeYso SBSgI
eMeIs toYIY SgeoM SYtuI YEtho ughtH
IoQes sesBS theeC eINLY NwoIE LEogB
QBsho wweou ghtto thBSR BMoTD eQtBC
etIut hBsou IgoYE YSLth eeCeI NLYNw
oIELB sCeIN seELo KQoSQ eISeL wBtho
TDeQt BCetI uthEo gBQBs thesQ BeSQe
oMthe DustB MBQYt BoSoM QoSQE usBoS
swehY CeIeY QheLT NSYtu IYEIe YsoSB
SgKNH oBSth eIeBs thYtM oIsuQ hSYtu
IYEIe YsoSB Sgtoo QQuIQ oSsQB ousSe
ssBsS otSeQ essYI NtheC eINIe YsoSw
eSeeL EogBQ YtYEE BsTeQ YuseK ostIe
YsoSB SgBsS otQoS sQBou sYtYE Eoooo
```

Letter frequencies suggest that $B \in \{a, i, r, n\}$. Since we have the sequence $thBsto$, $B \neq r, n$. Since we have the sequence $Bous$ we probably have $B \neq a$.

Try $B = i$

```
IeYso SiSgY SLEog iQYIe toeYQ hothe
IYshe YEthi stoKe LiQiS eoITe tteIY
sQoSL uQtis toKoI YEitN IeYso SiSgI
eMeIs toYIY SgeoM SYtuI YEtho ughtH
IoQes sesiS theeC eINLY NwoIE LEogi
Qisho wweou ghtto thiSR iMoTD eQtiC
etIut hisou IgoYE YSLth eeCeI NLYNw
oIELi sCeIN seELo KQoSQ eISeL witho
TDeQt iCetI uthEo giQis thesQ ieSQe
oMthe Dusti MiQYt ioSoM QoSQE usioS
swehY CeIeY QheLT NSYtu IYEIe YsoSi
SgKNH oiSth eIeis thYtM oIsuQ hSYtu
IYEIe YsoSi Sgtoo QQuIQ oSsQi ousSe
ssisS otSeQ essYI NtheC eINIe YsoSw
eSeeL EogiQ YtYEE isTeQ YuseK ostIe
YsoSi SgisS otQoS sQiou sYtYE Eoooo
```

Letter frequencies now suggest that $\{Y, S, I\} = \{a, r, n\}$. We have the sequence $isS\ otSeQ\ essY I\ N$ which looks like

'is not necessary' so try $S = n$, $Q = c$, $Y = a$, $I = r$, $Q = c$, $N = y$

```
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
```

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
```

Take $C = v$, $H = p$, $M = f$, $R = k$, $D = j$, $T = b$

```
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.