

Code Breaking 3

Chris Brew

Homework 1

RDEEI KEPQF QREPQ BFKQL EEPFL AIXEL MSADX EQFYX MSIFH
ERMQD BPEVF RDRDE NFAQB LKRDE CBITE QVDBR KMXMS HLMVM
YEIEA BLCEM PJBL L EPQDM VETEP JSCDX MSPAM MKJBL JBXQI
BTEXM SVFII KFEBQ XMSBP EIFTF LAMLB KSLAD EBNBL KXMSP
CDFIK PELRD EQBJE VEIIV DBRMY RDBRP ENIFE KRDEX MSLAE
PMYCM SPQEM SPVMP HFQPM SADBL KCMBP QEUSR MLRDE MRDEP
DBLKF RFQQS PEBLK VELEE KLMRU MVRMB LXMLE USRXM SFLXM
SPRMV LQBPE QSPPM SLKEK UXREJ NRBRF MLQRM KBXBI IJBXU
EPFAD RUSRR MJMPP MVRDE ETFIM LEJBX REJNR XMSPD SQUBL
KVFRD CBPKQ VFLEM PVMJE LBLKB IIVFI IAMRM PSFLK MLRQS
CDRDF LAQDB NNELM YRELE LMSAD

Frequency table

53 E

48 M

38 L

35 R

34 B

31 P

27 D

26 S

25 F

24 Q

Frequency table

53 E = E?

48 M = T?

38 L = A? O? I? N?

35 R = A? O? I? N?

34 B = A? O? I? N?

31 P = A? O? I? N?

27 D

26 S

25 F

24 Q

Homework 1

RDEEI KEPQF QREPQ BFKQL EEPFL AIXEL MSADX EQFYX MSIFH
.EE. .E.. ..E*. *...* EE.*. ...E* E.....
ERMQD BPEVF RDRDE NFAQB LKRDE CBITE QVDBR KMXMS HLMVM
YEIEA BLCEM PJBL L EPQDM VETEP JSCDX MSPAM MKJBL JBXQI
BTEXM SVFII KFEBQ XMSBP EIFTF LAMLB KSLAD EBNBL KXMSP
CDFIK PELRD EQBJE VEIIV DBRMY RDBRP ENIFE KRDEX MSLAE
PMYCM SPQEM SPVMP HFQPM SADBL KCMBP QEUSR MLRDE MRDEP
DBLKF RFQOS PEBLK VELEE KLMRU MVRMB LXMLE USRXM SFLXM
SPRMV LQBPE QSPPM SLKEK UXREJ NRBRF MLQRM KBXBI IJBXU
EPFAD RUSRR MJMPP MVRDE ETFIM LEJBX REJNR XMSPD SQUBL
KVFRD CBPKQ VFLEM PVMJE LBLKB IIVFI IAMRM PSFLK MLRQS
CDRDF LAQDB NNELM YRELE LMSAD

Frequent triples

- ◆ XMS, RDE, BLK
- ◆ Guess: XMS doesn't have the E in it
- ◆ So, what are these three likely to be?

Homework 1

RDEEI KEPQF QREPQ BFKQL EEPFL AIXEL MSADX EQFYX MSIFH
THEE. .E*.. ..E*.. A...N EE.*. ...E* OU... E...Y OU...
ERMQD BPEVF RDRDE NFAQB LKRDE CBITE QVDBR KMXMS HLMVM
E..... A.E... TETHEA NDTHE .D..E ..HAT DOYOU ..O.O
YEIEA BLCEM PJBLL EPQDM VETEP JSCDX MSPAM MKJBL JBXQI
.E.E. AN.E. ..ANN E..... .E.E.Y OU..O O..... ..Y..

Frequency table

53 E = E

48 M = O

38 L = N

35 R = T

34 B = A

31 P = I?

27 D = H

26 S = U

25 F

24 Q

Homework 1

RDEEI KEPQF QREPQ BFKQL EEPFL AIXEL MSADX EQFYX MSIFH
THEE. .EI.. ..EI. A...N EEI*EI OU... E...Y OU...
ERMQD BPEVF RDRDE NFAQB LKRDE CBITE QVDBR KMXMS HLMVM
E..... AIE.. TETHEA NDTHE .D..E ..HAT DOYOU ..O.O
YEIEA BLCEM PJBLL EPQDM VETEP JSCDX MSPAM MKJBL JBXQI
.E.E. AN.E. ..ANN E..... .E.E.Y OU..O O..... ..Y..

The case of P=1

- ◆ Doesn't look good. Too many vowels in sequence
- ◆ Would prefer a consonant
- ◆ ETAOIN SHRDLU - all possible

Homework 1

RDEEI KEPQF QREPQ BFKQL EEPFL AIXEL MSADX EQFYX MSIFH
THEE. .ER.. ..ER. A...N EER.N ...EN OU.NY E...Y OU...
ERMQD BPEVF RDRDE NFAQB LKRDE CBITE QVDBR KMXMS HLMVM
E...H ARE.. TETHEA NDTHE .A..E ..HAT DOYOU .NO.O
YEIEA BLCEM PJBLL EPQDM VETEP JSCDX MSPAM MKJBL JBXQI
.E.E. AN.EO R.ANN ER..O .E.ERY OUR.O O..AN .AY..

Homework 1

RDEEI KEPQF QREPQ BFKQL EEPFL AIXEL MSADX EQFYX MSIFH
THEE. .ER.. ..ER. A...N EER.N ...EN OU.NY E...Y OU...
ERMQD BPEVF RDRDE NFAQB LKRDE CBITE QVDBR KMXMS HLMVM
E...H ARE.. TETHEA NDTHE .A..E ..HAT DOYOU .NO.O
YEIEA BLCEM PJBLL EPQDM VETEP JSCDX MSPAM MKJBL JBXQI
.E.E. AN.EO R.ANN ER..O .E.ERY OUR.O O..AN .AY..

General monoalphabetic

HXVHX RZTVW KFXVU URMQW RVHRU QWHXV HAWXV JJFXY
AZVWU QWRBR ZFDZQ SXHRZ JRZQY UVNKV JVDMR YTVHH
VKXQW SXRZV WUXQN DRXVB QYAZU RKMVZ RUXQN CQNXR
NHYDR QWHXV HZRNJ RKHVN RVZWR NHVNX QNVDQ MQHOR
NCRZR NHZYW SXRZL YHXRZ HYYQW CXYNR LQWUW YHYWR

Frequències

- ◆ 106 R = E?
- ◆ 66 H = T? A? O? I? N? S?
- ◆ 65 V = T? A? O? I? N? S?
- ◆ 64 Q
- ◆ 56 W
- ◆ 55 Z
- ◆ 54 Y
- ◆ 53 X
- ◆ 44 N
- ◆

Sequences

- ◆ 11 HXR = Might be THE
- ◆ 8 XRZ = Might be TH?
- ◆ 8 VWU
- ◆ 7 XQN
- ◆ 5 TYZ
- ◆ 5 RUD
- ◆ 5 RMQ
- ◆ 5 MQW
- ◆ 4 ZRU
- ◆ 4 XVU
- ◆

the= HXR

HXVHX RZTVW KFXVU URMQW RVHRU QWHXV HAWXV JJFXY

th.th e.... ..h.. .e... e.te. ..th. t.... ...h.

AZVWU QWRBR ZFDZQ SXHRZ JRZQY UVNKV JVDMR YTVHH

..... ..e.ete. .e...e ...tt

VKXQW SXRZV WUXQN DRXVB QYAZU RKMVZ RUXQN CQNXR

NHYDR QWHXV HZRNJ RKHVN RVZWR NHVNX QNVDQ MQHQQR

NCRZR NHZYW SXRZL YHXRZ HYYQW CXYNR LQWUW YHYWR

the = HXR, spot V = a

HXVHX RZTVW KFXVU URMQW RVHRU QWHXV HAWXV JJFXY
thath e..a. ..ha. .e... e.te. ..tha t.... ...h.

AZVWU QWRBR ZFDZQ SXHRZ JRZQY UVNKV JVDMR YTVHH
..a.. ..e.ete. .e...a .a..e ..att

VKXQW SXRZV WUXQN DRXVB QYAZU RKMVZ RUXQN CQNXR
a.h.. .he.. ..h.. .eha. e..a. e.h.. ...he

NHYDR QWHXV HZRNJ RKHVN RVZWR NHVNX QNVDQ MQHQR
.t..e ..tha t.e.. e.ta. ea..e .ta.h ..a.. ..t.e

NCRZR NHZYW SXRZL YHXRZ HYYQW CXYNR LQWUW YHYWR
..e.e .t... .he.. .the. t.... .h..et..e

Sequences

- ◆ 11 HXR = THE
- ◆ 8 XRZ = THA
- ◆ 8 VWU = A.. ~ maybe AND
- ◆ 7 XQN = T..
- ◆ 5 TYZ = ..A
- ◆ 5 RUD = E..
- ◆ 5 RMQ = E..
- ◆ 5 MQW = ...
- ◆ 4 ZRU = .E.
- ◆ 4 XVU = H..
- ◆

the= HXR, VWU=and

HXVHX RZTVW KFXVU URMQW RVHRU QWHXV HAWXV JJFXY
thath e..an ..had de..n ente. .ntha t.n.a ...h.

AZVWU QWRBR ZFDZQ SXHRZ JRZQY UVNKV JVDMR YTVHH
..and .de.ete. .e...a .a..e ..att

VKXQW SXRZV WUXQN DRXVB QYAZU RKMVZ RUXQN CQNXR
a.h.n .he.a ndh.. .eha.d e..a. edh.. ...he

NHYDR QWHXV HZRNJ RKHVN RVZWR NHVNX QNVDQ MQHQR
.t..e ..tha t.e.. e.ta. ea..e .ta.h ..a.. ..t.e

NCRZR NHZYW SXRZL YHXRZ HYYQW CXYNR LQWUW YHYWR
..e.e .t..n .he.. .the. t...n .h..e ...dn .t.ne

Sequences

◆ 11 HXR = THE

◆ 8 XRZ = HE.

◆ 8 VWU = AND

◆ 7 XQN = T..

◆ 5 TYZ = ...

◆ 5 RUD = EN.

◆ 5 RMQ = E..

◆ 5 MQW = ..N

◆ 4 ZRU = .EN

◆ 4 XVU = HAD

106 R = E?

66 H = T

65 V = A

64 Q = O/I

56 W = N

55 Z = I/O

54 Y = ?

53 X = H

44 N = ?

the= HXK, VWU=and,

Q=o (not good)

HXVHX RZTVW KFXVU URMQW RVHRU QWHXV HAWXV JJFXY
thath e..an ..had de.on ente. ontha t.n.a ...h.

AZVWU QWRBR ZFDZQ SXHRZ JRZQY UVNKV JVDMR YTVHH
..and ode.eo ..te. .e.o.a .a..e ..att

VKXQW SXRZV WUXQN DRXVB QYAZU RKMVZ RUXQN CQNXR
a.hon .he.a ndho. .eha. o...d e..a. edho. .o.he

NHYDR QWHXV HZRNJ RKHVN RVZWR NHVNX QNVDQ MQHQR
.t..e o.tha t.e.. e.ta. ea..e .ta.h o.a.o .otoe

NCRZR NHZYW SXRZL YHXRZ HYYQW CXYNR LQWUW YHYWR
..e.e .t..n .he.. .the. t..on .h..e .o.dn .t.ne

the= HXK, VWU=and,

Q=i (better)

HXVHX RZTVW KFXVU URMQW RVHRU QWHXV HAWXV JJFXY
thath e..an ..had de.in ente. intha t.n.a ...h.

AZVWU QWRBR ZFDZQ SXHRZ JRZQY UVNKV JVDMR YTVHH
..and ide.ei ..te. .e.i.a .a..e ..att

VKXQW SXRZV WUXQN DRXVB QYAZU RKMVZ RUXQN CQNXR
a.hin .he.a ndhi. .eha. i...d e..a. edhi. .i.he

NHYDR QWHXV HZRNJ RKHVN RVZWR NHVNX QNVDQ MQHQR
.t..e i.tha t.e.. e.ta. ea..e .ta.h i.a.i .itie

NCRZR NHZYW SXRZL YHXRZ HYYQW CXYNR LQWUW YHYWR
..e.e .t..n .he.. .the. t..in .h..e .i.dn .t.ne

Is Z a vowel?

- ◆ Probably not, because of RZR
- ◆ If it is a consonant, may be r, s, d, l (t, h, n are taken)

Try r=Z?

HXVHX RZTVW KFXVU URMQW RVHRU QWHXV HAWXV JJFXY
thath er.an ..had de.in ente. intha t.n.a ...h.

AZVWU QWRBR ZFDZQ SXHRZ JRZQY UVNKV JVDNR YTVHH
..and ide.e r..ro ..te. .e.i.a .a..e ..att

VKXQW SXRZV WUXQN DRXVB QYAZU RKMVZ RUXQN CQNXR
a.hin .hera ndhi. .eha. i...d e..ar edhi. .i.he

NHYDR QWHXV HZRNJ RKHVN RVZWR NHVNX QNVDQ MQHQR
.t..e i.tha tre.. e.ta. ear.e .ta.h i.a.i .itie

NCRZR NHZYW SXRZL YHXRZ HYYQW CXYNR LQWUW YHYWR
..ere .tr.n .her. .the. t..in .h..e .i.dn .t.ne

Sequences

◆ 11 HXR = THE

◆ 8 XRZ = HE.

◆ 8 VWU = AND

◆ 7 XQN = TI.

◆ 5 TYZ = ..R

◆ 5 RUD = EN.

◆ 5 RMQ = E..

◆ 5 MQW = ..N

◆ 4 ZRU = REN

◆ 4 XVU = HAD

106 R = E

66 H = T

65 V = A

64 Q = I

56 W = N

55 Z = R

54 Y = O/S

53 X = H

44 N = S/O

Try Y=O, N=S

HXVHX RZTVW KFXVU URMQW RVHRU QWHXV HAWXV JJFXY
thath er.an ..had de.in ente. intha t.n.a ...ho

AZVWU QWRBR ZFDZQ SXHRZ JRZQY UVNKV JVDMR YTVHH
.rand ide.e r..ri ..te. .e.io .as.a .a..e o.att

VKXQW SXRZV WUXQN DRXVB QYAZU RKMVZ RUXQN CQNXR
a.hin .hera ndhis .eha. io..d e..ar edhis .ishe

NHYDR QWHXV HZRNJ RKHVN RVZWR NHVNX QNVDQ MQHQR
sto.e intha tres. e.ta. ear.e stash isa.i .itie

NCRZR NHZYW SXRZL YHXRZ HYYQW CXYNR LQWUW YHYWR
s.ere stron .her. other tooin .hose .indn otone

Start to see words

HXVHX RZTVW KFXVU URMQW RVHRU QWHXV HAWXV JJFXY
thath erfan cyhad delin eated intha tunha ppyho

AZVWU QWRBR ZFDZQ SXHRZ JRZQY UVNKV JVDMR YTVHH
urand ineve rybri ghter perio dasca pable ofatt

VKXQW SXRZV WUXQN DRXVB QYAZU RKMVZ RUXQN CQNXR
achin ghera ndhis behav iourd eclar edhis wishe

NHYDR QWHXV HZRNJ RKHVN RVZWR NHVNX QNVDQ MQHQR
stobe intha tresp ectas earne stash isabi litie

NCRZR NHZYW SXRZL YHXRZ HYYQW CXYNR LQWUW YHYWR
swere stron gherm other tooin whose mindn otone

And segment them out

HXVH XRZ TVWKF XVU URMQWRVHRU QW HXVH AWXVJJF XYAZ
that her fancy had delineated in that unhappy hour

VWU QW RBRZF DZQSXHRZ JRZQYU VN KVJVDMR YT VHHVKXQWS
and in every brighter period as capable of attaching

XRZ VWU XQN DRXVBQYAZ URKMOVZRU XQN CQNXRN HY DR
her and his behaviour declared his wishes to be

QW HXVH ZRNJRKH VN RVZWRNH VN XQN VDQMQRN CRZR
in that respect as earnest as his abilities were

NHZYWS XRZ LYHXRZ HYY QW CXYNR LQWU WYH YWR
strong. her mother too in whose mind not one

Remembering alphabets

- ◆ Random alphabets are hard to remember
- ◆ How to make memorable?

Keywords

- ◆ Let the keyword be BASKETBALL
- ◆ Generate an alphabet from that
- ◆ How?

Keywords

- ◆ Let the keyword be BASKETBALL
- ◆ Add the letters to the front of the alphabet, then add the rest
- ◆ BASKETLCFGHIJLMNOPQRUVWXYZ

Practice using keywords

- ◆ Let the keyword be JANE AUSTEN

Polyalphabetics

- ◆ How to efficiently use multiple alphabets