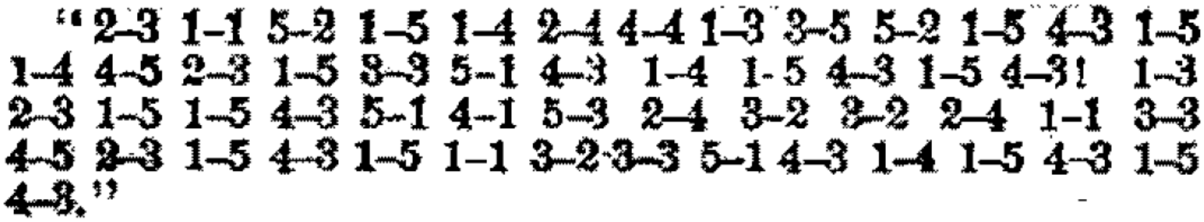


"2–3 1–1 5–2 1–5 1–4 2–4 4–4 1–3 3–5 5–2 1–5 4–3 1–5
1–4 4–5 2–3 1–5 3–3 5–1 4–3 1–4 1-5 4–3 1–5 4–3! 1–3
2–3 1–5 1–5 4–3 5–1 4-1 5–3 2–4 3–2 3–2 2–4 1–1 3–3
4–5 2–3 1–5 4–3 1–5 1–1 3–2 3–3 5–1 4–3 1–4 1–5 4–3 1–5
4–3."

`Have discovered the murderer! Cheer up William the real murderer.`

11. Can you think of a way to make the Polybius cipher more secure?

Answers will vary. One nice approach is to shuffle the digits that are obtained according to some rule, as an additional final step. Ideally, this shuffling (or transposition, as we'll call it later) would split apart pairs of numbers that represent single letters. This was the main idea behind a very good cipher the Germans used during World War I. However, there was a great French cryptanalysts willing to take on the challenge. See Chapter 6.

Chapter 2

1. Use a Caesar shift of 3 to encipher the following

```
I HAVE CROSSED THE RUBICON
```

```
L KDYH FURVVHG WKH UXELFRQ
```

2. The following ciphertext was obtained using a Caesar shift of 10. Shift back to recover the original message.

```
YXO NKI K MYYU SX DSTEKXK RKN DY ZBOZKBO CYWO WOKVC LED RO
GKC YED YP KVWYCD OFOBIDRSXQ KVV RO RKN GKC LBOKN MROOCO
KXN VODDEMO RO WKNO MBYDYXC CRBONNON DRO MROOCO KXN WSHON
LYDR GSDR DRO VODDEMO ZOYZVO VYFON SD DREC GKC LYBX DRO
MKOCKB CKVKN
```

```
ONE DAY A COOK IN TIJUANA HAD TO PREPARE SOME MEALS, BUT HE WAS
OUT OF ALMOST EVERYTHING. ALL HE HAD WAS BREAD CHEESE AND
LETTUCE. HE MADE CROTONS SHREDDED THE CHEESE AND MIXED BOTH WITH
THE  LETTUCE. PEOPLE LOVED IT. THUS WAS BORN THE CAESAR SALAD.
```

3. Decipher the message below that arose from a Caesar shift for some unknown value.

```
ZNA UNF ABG RIBYIRQ NA VAPU SEBZ GUR FYVZR GUNG FCNJARQ UVZ
```

```
MAN HAS NOT EVOLVED AN INCH FROM THE SLIME THAT SPAWNED HIM
```

4. As Stage 2 of his Cipher Challenge for $15,000, Simon Singh presented readers with a Caesar Shift Cipher. One of the students in a past cryptology class of mine came to me saying he couldn't get it. I laughed at first, since it is a simple matter of trying all 25 keys and proceeded to break it for him. I quickly saw why he got stuck and was then able to help him read the message. What could the catch be? See for yourself:

MHILY LZA ZBHL XBPZXBL MVYABUHL HWWPBZ JSHBKPBZ JHLJBZ
KPJABT HYJHUBT LZA ULBAYVU

FABER EST SUAE QUISQUE FORTUNAE – APPIUS CLAUDIUS CAECUS
DICTUM ARCANUM EST NEUTRON

Loosely translating this from Latin to English, we get:

Each man is the smith of his own fortune. The code word is neutron.

5. Use the keyphrase HIGHLANDER to encipher THERE CAN BE ONLY ONE.

TEAQA GHK IA MKFY MKA

6. The following was enciphered using the keyphrase BON JOVI. Recover the original message (it will give you Bon Jovi's way of defining isomorphic).

DSR BGG SCV RBHV LKGY SCV KBHVR CBUV NCBKAVJ

IT'S ALL THE SAME. ONLY THE NAMES HAVE CHANGED.

7. Use the keyphrase MARCUS AURELIUS to decipher

FJJD AMRD JVUO QLU KMPQ, WIQL IQP RLMHEIHE UGKIOUP QLMQ
OJPU MHC SUFF, MHC YJT RMH SJOUPUU QLU STQTPU, QJJ.

Look back over the past, with its changing empires that rose and fell, and you can foresee the future, too.

Since the Vikings also used encryption, exercises 8 through 11 give you some bits of Viking philosophy to decipher.[1]

8. Use the key HAMTHESMAL to decipher

JKJEK URGCV EQRBE JCLBR WBEJR BEJKP JQBHV EQNKF EJ.

None outlives the night when the Norns have spoken. (Hamthesmal 32)

[1] The plaintexts were found at http://evagirly.tripod.com/wright/id29.html.

9. Use the VIKINGR to decipher

```
BGWCS BVQBL PSEJC RGHTQ SSPYS PYVAV CJ.
```

He with a short knife must try, try again. (VFS, c.7)

10. Use the key JORVIK to decipher

```
SBIFL HAIPS BIUIH AIJHR ICQVP JWHLT SSBIG LPIQJ SCQKY CHACS
WCFFO I.
```

The longer the vengeance is drawn out, the more satisfying it will be. (LJS, c.13)

11. Use the key VOLSUNGA to decipher

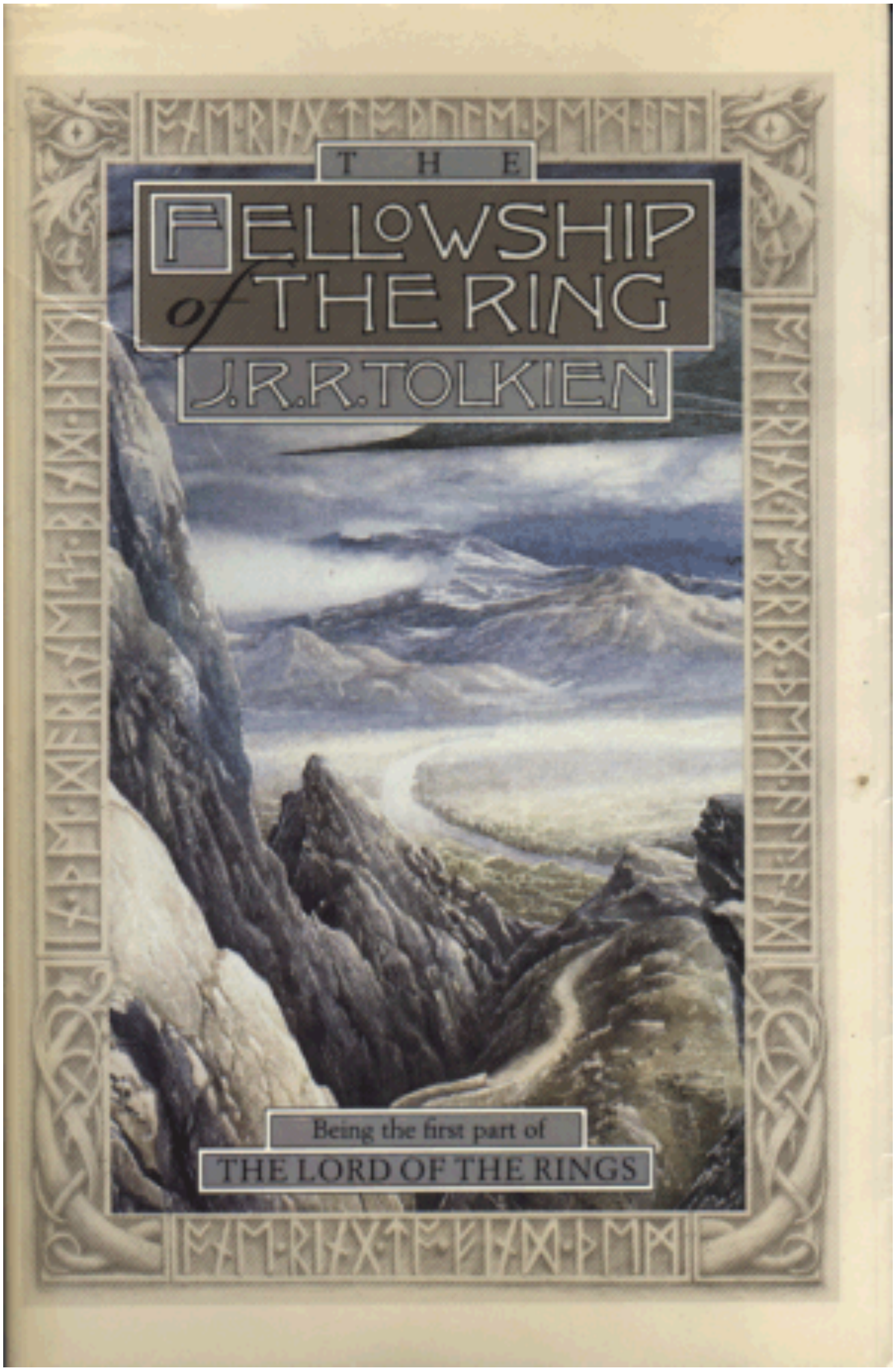
```
WAILV HPVYW AVQPI MMIWP UUFBH GEYLV MUNMU UNIED OUVMQ IQAUB
MEBNU PUHS.
```

Who can say what sorrow seemingly carefree folk bear to their life's end. (VS, c.24)

12. Use technology to compare the values of n! to those given by Stirling's approximation. How does the absolute error grow with n? How does the percentage error grow with n? This exercise should give you a better idea of what the ~ means in Stirling's formula.

The absolute error grows with n, but the percentage error converges to zero.

13. Decipher the text shown on the dust jacket of *The Fellowship of the Ring*.

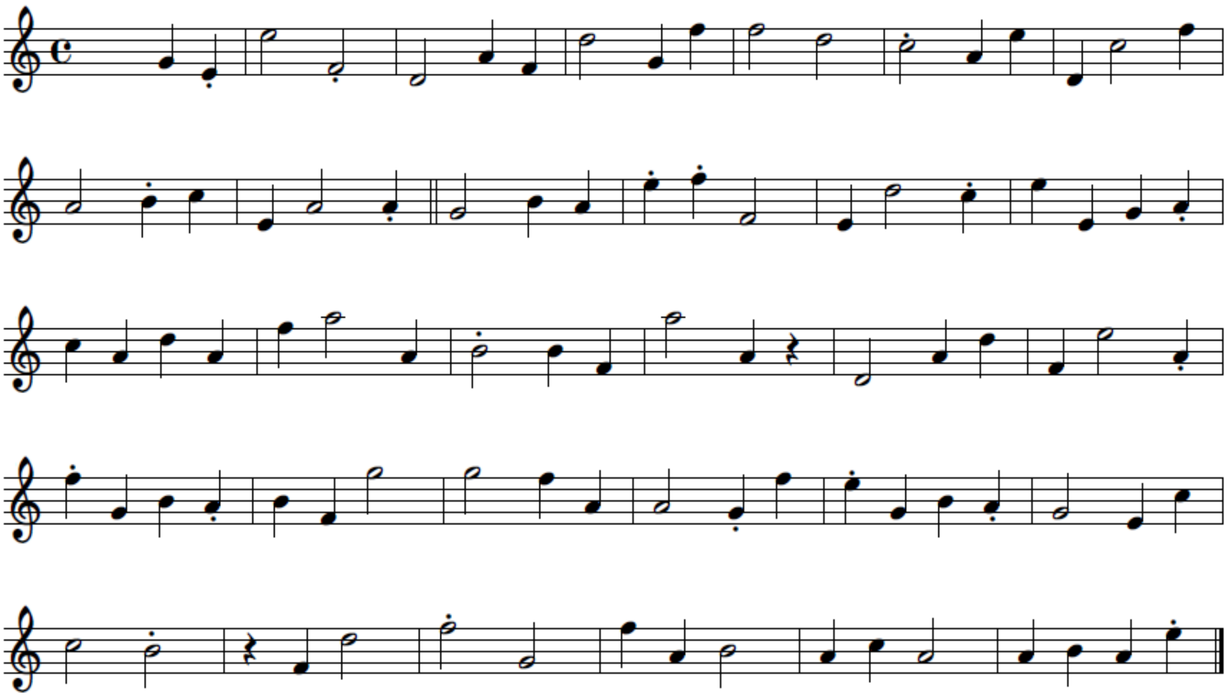


ONE RING TO RULE THEM ALL, ONE RING TO BRING THEM ALL, AND ONE RING TO FIND THEM, IN THE DARKNESS BIND THEM,

14. Decipher the secret message on the cover of Ozzy Osbourne's *Speak of the Devil* album. You will need to find an image of this album cover online first!

Howdy. Dial a Demon Productions in Conjunction with Graveyard Graphics, Proudly Present the Madman of Rock, Dumping in el Satano's Toiletio. Real Tasty

15. Decipher Mozart's cipher (retyped by Nicholas Lyman). Hint: the message was written at age 18 for a young English girl with whom he was in love. His father disapproved, hence the secret cipher. Expect a (mostly) English plaintext.



To my beautiful English Rose: when I your note received became I the happiest in the world - Auf Wiedersehen!

16. Can you decipher the message and its response placed in The Times "agony columns" in February, 1853?[2]

CENERENTOLA. N bnxm yt ywd nk dtz hfs wjfi
ymnx fsi fr rtxy fschtzx yt. Mjfw ymf esi, bmjs dtz
wjyzws fei mtb qtsldtz wjrfns, ncjwj. lt bwnyf f kjb
qnsjx jfuqnsl uqjfxy. N mfaj xnsbj dtz bjsy fbfd.

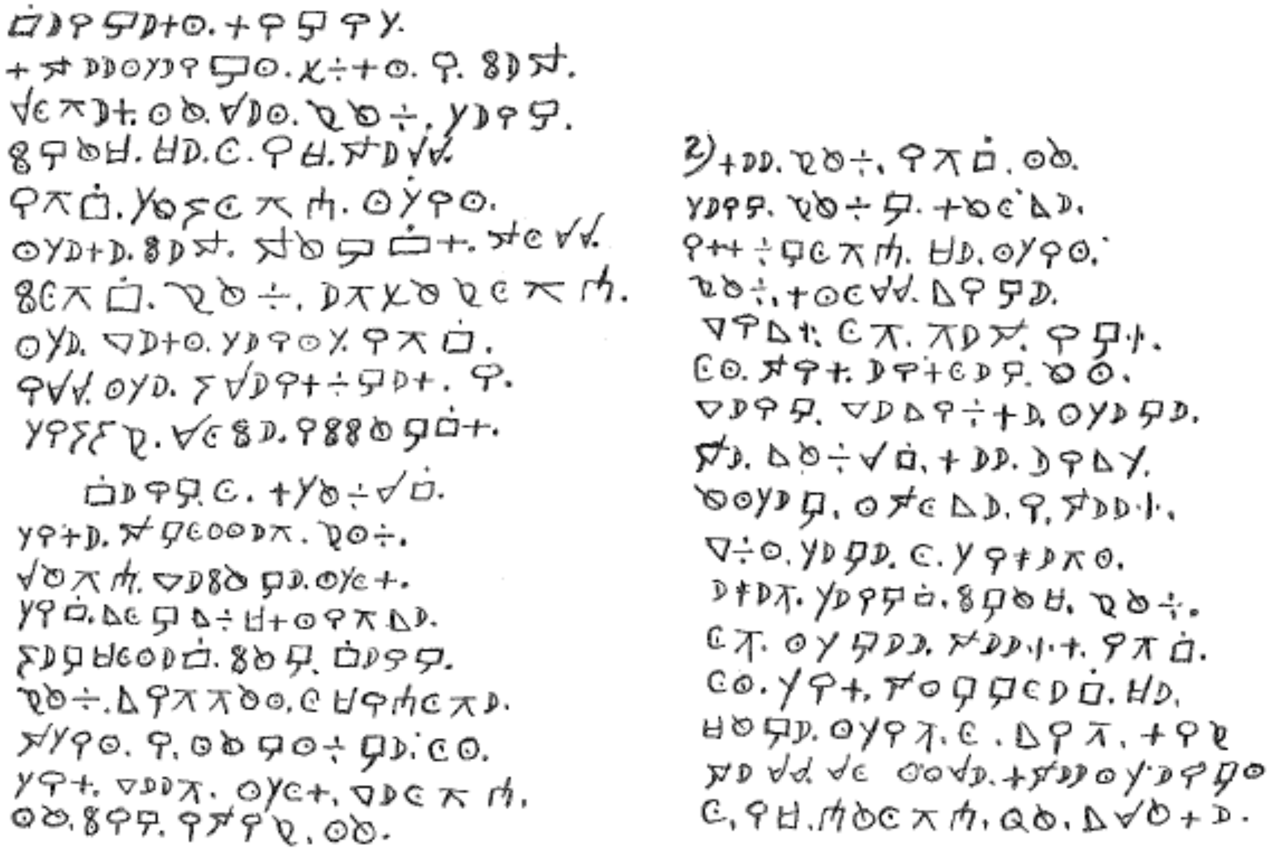
CENERENTOLA. I wish to try if you can read
this and am most anxious to hear that and when you
return and how long you remain here. Go write a few
lines explaining please I have since you went away.

[2] Found in McCormick, Donald, *Love in Code or How to Keep Your Secrets*, Eyre Methuen Ltd., London, 1980, p. 83.

CENERENTOLA. Zsyng rd n jtwy nx xnhp mfaj n y
wnj, yt kwfrj fs jcugfifynts ktw dtz lgzy hfssty.
Xnqjshj nx nf jny nk ymf ywzj bfzxy nx sty xzx jhyji;
nk ny nx, fgg xytwpjx bngg gj xnkyji yt ymjgtyytr. It
dtz wjrjgjw tzw htzxns'x knwxy nwtutxnynts:
ymnsp tk ny. N pstb Dtz.

CENERENTOLA. Until my heart is sick have I
tried to frame an explanation for you but cannot.
Silence is safest if the true cause is not suspected;
if it is, all stories will be sifted to the bottom. Do
remember our cousin's first proposition.
Think of it. I know you.

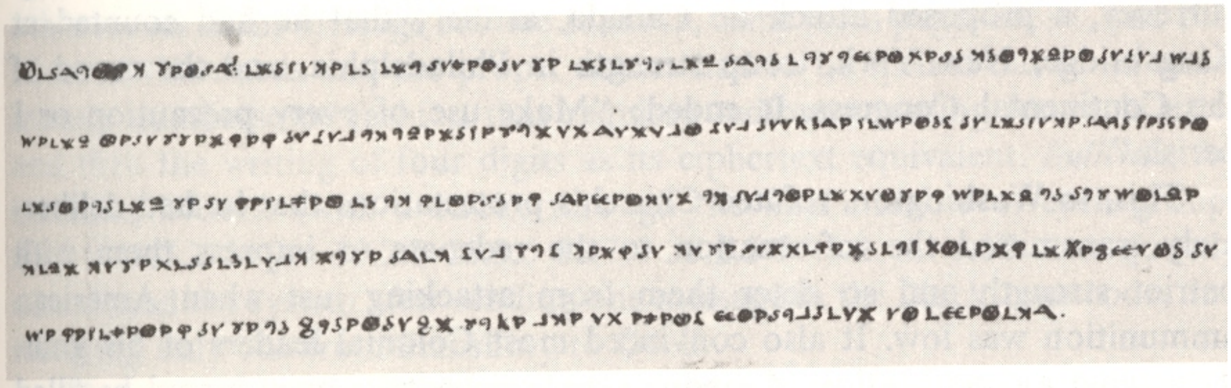
17. The following cipher has been reprinted several times.[3] It deserves to appear again! It was originally found in the prison yard of a penitentiary. Can you solve it?



[3] 1) Signal Corps Bulletin, September-October 1930 p. 55.
2) William F. Friedman, editor, *Cryptography and Cryptanalysis Articles Volume I*, Aegean Park Press, Laguna Hills, California, 1976, p.55.
3) There and There, *Cryptologia*, Vol. 2, No. 2, April 1978, p. 193.

Dearest Sarah, sweetheart: Just a few lines to let you hear from me. I am well and hoping that these few words will find you enjoying the best health and all the pleasures a happy life affords. Dear, I should have written you long before this had circumstances permitted, for dear. You can not imagine what a torture it has been this being too far away to see you and to hear you voice assuring me that you still care. Back in Newark it was easier to bear because there we could see each other twice a week but here haven't even heard from you in three weeks and it has worried me more than I can say. Well, little sweetheart, I am going to close.

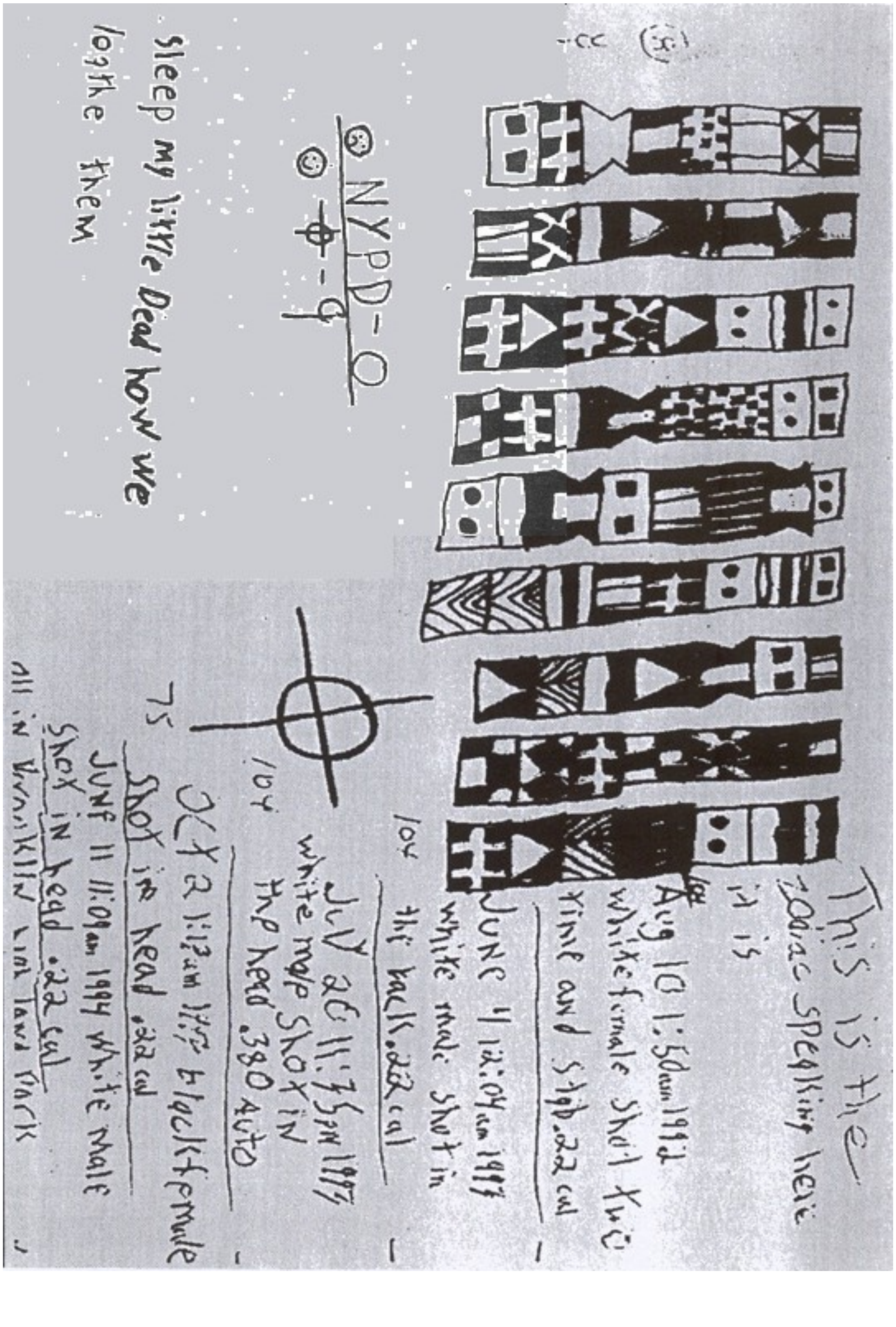
18. The last lines from a cipher message by Dr. Benjamin Church, a double agent working for the British during the Revolutionary War, is reproduced below from page 175 of The Codebreakers. Can you crack it?



The portion reproduced begins near the end of a sentence. That sentence (after deciphering) begins "I wish you could contrive to write me largely in cipher, by the way of Newport, addressed to Thomas." Like many other real ciphers, typos are present.

Richards, merch[an]t. Enclose it in a cover to me, intimating that I am a perfect stranger to you; but being recommended to you as a gentleman of honour, you took the liberty to enclose that letter, entreating me to deliver it as directed; the person, as you are informed, being at Cambri[d]ge. Sign some fictitious name. This you may send to some confidential friend at Newport, to be delivered to me at Watertown Make use of every precaution or I perish.

19. Murderer Heriberto Seda, posing as the Zodiac killer, sent ciphers to the police, just as the original had. Seda's ciphers were simpler. Decipher the one that follows.



This is the
zodiac speaking here
it is
Aug 10 1:50am 1992
white female shot two
time and stab .22 cal

JUNE 4 12:04 am 1993
white male shot in
the back .22 cal 104

JULY 20 11:45pm 1993
white male shot in
the head .380 auto 104

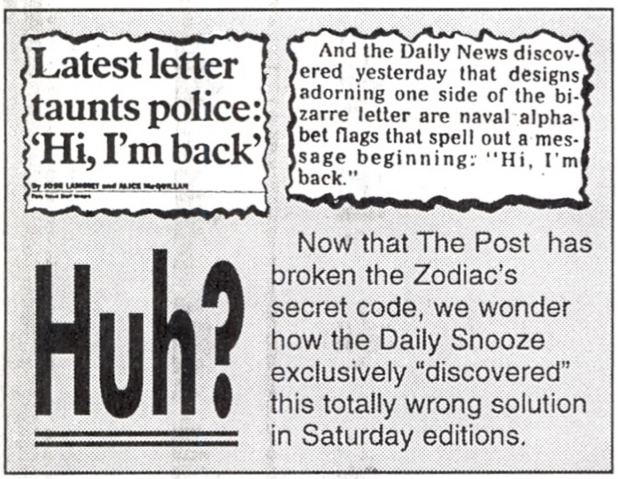
OCT 2 1:12am 1993 black female
shot in head .22 cal 75

JUNE 11 11:09am 1994 white male
shot in head .22 cal
all in brooklin and park

NYPD - O
⊕ - 9

Sleep my little Dead how we
loathe them

Note: *The Daily News* published a decipherment of this that was completely bogus. *New York Post* published the correct decipherment and mocked their competitor's incompetence.



Latest letter taunts police: 'Hi, I'm back'

By JOSE LAMBIET and ALICE McQUILLAN
Daily News Staff Writers

And the Daily News discovered yesterday that designs adorning one side of the bizarre letter are naval alphabet flags that spell out a message beginning: "Hi, I'm back."

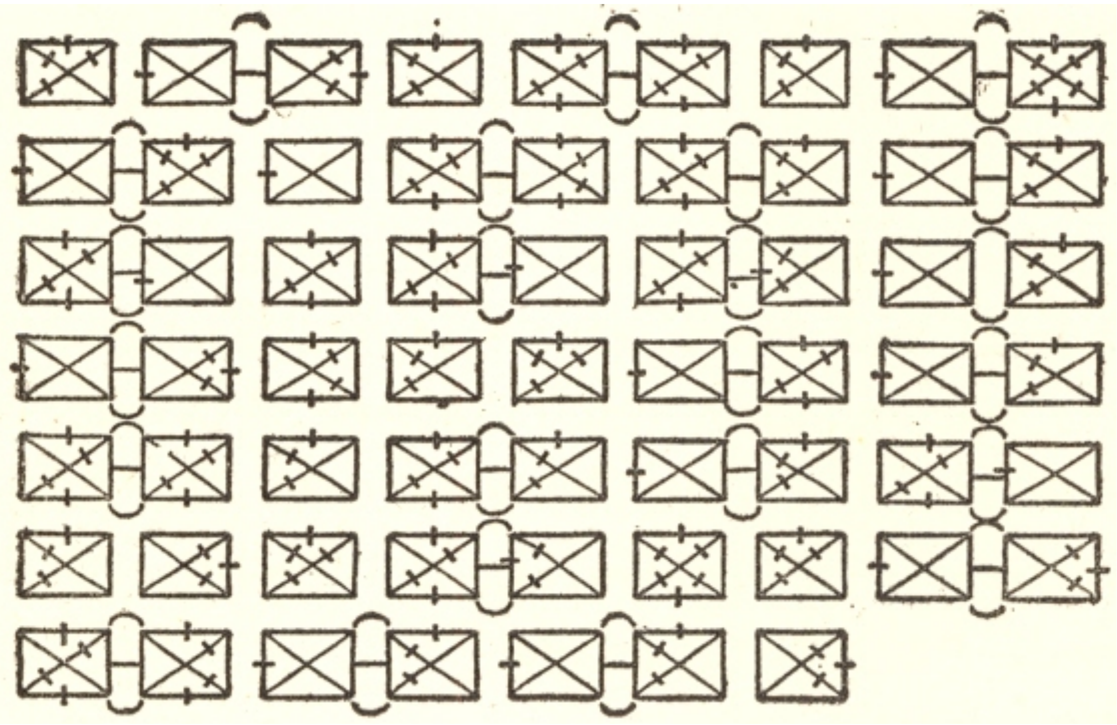
Huh?

Now that The Post has broken the Zodiac's secret code, we wonder how the Daily Snooze exclusively "discovered" this totally wrong solution in Saturday editions.

***New York Post* mocks incompetent cryptanalysts.**[4]

THIS IS THE ZODIAC SPEAKING
I AM IN CONTROL WHO MASTERY
BE READY FOR MORE
YOURS TRULY

20. Solve the ciphertext below from Chambers, Robert W. 1906. *The Tracer of Lost Persons*. New York: Appleton and Company, p. 104. This book is available online at http://www.gutenberg.org/etext/13180, but the cipher isn't included!



[4] Crowley, Kieran, *New York Post*, Monday, August 8, 1994, p. 5.

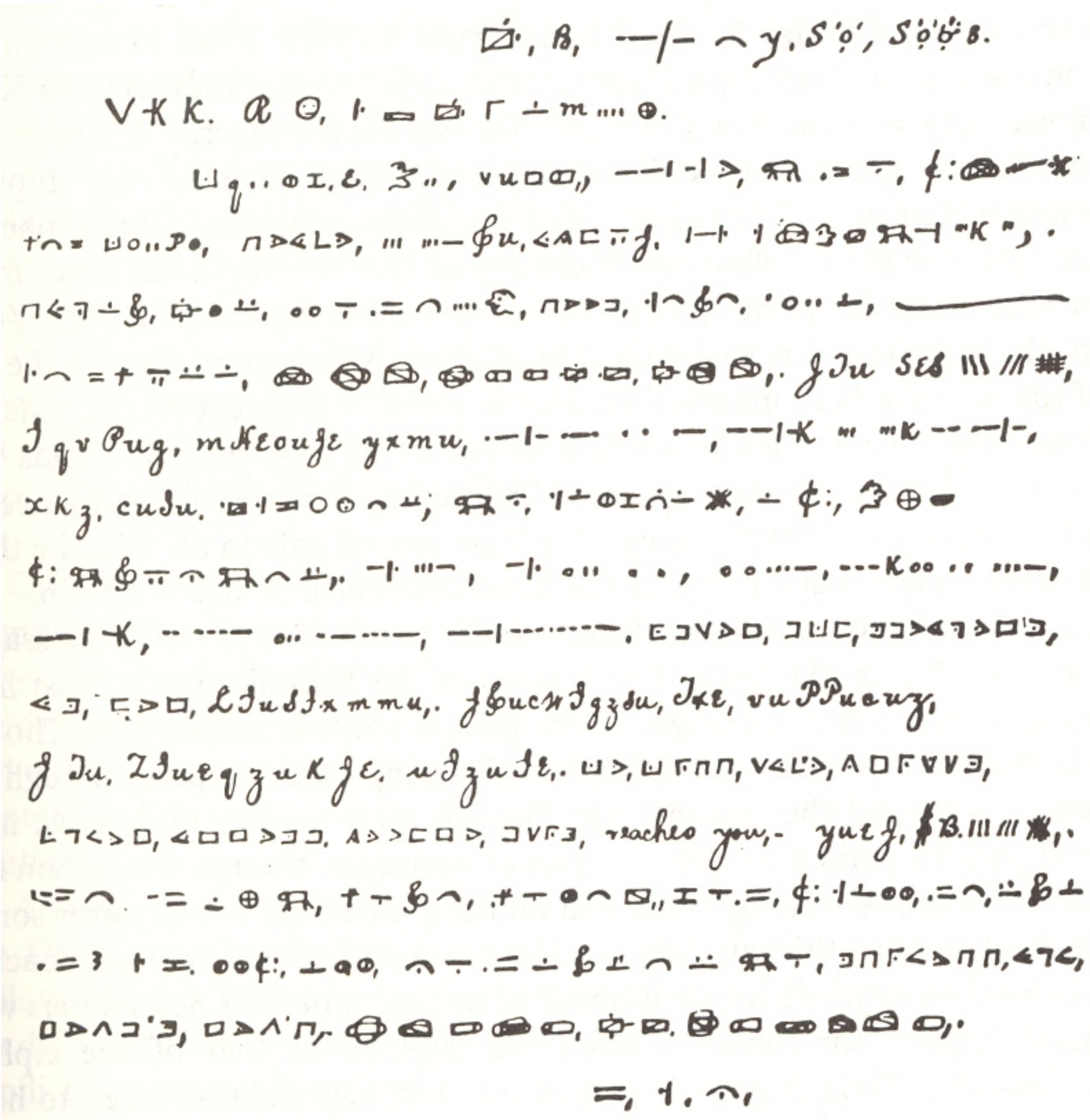
I NEVER SAW YOU BUT ONCE I LOVE YOU EDITH INWOOD

21. The Gold Bug cipher – The cipher from Poe's famous story follows below. Can you crack it?

```
"53++!305))6*;4826)4+)4+).;806*;48!8]60))85;1+8*:+(;:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8]8*;4069285);)6!8)4++;
1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?34;48)4+;161;:
188;+?;"
```

A good glass in the bishop's hostel in the devil's seat
forty-one degrees and thirteen minutes northeast and by north
main branch seventh limb east side shoot from the left eye of the death's-head
a bee line from the tree through the shot fifty feet out.

22. The following ciphertext message was produced by a confederate agent during the Civil War. The Union's codebreakers solved it – can you? (reproduced from page 219 of The Codebreakers)



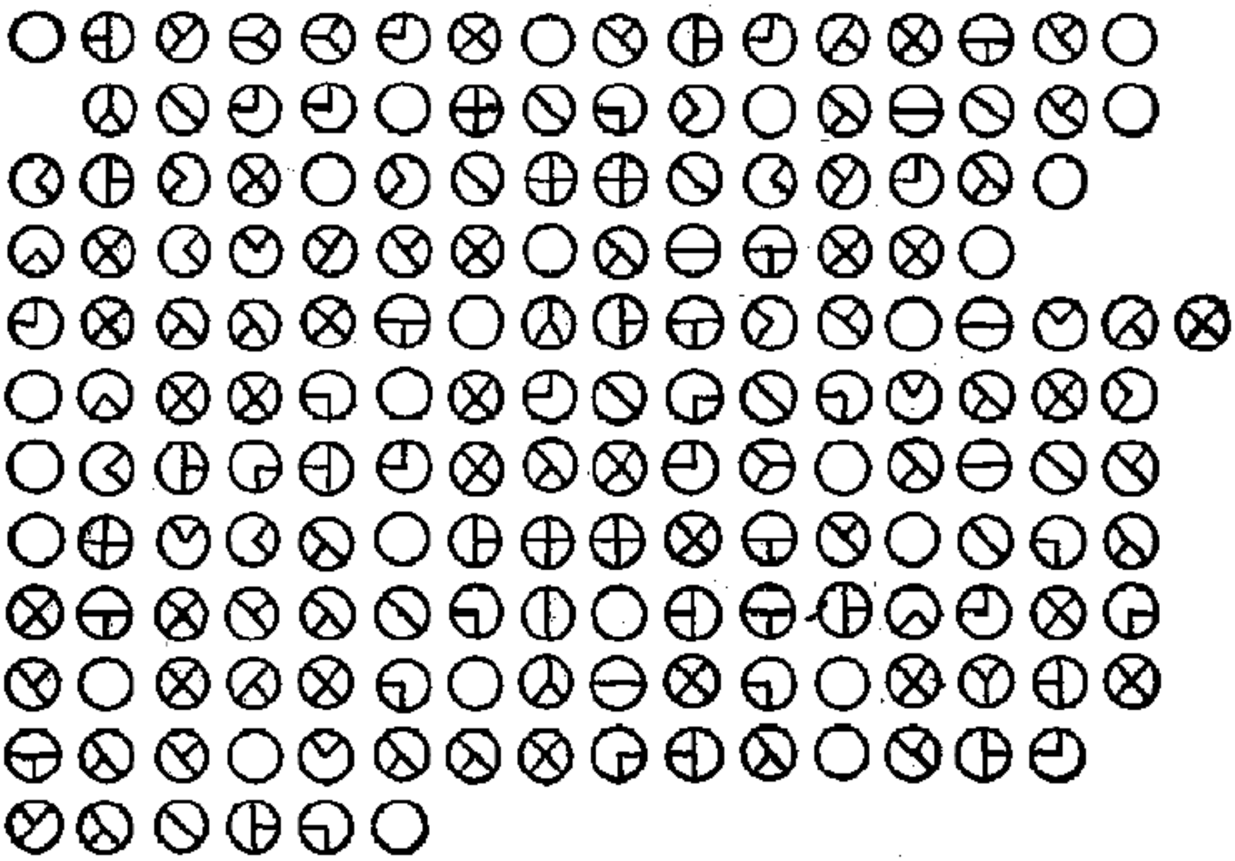
N Y Dec 18 1863

Hon J P Benjamin Secretary of State   Richmond Va

Willis is here The two steamers will leave here about Christmas Lamar and Bowers left here via Bermuda two weeks ago 12000 rifled muskets came duly to hand and were shipped to Halifax as instructed We will be able to seize the other two steamers as per programme Trowbridge has followed the Presidents orders We will have Briggs under arrest before this reaches you Cost $2000 We want more money Hoe shall we draw Bills are forwarded to Slidell and rects recd Write as before

J H C

23. The Shadow, a pulp hero of days gone by, faced the cipher reproduced below in one of his crime-fighting adventures.[5] Can you crack it?



PUZZLE SOLVERS WILL FIND THIS
CODE DIFFICULT BECAUSE THREE
LETTER WORDS HAVE BEEN ELIMINATED
COMPLETELY THIS FACT
OFFERS INTERESTING PROBLEMS
EVEN WHEN EXPERTS ATTEMPT
SOLUTION

24. Crack the following monoalphabetic substitution cipher in Spanish[6] and then use an online translation program such as Yahoo! Babel Fish®, http://babelfish.yahoo.com/, to render it into English:

```
XW YNCAWGNUJ ZJ XW GNARWR ZY RZYRZ SWGZ RNWY RZYZYTZQWRW.
WXHAJUY IWQQNUY MAZQUJ GWYN RZYCQANRUY TUQ GUOTXZCU. XUY
```

[5] Gibson, Walter (writing as Maxwell Grant), #058, Chain of Death, *The Shadow Magazine*, Vol. 10, No. 4, July, 15, 1934, available online at http://www.apprendre-en-ligne.net/crypto/bibliotheque/shadow/shadow340715.pdf.

[6] Taken from Wayne G. Barker's *Cryptograms in Spanish*, Aegean Park Press, Laguna Hills, California, 1985, p.1.

GUOIWCZY NHJUQWQUJ, RZYRZ GAWJRU GUOZJLWQUJ ZX RUONJHU TWYWRU, CQZGZ “GZYZY RZ MAZHU.

La situacion en la ciudad es desde hace dias desperada. Algunos barrios fueron casi destruidos por complete. Los combates ignoraron, desde cuando comenzaron el domingo pasado, trece ceses de fuego.

25. Crack the following monoalphabetic substitution cipher in Portuguese[7] and then use an online translation program such as Yahoo! Babel Fish®, http://babelfish.yahoo.com/, to render it into English:

MICROCOMPUTADORES PORTUGUESES VAO SURGIR ESTA SEMANA NO MERCADO. COM TECNOLOGIA QUE SE EQUIPARA COM A MAIS AVANCADA DO MUNDO, COMECAM ESTA SEMANA A SER COMERCIALIZADOS EM PORTUGAL OS PRIMEIROS MICROCOMPUTADORES DE FABRICO NACIONAL.

26. Crack the following monoalphabetic substitution cipher in German and then use an online translation program such as Yahoo! Babel Fish®, http://babelfish.yahoo.com/, to render it into English. Note: umlauts have been replaced by the same letter without an umlaut, followed by an e. For example, ue was substituted for ü prior to encipherment. The message is an Albert Einstein quote.

DKM VYNOXN WNXDTCYTCGIQG ENXNT UODNCGXDNTGJ PNOVNDCNOT YTX VYNOXN PNOGYKMNT ANDTN SONYTXN RYO NDTTLMAN XNO CINDKMNT ZQGDJDQT RY YNWNORNYCNT

ICH WUERDE BEDINGUNGSLOS JEDEN KRIEGSDIENST VERWEIGERN UND WUERDE VERSUCHEN MEINE FREUNDE ZUR EINNAHME DER GLEICHEN POSITION ZU UEBERZEUGEN.

27. Crack the following monoalphabetic substitution cipher in French[8] and then use an online translation program such as Yahoo! Babel Fish®, http://babelfish.yahoo.com/, to render it into English:

STNXYTJ H’PETLS, STNXYTJ HT WI NILST, R’IWWTJ ZIY I WI VXTSST, STNXYTJ HT ZISULS.

Y’LW NIXU HPRRTS YPR YIRV, IWWTJ HPRRTS WT APUST, APXY TUTY EPR IZPUST, QPRYLTXS WT ZSTYLHTRU.

refusez d’obéir,
refusez de la faire,

[7] Taken from Stewart Todd’s *Cryptograms in Portuguese*, Aegean Park Press, Laguna Hills, California, 1986, p.1.
[8] Thanks to Mary Boldt for suggesting the plaintext.

n’allez pas à la guerre,
refusez de partir.

S’il faut donner son sang,
allez donner le vôtre,
vous êtes bon apôtre,
monsieur le Président.

28. Apply Sukhotin’s Method to the following text and record which letters it categorizes as vowels.

> “The evil incident to invasion of privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of persons at both ends of the line is invaded, and all conversations between them upon any subject, although proper, confidential and privileged, may be overheard. Moreover, the tapping of one man’s telephone line involves the tapping of the telephone of every other person whom he may or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping.”[9]

We start with the following.

	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	R	S	T	U	V	W	Y
A	0	0	3	1	3	1	1	2	2	0	5	6	12	0	5	8	4	10	0	4	1	3
B	0	0	0	0	2	0	0	0	0	1	0	0	0	1	0	0	0	0	2	0	0	0
C	3	0	0	0	2	0	0	0	1	0	0	0	2	3	0	0	0	1	0	0	0	2
D	1	0	0	0	8	0	0	0	2	0	0	0	5	0	0	1	1	0	0	0	0	0
E	3	2	2	8	1	0	4	14	0	1	9	3	18	1	9	18	3	7	0	10	1	0
F	1	0	0	0	0	0	0	0	1	0	0	0	1	10	0	0	0	0	0	0	0	0
G	1	0	0	0	4	0	0	1	0	0	0	0	4	0	0	1	0	0	1	0	0	0
H	2	0	0	0	14	0	1	0	1	0	0	0	0	7	4	1	0	16	0	0	4	0
I	2	0	1	2	0	1	0	1	0	0	6	1	14	4	4	6	7	5	0	5	3	0
J	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
L	5	0	0	0	9	0	0	0	6	0	2	0	0	2	0	0	1	1	0	2	0	0
M	6	0	0	0	3	0	0	0	1	0	0	0	0	3	2	0	0	0	1	0	0	0
N	12	0	2	5	18	1	4	0	14	0	0	0	1	14	0	0	5	4	1	5	0	3
O	0	1	3	0	1	10	0	7	4	0	2	3	14	0	3	3	2	3	1	4	0	0
P	5	0	0	0	9	0	0	4	4	0	0	2	0	3	5	5	1	0	2	0	0	0
R	8	0	0	1	18	0	1	1	6	0	0	0	0	3	5	1	3	1	1	0	1	2
S	4	0	0	1	3	0	0	0	7	0	1	0	5	2	1	3	2	5	1	0	0	0
T	10	0	1	0	7	0	0	16	5	0	1	0	4	3	0	1	5	0	1	0	1	1
U	0	2	0	0	0	0	1	0	0	0	0	1	1	1	2	1	1	1	0	0	0	0
V	4	0	0	0	10	0	0	0	5	0	2	0	5	4	0	0	0	0	0	0	0	0
W	1	0	0	0	1	0	0	4	3	0	0	0	0	0	0	1	0	1	0	0	0	0
Y	3	0	2	0	0	0	0	0	0	0	0	0	3	0	0	2	0	1	0	0	0	0

K Q X AND Z DON’T APPEAR IN THE MESSAGE AND ARE THEREFORE NOT IN THE TABLE

[9] Justice Louis Brandeis, dissenting opinion in Olmstead v. United States (277 U.S. 438, 1928, pp. 475-476), quoted here from Diffie, Whitfield, and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, The MIT Press, Cambridge, Massachusetts, 1998.

Our first step is to make the diagonal all 0 and list the row sums. We start by assuming all letters are consonants, indicated by C.

	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	0	3	1	3	1	1	2	2	0	5	6	12	0	5	8	4	10	0	4	1	3	71	C
B	0	0	0	0	2	0	0	0	0	1	0	0	0	1	0	0	0	0	2	0	0	0	6	C
C	3	0	0	0	2	0	0	0	1	0	0	0	2	3	0	0	0	1	0	0	0	2	14	C
D	1	0	0	0	8	0	0	0	2	0	0	0	5	0	0	1	1	0	0	0	0	0	18	C
E	3	2	2	8	0	0	4	14	0	1	9	3	18	1	9	18	3	7	0	10	1	0	113	C
F	1	0	0	0	0	0	0	0	1	0	0	0	1	10	0	0	0	0	0	0	0	0	13	C
G	1	0	0	0	4	0	0	1	0	0	0	0	4	0	0	1	0	0	1	0	0	0	12	C
H	2	0	0	0	14	0	1	0	1	0	0	0	0	7	4	1	0	16	0	0	4	0	50	C
I	2	0	1	2	0	1	0	1	0	0	6	1	14	4	4	6	7	5	0	5	3	0	62	C
J	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	C
L	5	0	0	0	9	0	0	0	6	0	0	0	0	2	0	0	1	1	0	2	0	0	26	C
M	6	0	0	0	3	0	0	0	1	0	0	0	0	3	2	0	0	0	1	0	0	0	16	C
N	12	0	2	5	18	1	4	0	14	0	0	0	0	14	0	0	5	4	1	5	0	3	88	C
O	0	1	3	0	1	10	0	7	4	0	2	3	14	0	3	3	2	3	1	4	0	0	61	C
P	5	0	0	0	9	0	0	4	4	0	0	2	0	3	0	5	1	0	2	0	0	0	35	C
R	8	0	0	1	18	0	1	1	6	0	0	0	0	3	5	0	3	1	1	0	1	2	51	C
S	4	0	0	1	3	0	0	0	7	0	1	0	5	2	1	3	0	5	1	0	0	0	33	C
T	10	0	1	0	7	0	0	16	5	0	1	0	4	3	0	1	5	0	1	0	1	1	56	C
U	0	2	0	0	0	0	1	0	0	0	0	1	1	1	2	1	1	1	0	0	0	0	11	C
V	4	0	0	0	10	0	0	0	5	0	2	0	5	4	0	0	0	0	0	0	0	0	30	C
W	1	0	0	0	1	0	0	4	3	0	0	0	0	0	0	1	0	1	0	0	0	0	11	C
Y	3	0	2	0	0	0	0	0	0	0	0	0	3	0	0	2	0	1	0	0	0	0	11	C

The highest row sum is for E, so we assume E is a vowel and subtract from each row sum twice the number of times it occurs next to E.

	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	0	3	1	3	1	1	2	2	0	5	6	12	0	5	8	4	10	0	4	1	3	65	C
B	0	0	0	0	2	0	0	0	0	1	0	0	0	1	0	0	0	0	2	0	0	0	2	C
C	3	0	0	0	2	0	0	0	1	0	0	0	2	3	0	0	0	1	0	0	0	2	10	C
D	1	0	0	0	8	0	0	0	2	0	0	0	5	0	0	1	1	0	0	0	0	0	2	C
E	3	2	2	8	0	0	4	14	0	1	9	3	18	1	9	18	3	7	0	10	1	0	113	V
F	1	0	0	0	0	0	0	0	1	0	0	0	1	10	0	0	0	0	0	0	0	0	13	C
G	1	0	0	0	4	0	0	1	0	0	0	0	4	0	0	1	0	0	1	0	0	0	4	C
H	2	0	0	0	14	0	1	0	1	0	0	0	0	7	4	1	0	16	0	0	4	0	22	C
I	2	0	1	2	0	1	0	1	0	0	6	1	14	4	4	6	7	5	0	5	3	0	62	C
J	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	C
L	5	0	0	0	9	0	0	0	6	0	0	0	0	2	0	0	1	1	0	2	0	0	8	C
M	6	0	0	0	3	0	0	0	1	0	0	0	0	3	2	0	0	0	1	0	0	0	10	C
N	12	0	2	5	18	1	4	0	14	0	0	0	0	14	0	0	5	4	1	5	0	3	52	C
O	0	1	3	0	1	10	0	7	4	0	2	3	14	0	3	3	2	3	1	4	0	0	59	C
P	5	0	0	0	9	0	0	4	4	0	0	2	0	3	0	5	1	0	2	0	0	0	17	C
R	8	0	0	1	18	0	1	1	6	0	0	0	0	3	5	0	3	1	1	0	1	2	15	C
S	4	0	0	1	3	0	0	0	7	0	1	0	5	2	1	3	0	5	1	0	0	0	27	C
T	10	0	1	0	7	0	0	16	5	0	1	0	4	3	0	1	5	0	1	0	1	1	42	C
U	0	2	0	0	0	0	1	0	0	0	0	1	1	1	2	1	1	1	0	0	0	0	11	C
V	4	0	0	0	10	0	0	0	5	0	2	0	5	4	0	0	0	0	0	0	0	0	10	C
W	1	0	0	0	1	0	0	4	3	0	0	0	0	0	0	1	0	1	0	0	0	0	9	C
Y	3	0	2	0	0	0	0	0	0	0	0	0	3	0	0	2	0	1	0	0	0	0	11	C

Now the highest consonant row sum is A, so we assume A is a vowel and subtract from each consonant's row sum twice the number of times it occurs next to A.

	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	0	3	1	3	1	1	2	2	0	5	6	12	0	5	8	4	10	0	4	1	3	65	V
B	0	0	0	0	2	0	0	0	0	1	0	0	0	1	0	0	0	0	2	0	0	0	2	C
C	3	0	0	0	2	0	0	0	1	0	0	0	2	3	0	0	0	1	0	0	0	2	4	C
D	1	0	0	0	8	0	0	0	2	0	0	0	5	0	0	1	1	0	0	0	0	0	0	C
E	3	2	2	8	0	0	4	14	0	1	9	3	18	1	9	18	3	7	0	10	1	0	113	V
F	1	0	0	0	0	0	0	0	1	0	0	0	1	10	0	0	0	0	0	0	0	0	11	C
G	1	0	0	0	4	0	0	1	0	0	0	0	4	0	0	1	0	0	1	0	0	0	2	C
H	2	0	0	0	14	0	1	0	1	0	0	0	0	7	4	1	0	16	0	0	4	0	18	C
I	2	0	1	2	0	1	0	1	0	0	6	1	14	4	4	6	7	5	0	5	3	0	58	C
J	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	C
L	5	0	0	0	9	0	0	0	6	0	0	0	0	2	0	0	1	1	0	2	0	0	-2	C
M	6	0	0	0	3	0	0	0	1	0	0	0	0	3	2	0	0	0	1	0	0	0	-2	C
N	12	0	2	5	18	1	4	0	14	0	0	0	0	14	0	0	5	4	1	5	0	3	28	C
O	0	1	3	0	1	10	0	7	4	0	2	3	14	0	3	3	2	3	1	4	0	0	59	C
P	5	0	0	0	9	0	0	4	4	0	0	2	0	3	0	5	1	0	2	0	0	0	7	C
R	8	0	0	1	18	0	1	1	6	0	0	0	0	3	5	0	3	1	1	0	1	2	-1	C
S	4	0	0	1	3	0	0	0	7	0	1	0	5	2	1	3	0	5	1	0	0	0	19	C
T	10	0	1	0	7	0	0	16	5	0	1	0	4	3	0	1	5	0	1	0	1	1	22	C
U	0	2	0	0	0	0	1	0	0	0	0	1	1	1	2	1	1	1	0	0	0	0	11	C
V	4	0	0	0	10	0	0	0	5	0	2	0	5	4	0	0	0	0	0	0	0	0	2	C
W	1	0	0	0	1	0	0	4	3	0	0	0	0	0	0	1	0	1	0	0	0	0	7	C
Y	3	0	2	0	0	0	0	0	0	0	0	0	3	0	0	2	0	1	0	0	0	0	5	C

Now the highest consonant row sum is O, so we assume O is a vowel and subtract from each consonant's row sum twice the number of times it occurs next to O.

	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	0	3	1	3	1	1	2	2	0	5	6	12	0	5	8	4	10	0	4	1	3	65	V
B	0	0	0	0	2	0	0	0	0	1	0	0	0	1	0	0	0	0	2	0	0	0	0	C
C	3	0	0	0	2	0	0	0	1	0	0	0	2	3	0	0	0	1	0	0	0	2	-2	C
D	1	0	0	0	8	0	0	0	2	0	0	0	5	0	0	1	1	0	0	0	0	0	0	C
E	3	2	2	8	0	0	4	14	0	1	9	3	18	1	9	18	3	7	0	10	1	0	113	V
F	1	0	0	0	0	0	0	0	1	0	0	0	1	10	0	0	0	0	0	0	0	0	-9	C
G	1	0	0	0	4	0	0	1	0	0	0	0	4	0	0	1	0	0	1	0	0	0	2	C
H	2	0	0	0	14	0	1	0	1	0	0	0	0	7	4	1	0	16	0	0	4	0	4	C
I	2	0	1	2	0	1	0	1	0	0	6	1	14	4	4	6	7	5	0	5	3	0	50	C
J	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	C
L	5	0	0	0	9	0	0	0	6	0	0	0	0	2	0	0	1	1	0	2	0	0	-6	C
M	6	0	0	0	3	0	0	0	1	0	0	0	0	3	2	0	0	0	1	0	0	0	-8	C
N	12	0	2	5	18	1	4	0	14	0	0	0	0	14	0	0	5	4	1	5	0	3	0	C
O	0	1	3	0	1	10	0	7	4	0	2	3	14	0	3	3	2	3	1	4	0	0	59	V
P	5	0	0	0	9	0	0	4	4	0	0	2	0	3	0	5	1	0	2	0	0	0	1	C
R	8	0	0	1	18	0	1	1	6	0	0	0	0	3	5	0	3	1	1	0	1	2	-7	C
S	4	0	0	1	3	0	0	0	7	0	1	0	5	2	1	3	0	5	1	0	0	0	15	C
T	10	0	1	0	7	0	0	16	5	0	1	0	4	3	0	1	5	0	1	0	1	1	16	C
U	0	2	0	0	0	0	1	0	0	0	0	1	1	1	2	1	1	1	0	0	0	0	9	C
V	4	0	0	0	10	0	0	0	5	0	2	0	5	4	0	0	0	0	0	0	0	0	-6	C
W	1	0	0	0	1	0	0	4	3	0	0	0	0	0	0	1	0	1	0	0	0	0	7	C
Y	3	0	2	0	0	0	0	0	0	0	0	0	3	0	0	2	0	1	0	0	0	0	5	C

Now the highest consonant row sum is I, so we assume I is a vowel and subtract from each consonant's row sum twice the number of times it occurs next to I.

	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	0	3	1	3	1	1	2	2	0	5	6	12	0	5	8	4	10	0	4	1	3	65	V
B	0	0	0	0	2	0	0	0	0	1	0	0	0	1	0	0	0	0	2	0	0	0	0	C
C	3	0	0	0	2	0	0	0	1	0	0	0	2	3	0	0	0	1	0	0	0	2	-4	C
D	1	0	0	0	8	0	0	0	2	0	0	0	5	0	0	1	1	0	0	0	0	0	-4	C
E	3	2	2	8	0	0	4	14	0	1	9	3	18	1	9	18	3	7	0	10	1	0	113	V
F	1	0	0	0	0	0	0	0	1	0	0	0	1	10	0	0	0	0	0	0	0	0	-11	C
G	1	0	0	0	4	0	0	1	0	0	0	0	4	0	0	1	0	0	1	0	0	0	2	C
H	2	0	0	0	14	0	1	0	1	0	0	0	0	7	4	1	0	16	0	0	4	0	2	C
I	2	0	1	2	0	1	0	1	0	0	6	1	14	4	4	6	7	5	0	5	3	0	50	V
J	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	C
L	5	0	0	0	9	0	0	0	6	0	0	0	0	2	0	0	1	1	0	2	0	0	-18	C
M	6	0	0	0	3	0	0	0	1	0	0	0	0	3	2	0	0	0	1	0	0	0	-10	C
N	12	0	2	5	18	1	4	0	14	0	0	0	0	14	0	0	5	4	1	5	0	3	-28	C
O	0	1	3	0	1	10	0	7	4	0	2	3	14	0	3	3	2	3	1	4	0	0	59	V
P	5	0	0	0	9	0	0	4	4	0	0	2	0	3	0	5	1	0	2	0	0	0	-7	C
R	8	0	0	1	18	0	1	1	6	0	0	0	0	3	5	0	3	1	1	0	1	2	-19	C
S	4	0	0	1	3	0	0	0	7	0	1	0	5	2	1	3	0	5	1	0	0	0	1	C
T	10	0	1	0	7	0	0	16	5	0	1	0	4	3	0	1	5	0	1	0	1	1	6	C
U	0	2	0	0	0	0	1	0	0	0	0	1	1	1	2	1	1	1	0	0	0	0	9	C
V	4	0	0	0	10	0	0	0	5	0	2	0	5	4	0	0	0	0	0	0	0	0	-16	C
W	1	0	0	0	1	0	0	4	3	0	0	0	0	0	0	1	0	1	0	0	0	0	1	C
Y	3	0	2	0	0	0	0	0	0	0	0	0	3	0	0	2	0	1	0	0	0	0	5	C

Now the highest consonant row sum is U, so we assume U is a vowel and subtract from each consonant’s row sum twice the number of times it occurs next to U.

	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	0	3	1	3	1	1	2	2	0	5	6	12	0	5	8	4	10	0	4	1	3	65	V
B	0	0	0	0	2	0	0	0	0	1	0	0	0	1	0	0	0	0	2	0	0	0	-4	C
C	3	0	0	0	2	0	0	0	1	0	0	0	2	3	0	0	0	1	0	0	0	2	-4	C
D	1	0	0	0	8	0	0	0	2	0	0	0	5	0	0	1	1	0	0	0	0	0	-4	C
E	3	2	2	8	0	0	4	14	0	1	9	3	18	1	9	18	3	7	0	10	1	0	113	V
F	1	0	0	0	0	0	0	0	1	0	0	0	1	10	0	0	0	0	0	0	0	0	-11	C
G	1	0	0	0	4	0	0	1	0	0	0	0	4	0	0	1	0	0	1	0	0	0	0	C
H	2	0	0	0	14	0	1	0	1	0	0	0	0	7	4	1	0	16	0	0	4	0	2	C
I	2	0	1	2	0	1	0	1	0	0	6	1	14	4	4	6	7	5	0	5	3	0	50	V
J	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	C
L	5	0	0	0	9	0	0	0	6	0	0	0	0	2	0	0	1	1	0	2	0	0	-18	C
M	6	0	0	0	3	0	0	0	1	0	0	0	0	3	2	0	0	0	1	0	0	0	-12	C
N	12	0	2	5	18	1	4	0	14	0	0	0	0	14	0	0	5	4	1	5	0	3	-30	C
O	0	1	3	0	1	10	0	7	4	0	2	3	14	0	3	3	2	3	1	4	0	0	59	V
P	5	0	0	0	9	0	0	4	4	0	0	2	0	3	0	5	1	0	2	0	0	0	-11	C
R	8	0	0	1	18	0	1	1	6	0	0	0	0	3	5	0	3	1	1	0	1	2	-21	C
S	4	0	0	1	3	0	0	0	7	0	1	0	5	2	1	3	0	5	1	0	0	0	-1	C
T	10	0	1	0	7	0	0	16	5	0	1	0	4	3	0	1	5	0	1	0	1	1	4	C
U	0	2	0	0	0	0	1	0	0	0	0	1	1	1	2	1	1	1	0	0	0	0	9	V
V	4	0	0	0	10	0	0	0	5	0	2	0	5	4	0	0	0	0	0	0	0	0	-16	C
W	1	0	0	0	1	0	0	4	3	0	0	0	0	0	0	1	0	1	0	0	0	0	1	C
Y	3	0	2	0	0	0	0	0	0	0	0	0	3	0	0	2	0	1	0	0	0	0	5	C

Now the highest consonant row sum is Y, so we assume Y is a vowel and subtract from each consonant’s row sum twice the number of times it occurs next to Y.

	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	0	3	1	3	1	1	2	2	0	5	6	12	0	5	8	4	10	0	4	1	3	65	V
B	0	0	0	0	2	0	0	0	0	1	0	0	0	1	0	0	0	0	2	0	0	0	-4	C
C	3	0	0	0	2	0	0	0	1	0	0	0	2	3	0	0	0	1	0	0	0	2	-8	C
D	1	0	0	0	8	0	0	0	2	0	0	0	5	0	0	1	1	0	0	0	0	0	-4	C
E	3	2	2	8	0	0	4	14	0	1	9	3	18	1	9	18	3	7	0	10	1	0	113	V
F	1	0	0	0	0	0	0	0	1	0	0	0	1	10	0	0	0	0	0	0	0	0	-11	C
G	1	0	0	0	4	0	0	1	0	0	0	0	4	0	0	1	0	0	1	0	0	0	0	C
H	2	0	0	0	14	0	1	0	1	0	0	0	0	7	4	1	0	16	0	0	4	0	2	C
I	2	0	1	2	0	1	0	1	0	0	6	1	14	4	4	6	7	5	0	5	3	0	50	V
J	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	C
L	5	0	0	0	9	0	0	0	6	0	0	0	0	2	0	0	1	1	0	2	0	0	-18	C
M	6	0	0	0	3	0	0	0	1	0	0	0	0	3	2	0	0	0	1	0	0	0	-12	C
N	12	0	2	5	18	1	4	0	14	0	0	0	0	14	0	0	5	4	1	5	0	3	-36	C
O	0	1	3	0	1	10	0	7	4	0	2	3	14	0	3	3	2	3	1	4	0	0	59	V
P	5	0	0	0	9	0	0	4	4	0	0	2	0	3	0	5	1	0	2	0	0	0	-11	C
R	8	0	0	1	18	0	1	1	6	0	0	0	0	3	5	0	3	1	1	0	1	2	-25	C
S	4	0	0	1	3	0	0	0	7	0	1	0	5	2	1	3	0	5	1	0	0	0	-1	C
T	10	0	1	0	7	0	0	16	5	0	1	0	4	3	0	1	5	0	1	0	1	1	2	C
U	0	2	0	0	0	0	1	0	0	0	0	1	1	1	2	1	1	1	0	0	0	0	9	V
V	4	0	0	0	10	0	0	0	5	0	2	0	5	4	0	0	0	0	0	0	0	0	-16	C
W	1	0	0	0	1	0	0	4	3	0	0	0	0	0	0	1	0	1	0	0	0	0	1	C
Y	3	0	2	0	0	0	0	0	0	0	0	0	3	0	0	2	0	1	0	0	0	0	5	V

Now the highest consonant row sum is a tie between `H` and `T`. We pick `H`, since it appears before `T` in our table (an arbitrary rule for tie-breaking). We assume `H` is a vowel and subtract from each consonant's row sum twice the number of times it occurs next to `H`.

	A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	0	3	1	3	1	1	2	2	0	5	6	12	0	5	8	4	10	0	4	1	3	65	V
B	0	0	0	0	2	0	0	0	0	1	0	0	0	1	0	0	0	0	2	0	0	0	-4	C
C	3	0	0	0	2	0	0	0	1	0	0	0	2	3	0	0	0	1	0	0	0	2	-8	C
D	1	0	0	0	8	0	0	0	2	0	0	0	5	0	0	1	1	0	0	0	0	0	-4	C
E	3	2	2	8	0	0	4	14	0	1	9	3	18	1	9	18	3	7	0	10	1	0	113	V
F	1	0	0	0	0	0	0	0	1	0	0	0	1	10	0	0	0	0	0	0	0	0	-11	C
G	1	0	0	0	4	0	0	1	0	0	0	0	4	0	0	1	0	0	1	0	0	0	-2	C
H	2	0	0	0	14	0	1	0	1	0	0	0	0	7	4	1	0	16	0	0	4	0	2	V
I	2	0	1	2	0	1	0	1	0	0	6	1	14	4	4	6	7	5	0	5	3	0	50	V
J	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	C
L	5	0	0	0	9	0	0	0	6	0	0	0	0	2	0	0	1	1	0	2	0	0	-18	C
M	6	0	0	0	3	0	0	0	1	0	0	0	0	3	2	0	0	0	1	0	0	0	-12	C
N	12	0	2	5	18	1	4	0	14	0	0	0	0	14	0	0	5	4	1	5	0	3	-36	C
O	0	1	3	0	1	10	0	7	4	0	2	3	14	0	3	3	2	3	1	4	0	0	59	V
P	5	0	0	0	9	0	0	4	4	0	0	2	0	3	0	5	1	0	2	0	0	0	-19	C
R	8	0	0	1	18	0	1	1	6	0	0	0	0	3	5	0	3	1	1	0	1	2	-27	C
S	4	0	0	1	3	0	0	0	7	0	1	0	5	2	1	3	0	5	1	0	0	0	-1	C
T	10	0	1	0	7	0	0	16	5	0	1	0	4	3	0	1	5	0	1	0	1	1	-30	C
U	0	2	0	0	0	0	1	0	0	0	0	1	1	1	2	1	1	1	0	0	0	0	9	V
V	4	0	0	0	10	0	0	0	5	0	2	0	5	4	0	0	0	0	0	0	0	0	-16	C
W	1	0	0	0	1	0	0	4	3	0	0	0	0	0	0	1	0	1	0	0	0	0	-7	C
Y	3	0	2	0	0	0	0	0	0	0	0	0	3	0	0	2	0	1	0	0	0	0	5	V

None of the consonants have positive row sums at this point, so we stop. We've identified `E`, `A`, `O`, `I`, `U`, `Y`, and `H` as the vowels. We obtained all of the actual vowels and only misidentified one consonant, `H`, as a vowel. Of course, we wouldn't expect seven vowels, so we could eliminate any extras. Our greatest confidence is in the vowels identified in the earliest iterations.

29. Apply Sukhotin's Method to the following text and record which letters it categorizes as vowels. Use every letter, including those in names.

> "Senator Herman Talmadge: Do you remember when we were in law school, we studied a famous principle of law that came from England and also is well known in this country, that no matter how humble a man's cottage is, that even the King of England cannot enter without his consent.
>
> Witness John Ehrlichman: I am afraid that has been considerably eroded over the years, has it not?
>
> Senator Talmadge: Down in my country we still think of it as a pretty legitimate piece of law."[10]

We start with the following.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0
E	1	2	2	4	1	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0
L	8	2	0	0	4	0	2	0	2	0	0	2	2	0	1	1	1	1	0	0	0	0	1
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1
N	9	0	1	3	10	0	3	1	6	0	2	0	0	1	6	0	0	3	5	2	0	2	0
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	1	0	4	1	5	5	1	3	1
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	1	2	1	0	0	0
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	3	2	0	0	1
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0

Q, X, AND Z DON'T APPEAR IN THE MESSAGE AND ARE THEREFORE NOT IN THE TABLE

[10] United States Senate, Select Committee on Presidential Campaign Activities, Hearings, Phase 1: Watergate Investigation, Ninety-Third Congress, First Session, 1973, p. 2601, quoted here from Diffie, Whitfield, and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, The MIT Press, Cambridge, Massachusetts, 1998.

Our first step is to make the diagonal all 0 and list the row sums. We start by assuming all letters are consonants, indicated by C.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0	63	C
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	7	C
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0	15	C
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0	18	C
E	1	2	2	4	0	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1	64	C
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0	8	C
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0	13	C
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0	34	C
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0	39	C
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	C
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	3	C
L	8	2	0	0	4	0	2	0	2	0	0	0	2	0	1	1	1	1	0	0	0	0	1	25	C
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1	23	C
N	9	0	1	3	10	0	3	1	6	0	2	0	0	0	6	0	0	3	5	2	0	2	0	53	C
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	0	0	4	1	5	5	1	3	1	46	C
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0	5	C
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2	31	C
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	0	2	1	0	0	0	22	C
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	0	2	0	0	1	48	C
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0	13	C
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	4	C
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0	16	C
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0	7	C

The highest row sum is for E, so we assume E is a vowel and subtract from each row sum twice the number of times it occurs next to E.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0	61	C
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	3	C
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0	11	C
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0	10	C
E	1	2	2	4	0	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1	64	V
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0	8	C
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0	5	C
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0	24	C
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0	35	C
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	C
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	3	C
L	8	2	0	0	4	0	2	0	2	0	0	0	2	0	1	1	1	1	0	0	0	0	1	17	C
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1	19	C
N	9	0	1	3	10	0	3	1	6	0	2	0	0	0	6	0	0	3	5	2	0	2	0	33	C
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	0	0	4	1	5	5	1	3	1	46	C
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0	5	C
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2	9	C
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	0	2	1	0	0	0	14	C
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	0	2	0	0	1	40	C
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0	13	C
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-2	C
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0	6	C
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0	5	C

Now the highest consonant row sum is A, so we assume A is a vowel and subtract from each consonant's row sum twice the number of times it occurs next to A.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0	61	V
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	1	C
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0	7	C
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0	6	C
E	1	2	2	4	0	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1	64	V
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0	4	C
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0	3	C
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0	12	C
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0	33	C
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	C
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	3	C
L	8	2	0	0	4	0	2	0	2	0	0	0	2	0	1	1	1	1	0	0	0	0	1	1	C
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1	-1	C
N	9	0	1	3	10	0	3	1	6	0	2	0	0	0	6	0	0	3	5	2	0	2	0	15	C
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	0	0	4	1	5	5	1	3	1	46	C
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0	5	C
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2	3	C
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	0	2	1	0	0	0	8	C
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	0	2	0	0	1	18	C
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0	13	C
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-2	C
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0	0	C
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0	5	C

Now the highest consonant row sum is O, so we assume O is a vowel and subtract from each consonant's row sum twice the number of times it occurs next to O.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0	61	V
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	1	C
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0	-3	C
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0	0	C
E	1	2	2	4	0	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1	64	V
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0	-4	C
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0	3	C
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0	4	C
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0	33	C
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	C
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	3	C
L	8	2	0	0	4	0	2	0	2	0	0	0	2	0	1	1	1	1	0	0	0	0	1	-1	C
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1	-5	C
N	9	0	1	3	10	0	3	1	6	0	2	0	0	0	6	0	0	3	5	2	0	2	0	3	C
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	0	0	4	1	5	5	1	3	1	46	V
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0	5	C
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2	-5	C
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	0	2	1	0	0	0	6	C
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	0	2	0	0	1	8	C
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0	3	C
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-4	C
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0	-6	C
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0	3	C

Now the highest consonant row sum is I, so we assume I is a vowel and subtract from each consonant's row sum twice the number of times it occurs next to I.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0	61	V
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	1	C
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0	-7	C
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0	-6	C
E	1	2	2	4	0	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1	64	V
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0	-4	C
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0	1	C
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0	-2	C
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0	33	V
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	C
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	1	C
L	8	2	0	0	4	0	2	0	2	0	0	0	2	0	1	1	1	1	0	0	0	0	1	-5	C
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1	-7	C
N	9	0	1	3	10	0	3	1	6	0	2	0	0	0	6	0	0	3	5	2	0	2	0	-9	C
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	0	0	4	1	5	5	1	3	1	46	V
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0	1	C
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2	-7	C
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	0	2	1	0	0	0	-4	C
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	0	2	0	0	1	-6	C
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0	3	C
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-4	C
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0	-10	C
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0	3	C

Now the highest consonant row sum is a tie between U and Y. We pick U, since it appears before Y in our table (an arbitrary rule for tie-breaking). We assume U is a vowel and subtract from each consonant's row sum twice the number of times it occurs next to U.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0	61	V
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	1	C
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0	-7	C
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0	-8	C
E	1	2	2	4	0	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1	64	V
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0	-4	C
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0	1	C
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0	-4	C
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0	33	V
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	C
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	1	C
L	8	2	0	0	4	0	2	0	2	0	0	0	2	0	1	1	1	1	0	0	0	0	1	-5	C
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1	-9	C
N	9	0	1	3	10	0	3	1	6	0	2	0	0	0	6	0	0	3	5	2	0	2	0	-13	C
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	0	0	4	1	5	5	1	3	1	46	V
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0	1	C
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2	-7	C
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	0	2	1	0	0	0	-6	C
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	0	2	0	0	1	-10	C
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0	3	V
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-4	C
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0	-10	C
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0	3	C

Now the highest consonant row sum is Y, so we assume Y is a vowel and subtract from each consonant's row sum twice the number of times it occurs next to Y.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0	61	V
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	1	C
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0	-7	C
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0	-8	C
E	1	2	2	4	0	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1	64	V
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0	-4	C
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0	1	C
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0	-4	C
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0	33	V
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	C
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	1	C
L	8	2	0	0	4	0	2	0	2	0	0	0	2	0	1	1	1	1	0	0	0	0	1	-7	C
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1	-11	C
N	9	0	1	3	10	0	3	1	6	0	2	0	0	0	6	0	0	3	5	2	0	2	0	-13	C
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	0	0	4	1	5	5	1	3	1	46	V
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0	1	C
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2	-11	C
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	0	2	1	0	0	0	-6	C
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	0	2	0	0	1	-12	C
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0	3	V
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-4	C
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0	-10	C
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0	3	V

Now the highest consonant row sum is a tie between B, G, K, and P. We pick B, since it appears before the rest in our table. We assume B is a vowel and subtract from each consonant's row sum twice the number of times it occurs next to B.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0	61	V
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	1	V
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0	-7	C
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0	-8	C
E	1	2	2	4	0	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1	64	V
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0	-4	C
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0	1	C
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0	-4	C
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0	33	V
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	C
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	1	C
L	8	2	0	0	4	0	2	0	2	0	0	0	2	0	1	1	1	1	0	0	0	0	1	-11	C
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1	-15	C
N	9	0	1	3	10	0	3	1	6	0	2	0	0	0	6	0	0	3	5	2	0	2	0	-13	C
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	0	0	4	1	5	5	1	3	1	46	V
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0	1	C
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2	-11	C
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	0	2	1	0	0	0	-6	C
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	0	2	0	0	1	-12	C
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0	3	V
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-4	C
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0	-10	C
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0	3	V

Now the highest consonant row sum is a tie between G, K, and P. We pick G, since it appears before the rest in our table. We assume G is a vowel and subtract from each consonant’s row sum twice the number of times it occurs next to G.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0	61	V
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	1	V
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0	-7	C
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0	-12	C
E	1	2	2	4	0	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1	64	V
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0	-4	C
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0	1	V
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0	-4	C
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0	33	V
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	C
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	1	C
L	8	2	0	0	4	0	2	0	2	0	0	0	2	0	1	1	1	1	0	0	0	0	1	-15	C
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1	-15	C
N	9	0	1	3	10	0	3	1	6	0	2	0	0	0	6	0	0	3	5	2	0	2	0	-19	C
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	0	0	4	1	5	5	1	3	1	46	V
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0	1	C
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2	-11	C
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	0	2	1	0	0	0	-6	C
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	0	2	0	0	1	-12	C
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0	3	V
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-4	C
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0	-10	C
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0	3	V

Now the highest consonant row sum is a tie between K, and P. We pick K, since it appears before the rest in our table. We assume K is a vowel and subtract from each consonant’s row sum twice the number of times it occurs next to K.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	Y	SUM	C or V
A	0	1	2	2	1	2	1	6	1	0	0	8	10	9	0	0	3	3	11	0	0	3	0	61	V
B	1	0	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	1	V
C	2	0	0	0	2	0	0	2	2	0	0	0	0	1	5	0	0	1	0	0	0	0	0	-7	C
D	2	0	0	0	4	0	2	0	3	0	0	0	0	3	3	0	0	0	0	1	0	0	0	-12	C
E	1	2	2	4	0	0	4	5	2	0	0	4	2	10	0	0	11	4	4	0	3	5	1	64	V
F	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	2	0	0	0	0	0	0	-4	C
G	1	0	0	2	4	0	0	0	1	0	0	2	0	3	0	0	0	0	0	0	0	0	0	1	V
H	6	0	2	0	5	0	0	0	3	0	0	0	1	1	4	0	1	0	9	1	0	1	0	-4	C
I	1	0	2	3	2	0	1	3	0	0	1	2	1	6	0	2	1	5	7	0	0	2	0	33	V
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-1	C
K	0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	1	V
L	8	2	0	0	4	0	2	0	2	0	0	0	2	0	1	1	1	1	0	0	0	0	1	-15	C
M	10	2	0	0	2	0	0	1	1	0	0	2	0	0	2	0	1	0	0	1	0	0	1	-15	C
N	9	0	1	3	10	0	3	1	6	0	2	0	0	0	6	0	0	3	5	2	0	2	0	-23	C
O	0	0	5	3	0	4	0	4	0	1	0	1	2	6	0	0	4	1	5	5	1	3	1	46	V
P	0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	2	0	0	0	0	0	0	1	C
R	3	0	0	0	11	2	0	1	1	0	0	1	1	0	4	2	0	1	2	0	0	0	2	-11	C
S	3	0	1	0	4	0	0	0	5	0	0	1	0	3	1	0	1	0	2	1	0	0	0	-6	C
T	11	0	0	0	4	0	0	9	7	0	0	0	0	5	5	0	2	2	0	2	0	0	1	-12	C
U	0	0	0	1	0	0	0	1	0	0	0	0	1	2	5	0	0	1	2	0	0	0	0	3	V
V	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	-4	C
W	3	0	0	0	5	0	0	1	2	0	0	0	0	2	3	0	0	0	0	0	0	0	0	-10	C
Y	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	2	0	1	0	0	0	0	3	V

There is only one consonant left that has a positive row some, namely P, so we assume P is a vowel and stop. We've identified `E`, `A`, `O`, `I`, `U`, `Y`, `B`, `G`, `K`, and `P` as the vowels. We obtained all of the actual vowels, but misidentified four consonants as vowels. Of course, we wouldn't expect seven vowels, so we could eliminate any extras. Our greatest confidence is in the vowels identified in the earliest iterations.

30. For all ciphers (except the one-time pad, which we'll discuss later) there is an amount of ciphertext that can have only one possible plaintext solution. If the cryptanalyst has enough time, it can be found, through brute-force, if not by other means. This length of ciphertext is referred to as the unicity point. For a monoalphabetic substitution cipher, this length is 27-30 characters (30 according to Claude Shannon's "Communication Theory of Secrecy Systems" October 1949, p. 660 using H(K)/D, log base 10, D=.7 – but Deavours page 54 says 24 letters (backed by formula) and he mentions Friedman who estimated 25). Monoalphabetic substitution ciphers shorter than this may have more than one solution and the cryptanalyst might not be able to decide which is right. How many solutions can you find for the following?

```
H PHDM RVOS WJJDF
```

I enciphered `I LIKE MATH BOOKS.`

Many other decipherments are possible. Only a few are given below. If you don't use a computer to hunt for solutions, what you find might indicate something about your personality!

```
I LIKE MANY BOOKS
I LIKE ARMY COOKS
A LADY WITH NEEDS
A PARK WITH BEERS
```

31. How many monoalphabetic substitution ciphers are there in which no letter is enciphered as itself? In other words, how many derangements are there on a 26 letter alphabet? (Recall that a derangement is a rearrangement of objects such that none occupies its original position.) An outline of how to solve this problem is presented below.

a) Often solving a simpler problem gives insight into the harder problem.

For a two letter alphabet, **ab**, there are two arrangements: ab and ba.
Thus, we have 1 arragement and 1 derangement.

Now consider three letters, **abc**. There are 3! = 6 arrangements. Listing them all:
abc, acb, bac, bca, cab, cba, we see that 2 are derangements.

Keep enlarging the alphabet and be careful to count each possibility. You won't get to the answer for the full 26 letter alphabet, but a pattern will emerge, so that you don't need to.

Letting D_n denote the number of derangements for n letters, one pattern that emerges is $D_n = (n - 1)(D_{n-1} + D_{n-2})$. Thus, we get the following values (up to the desired D_{26}):

N	D_n
2	1
3	2
4	9
5	44
6	265
7	1854
8	14833
9	133496
10	1334961
11	14684570
12	176214841
13	2290792932
14	32071101049
15	481066515734
16	7697064251745
17	130850092279664
18	2355301661033953
19	44750731559645106
20	895014631192902121
21	18795307255050944540
22	413496759611120779881
23	9510425471055777937262
24	228250211305338670494289
25	5706255282633466762357224
26	148362637348470135821287825

b) Use your answers from a) to fill in as many rows of the table below as needed, until you see the pattern that emerges in the final column. What do you think the limit as n approached infinity of A_n/D_n is?

N	Arrangements	Derangements	Arr/Der
1	1	0	NA
2	2	1	2
3	6	2	3

The answer can be found at http://mathworld.wolfram.com/Subfactorial.html, but work on it yourself first!

N	**Arrangements**	**Derangements**	**Arr/Der**
1	1	0	NA
2	2	1	2
3	6	2	3
4	24	9	2.66666666666666666…
5	120	44	2.72727272727272727…
6	720	265	2.71698113207547169…
7	5040	1854	2.71844660194174757…
8	40320	14833	2.71826333176026427…
9	362880	133496	2.71828369389344999…
10	3628800	1334961	2.71828165766640373…
11	39916800	14684570	2.71828184277782733…
12	479001600	176214841	2.71828182735187440…
13	6227020800	2290792932	2.71828182853848616…
14	87178291200	32071101049	2.71828182845372818…
15	1307674368000	481066515734	2.71828182845937871…

The last column will converge to e as n approaches infinity.

32. Refer back to the sample cipher from the original Zodiac killer. Give some evidence supporting the conclusion that it isn't a monoalphabetic substitution cipher.

There are far more than 26 distinct symbols in the cipher.

33. Suppose you attack a monoalphabetic substitution cipher by using brute force. That is, every possible substitution alphabet is tried without any attention being paid to the statistics. How long will it take, on average, to find the solution if

a) a different key is tested every second?

Since 26! = 403291461126605635584000000, it will take that many seconds. Dividing by approximately 60*60*24*365.25 seconds per year, we get 12779535234827922135 years to try every key. On average, the correct solution will be obtained after trying half of the keys. Thus, the answer is about 6389767617413961067 years.

c) a million distinct keys are tested every second?

Dividing our previous result by a million, we get 638976717413 years, which is still far greater than the age of the universe.

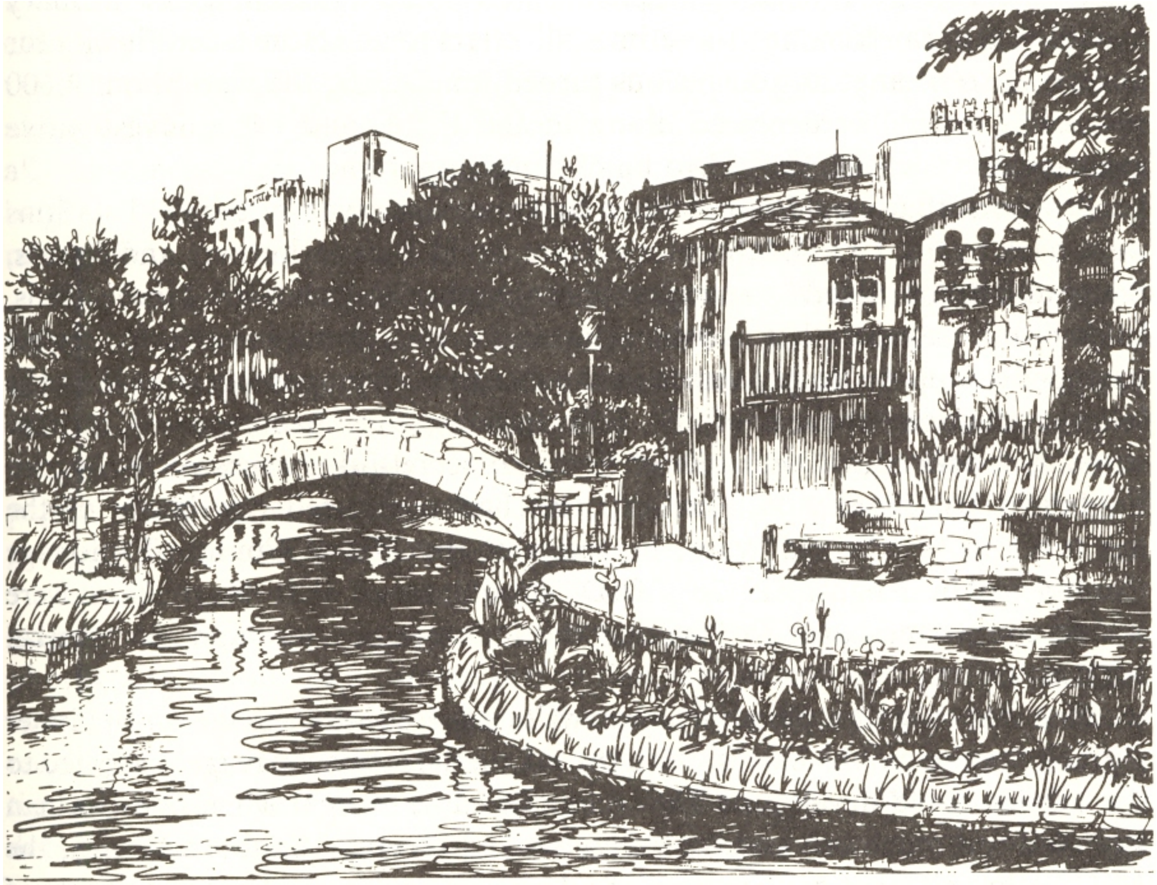
34. Make up a cipher of your own, like the ones discussed in this chapter, and challenge a friend to break it!

Answers will, of course, vary.

35. When using Morse code, it is important to leave spaces between the letters. Can you come up with a message in Morse code, like the example in this chapter, that has two possible decodings if the spacing is altered?

Answers will vary. The results of a thorough study of this problem are presented at http://www.datagenetics.com/blog/march42012/results.html.

36. Can you find the secret message in the seemingly innocent sketch of San Antonio's Riverwalk below? It was made in the 1940s at the San Antonio postal censorship station and uses Morse code.[11]



San Antonio's Riverwalk[12]

The message is conveyed in Morse code using short blades of grass for dots and long blades of grass for dashes. It reads

Compliments of CPSA MA to our chief Col. Harold R. Shaw on his visit to San Antonio May 11th 1945.

37. Encipher the following using an affine cipher with the key (15, 9).

[11] Kahn, David, *The Codebreakers*, 2nd ed., Scribner, New York, 1996, p. 1134.

[12] Picture from Kahn, David, *The Codebreakers*, Second edition, Scribner, New York, 1996, p. 523.

TOO MANY MATH AND SCIENCE MAJORS END UP WORKING FOR SKYNET

ILL HJWF HJIK JWC TNZRWNR HJOLET RWC XA BLEDZWV GLE TDFWRI

38. Encipher the following with an affine cipher using the key (3, 18).

WE MATHEMATICIANS ARE ALL A LITTLE BIT CRAZY

GE CSXNECSXQYQSFU SRE SZZ S ZQXXZE VQX YRSPM

39. If an affine cipher uses the key (21, 4) for enciphering, what key pair can be used to decipher?

(5,6)

40. If an affine cipher uses the key (11, 5) for enciphering, what key pair can be used to decipher?

(19,9)

41. Crack the following affine cipher (using any technique you like) and recover the key.

05 25 04 00 02 14 14 22 12 18 04 05 02 09 04 05 05 04 17 00 22 17
01 23 06 24 14 22 12 23 22 15 05 03 12 05 12 03 00 06 05 25 24 12
09 24 05 02 15 23 02 17 23 02 15 14 05 25 06 15 18

THE WAY YOU GET A BETTER WORLD IS YOU DON’T PUT UP WITH SUB STANDARD ANYTHING.

This quote is from Joe Strummer of The Clash.

The Key was (7, 2).

42. Crack the following affine cipher (using any technique you like) and recover the key.

10 18 24 22 04 17 24 22 01 02 06 14 19 01 02 13 24 11 04 16 24 01
19 15 06 01 19 04 18 10 08 04 22 10 01 04 17 17 24 09 24 20
10 23 20 04 22 01 02 17

A MISER IS TOUGH TO LIVE WITH, BUT HE MAKES A TERRIFIC ANCESTOR.

This quote is from issue 205 (March 1979) of MAD Magazine.

The key was (5, 10).

43. Consider the alphabet portion of a nomenclator and the homophones. If there are N homophones for each letter, the unicity point is given by $(\log((26*N)!/(N!)^{26}))/1.11$.[13] Typically one would have more homophones for more frequent letters, rather than the same number for all. If the Zodiac, in his 340 character unsolved cipher, distributed the homophones evenly, should a unique solution exist?

The table below shows that Zodiac's message is likely to have a unique solution if 10 or fewer homophones existed for each letter.

N	$(\log((26*N)!/(N!)^{26}))/1.11$
2	54
3	86
4	117
5	149
6	182
7	214
8	248
9	279
10	312
11	344

If 10 homophones were used for each letter, then 260 distinct symbols would be required for the system. The cipher in question only contains 65 distinct symbols, but we may not immediately conclude than less than 260 existed. It is, for example, unlikely that the original 340 character plaintext message would contain the letter Z ten times. Hence, there could be homophones in the system that were not required by the messsage. Thus, we need to look a bit closer.

Using Table 2.1, we see that E is about 12.7%, of typical English text, so the original message should contain about (.127)(340) = 43 Es. On the other hand, we'd only expect (.001)(340) = .34 Zs.

So, if we assume the homophones were used uniformly, we should have seen all 10 representations of E in the ciphertext, but none of the representations of Z (since Z is not likely to appear in the original message).

So, for which letters should we expect to see all 10 possible representations? We need the frequency of the letter times 340 to exceed 9.5. In other words, the frequency of the letter must exceed 9.5/340 or 2.79%. According to Table 2.1, A, C, D, E, H, I, L, N, O, R, S, T, and U all exceed this value. Hence, these 13 letters should each be represented by all 10 homophones somewhere in the ciphertext. This puts us at 130 distinct symbols. The fact that other letters (with lower frequencies) likely occur (although not 10 times each) is no longer relevant. We've already seen that we can expect far more than the 65 distinct symbols that are present, if 10 (or more) homophones existed for each letter.

[13] The formulas for the unicity point were taken from Deavours, C. A., Unicity Points in Cryptanalysis, *Cryptologia*, Vol. 1, No. 1, January 1977.

Thus, it is likely that zodiac used fewer than 10 homophones for each letter, and therefore the ciphertext length exceeds the unicity point. In other words, a unique solution can be expected.

44. If I wish to send a message 1,000 letters long, how many homophones should I have for each letter, if I want the unicity point to exceed the message length? Note: If I continue to send messages in this system, I’m in danger when the total length of all messages exceeds the unicity point. It isn’t sufficient to have each individual message beneath the unicity point – they will be attacked as a group!

The two values shown below indicate that 31 homophones for each letter would be required to keep a 1000 character message below the unicity point.

N	$(\log((26*N)!/(N!)^{26}))/1.11$
30	969
31	1002

45. Below is a message sent by General Charles Cornwallis less than a year before he surrendered to General George Washington at Yorktown in 1781, ending the Revolutionary War. It uses homophones and nulls, but some words are unenciphered, providing a bit more context. Can you break it?[14]

Charlottetown, Oct. 7th 1780

Sir,

The state of the lower boundary, and the absolute necessity of preventing the enemy from being in quiet possession of the East bank of the Santee obliges me to change the destination of the 63rd Regiment. I will therefore explain my plan to you and the part you are to bear in it. 19,3,4,10- 1,14,2,44,15,19- 31,60,18- 24,8,22,15,3,42,29,21- 72,29,19,1- 29,61,22,19,70,3- 15,48,22,71,5,2,29,8- 52,6,31,29,35,37- 19,80,71- 22,68,62,6,4- 24,64,29- which from every account I have received 31,18,19,73,74- 29,39,24,14,4,22- 1,18,71,99,22- 18,22,60,32,44,29,26,6- there is great reason to hope may be done 19,91,8,17,74,22,77- 15,1,29,6,2,26,4,22,8,14,55,64- 68,24,71,69,29,19- For this purpose I shall 24,1,17,60,4- 32,50,29- 8,14,1,9,19- 19,44,29- 31,22- 19,13,40,4,35,17,74- 26,68,7,6- 10,80,81- 36,38,35,2,6,14,9,22,7- 8,29,26,18,22,1,24- 19,3,4,29,15,44- 32,29,17,2,19,4- 38,85- 5,1,7,8,45,2,66,19,6,31,18- 19,3,74,70- 29,4,2,21,33,14,71,9,22,42,29,21- 15,1,9,29,19,57,6- 19,91- 22,54,25,8,2,22,90- 19,1,51,49,22- 6,19,8,29,26,38,22,26- to be formed into Provincial Corps and armed, clothed and appointed as soon as we can do it- From 19,3,4,29,15,80,84- 32,24,4,8,29- 19,1,24,71,17,84,24,7- 13,33,31,5,54- 18,41,22,15,4- 26,1,13,70,29- 19,1- 15,22,1,6,60,80,15,22,4,11,90- 8,6,2,19,13,42,5- 19,33,74,29- 14,4,8,14,1,9,19- 19,3,4- 24,2,26,35,34,1,18- 29,51,17,4,24,14,74,22- 2,3,1,25,4- the 5,1,13,4,22,15,41,9,29,19,90,22,37- 13,32,5,14,4- 73,74,48,5,19,3,7- I shall then be in 18,9,5- 15,1,24,9,29,2,15,8,19,32,51,29- 13,2,19,33,1,9,22,6,3,2,25,32,29,21- 8,29,26- 6,33,38,5- 22,4,15,54,42,17,44- 48,35,19,3,4,8,22,24,6- 68,29,26- 15,5,1,19,3,32,29,21-

[14] The original resides in the National Archives, Papers of the Continental Congress, Microcopy No. 247, Roll 65, Frame 4818. It was taken here from Fagone, Peter P., A Message in Cipher Written by General Cornwallis During the Revolutionary War, *Cryptologia*, Vol. 1, No. 4, 1977, pp. 392-395.

19,3,58,19- 15,3,8,22,5,4,66,19,31,13,29- 15,48,60,29- 38,18,41,22,26- I would have you 24,1,9,29,19- 7,51,59,22- 13,3,31,5,4- 22,34,21,2,24,54,29,19- 8,29,26,2,18- 37,31,99- 19,3,2,29,11- 7,41,39,22,6,4,5,19- 19,31,1- 13,4,8,11,19,98,11,4- 24,4,29- 18,22,1,24- 19,9,22,29,14,79,5,35- 26,4,6,2,22,42,29,21- 33,2,34- to detain in 19,3,44,2,22,60- 25,5,8,15,4- 8,6,24,8,29,37- 31,18,1,9,22- convalescents, and proceed into 19,33,70,44- 15,1,9,29,19,22,7- 8,6,66,1,31,29,88,56- 25,51,6,2,14,5,4- I can give you 29,1- 25,8,22,19,2,15,9,5,78,22- 26,42,22,4,15,19,62,71,29,6- 24,60,7- 31,14,32,4,15,19- 72,6,19,1- 20,25,22,44,17,4,29,19- 19,33,44- 4,29,74,24,7- 10,18,22,31,24- 19,3,1,22,71,9,21,33,55,77- 24,8,6,19,54,22,76- 1,18,19,3,54- 15,1,9,29,19,22,60,7- 77,51,99- 73,78,17,4- 35,64,18,19- 57,41,9- 13,2,5,35- 19,3,4,22,74, 18,1,22,94- 8,15,19- 78,15,1,22,26,2,29,21- to your 26,2,6,15,22,4,19,2,1,29- 38,29,26,19,3,44- 2,29,19,4,5,82,21,74,29,15,34- you may 22,4,15,84,52,17,94,60- 4,2,19,344,22- 31,18,74,29,66,42,17,4,5,7- 70,1,22- 26,4,18,34,29,6,32,17,34,35,97- 9,29,19,32,5- 37,1,9- 3,4,8,22- 1,18,24,67- 24,8,22,15,3- 19,71- 15,22,31,6,15,22,4,11- 13,3,44,29- 57,51,59,13,2,5- 32,61,2,29- 24,4- We may correspond by means of cypher- You will please give a copy of the cypher to Turnbull and send another by a safe conveyance to Balfour. Tell Turnbull that I address this letter to you as he is ill, and show him the contents- You will of course take Harrison's Corps, and what Militia you please- You will send a copy of this letter to Balfour, which, you may, I suppose venture without cypher as the only danger is near this place and you will afterwards correspond with him when you think it necessary-

I am
Sir
Your most obedient
Humble Servant
Cornwallis

To Major Win (?)
63rd Regiment
Camdan

Note: line breaks have not been preserved from the original here. An average word length calculation will indicate if nulls are part of this cipher. Fagone has corrected enciphering errors that were present in the original.

Charlottetown, Oct. 7th 1780

Sir,

The state of the lower boundary, and the absolute necessity of preventing the enemy from being in quiet possession of the East bank of the Santee obliges me to change the destination of the 63rd Regiment. I will therefore explain my plan to you and the part you are to bear in it. The object of marching into North Carolina is only to raise men, which from every account I have received of the number of our friends, there is great reason to hope may be done to a very considerable amount. For this purpose I shall move in about ten or twelve days to Salisbury and from thence invite all loyalists of the neighbouring countries to repair to our standard to be formed into Provincial Corps and armed, clothed and appointed as soon as we can do it- From thence, I mean to move my whole force down to Cross Creek. As it will then be about the middle of November, I hope the lower country will be healthy. I shall then be in full communication with our shipping and shall receive all the arms and clothing that Charlestown can afford.I would have you mount your whole regiment and, if you think yourself too weak, take thirty men from Turnbull, desiring him to detain in their place as many of our convalescents, and proceed into the country as soon as possible. I can give you no particular directions. My object is to prevent the enemy from being thoroughly masters of the country you have left. You will therefore act, according to your discretion and the intelligence you may receive, either offensively or defensively until you hear of my march to Cross Creek, when you will join me. We may correspond by means of cypher- You will please give a copy of the cypher to Turnbull and send another by a safe conveyance to Balfour. Tell Turnbull that I address this letter to you as he is ill, and show him the contents- You will of course take Harrison's Corps, and what Militia you please- You will send a copy of this letter to Balfour, which, you may, I suppose venture without cypher as the only danger is near this place and you will afterwards correspond with him when you think it necessary-

I am
Sir
Your most obedient
Humble Servant
Cornwallis

To Major Win (?)
63rd Regiment
Camdan

Chapter 3

1. For the Lewis and Clark Expedition, Thomas Jefferson instructed Lewis to "communicate to us, seasonable at intervals, a copy of your journal, notes and observations, of every kind, putting into cipher whatever might do injury if betrayed." Jefferson had the Vigenère cipher in mind, but it was never used.[15] Pretend that you are the expedition cryptographer and encipher the following message using the key EXPLORE.

```
I discovered immense ranges of high mountains still to the
West of us with their tops partially covered with snow.
```

```
MAXDQ FZIOT OWDQI KHPFR RKBHZ TYMKE BZIEX EFCDG KMPII ZHYIA
BHECW YWTXE VKLIF GECGW TXGEW RPPVR ZJVVI ALTHY WRLL
```

2. Decipher the following message using the key EXPLORE.

```
SKTZT KLITP CFZSV PISSE TYIAP RLTXE TRFRW WFCEV VGIKI PFFJX
ETWCU KICDC AZRKX HXOCP GFGNZ VSJXQ ZIKXA LUPSK MRAXL AVXIO
ISSTL MBUYS OXTOD OITIH EXDDZ TIXCO BRXMS TECSE GZDLB UFIDP
YOCSR DRPFV QSKNZ TKLIM XAS
```

```
One of the warriors then pulled up the grass in the center
of the lodge forming a small circle of about two feet in
diameter the chief next produced his pipe and native tobacco
and began a long ceremony of the pipe.
```

3. Encipher the following message using the key GRAFFIN.

```
I'm a twenty-first century digital boy.
I don't know how to read, but I've got a lot of toys.
```

[15] http://www.loc.gov/exhibits/lewisandclark/preview.html