Volume 25
Number 3

bacus

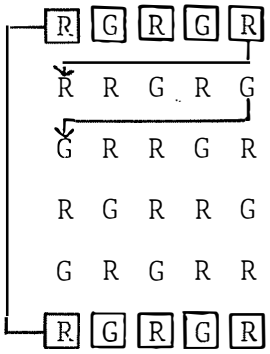
A publication of the O.A.M.E.

February 1987

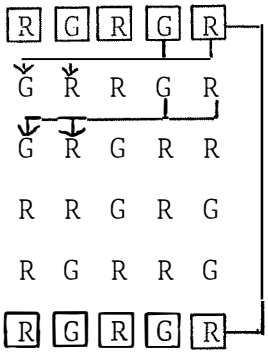
DISCOVERING STRUCTURE THROUGH PATTERNS

Make a pattern from five objects.

Move the objects as shown below.



or



or ...

5 objects

5 moves

5 objects

5 moves

Patterns?

Extensions?

Editor: TREVOR BROWN
TORONTO BOARD OF EDUCATION

Typing: BETTE WITHERS
MATHEMATICS DEPARTMENT
TORONTO BOARD OF EDUCATION

Layout: LEARNXS PRESS

SUBTRACTION PATTERNS

You can use a table like this for subtraction.

-	11	12	13	14	15	16	17	18	19	20
10	1	2	3	4	5	6	7	8	9	10
9	2	3	4	5	6	7	8	9	10	11
8	3	4	5	6	7	8	9	10	11	12
7	4	5	6	7	8	9	10	11	12	13
6	5	6	7	8	9	10	11	12	13	14
5	6	7	8	9	10	11	12	13	14	15
4	7	8	9	10	11	12	13	14	15	16
3	8	9	10	11	12	13	14	15	16	17
2	9	10	11	12	13	14	15	16	17	18
1	10	11	12	13	14	15	16	17	18	19

For example 14 - 8 =

Look down the 14 column till you reach the 8 row.

The number in the square where the 14 column crosses the 8 row is 6, so 14 - 8 = 6.

-	11	12	13	↓ 14
10	1	2	3	4
9	2	3	4	5
→ 8	3	4	5	6

1. Use this table to answer these:

   (a) 14 - 5 (b) 17 - 3 (c) 19 - 5 (d) 20 - 5

   (e) 19 - 5 (f) 12 - 3 (g) 15 - 5 (h) 17 - 7

   Look for patterns in the subtraction table.

2. Even numbers can all be divided by 2 without a remainder

   -2, 4, 6, 8, 10, ...

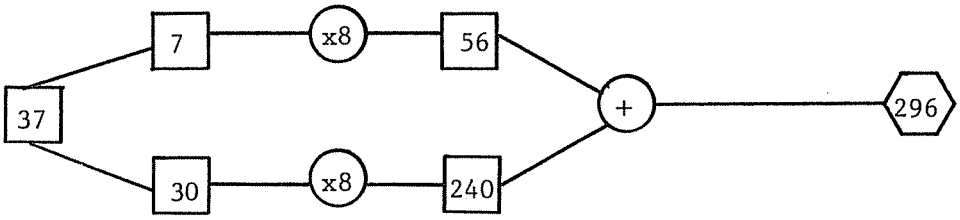
   Odd numbers have a remainder of 1 when divided by 2.

   -3, 5, 7, 9, 11, ...

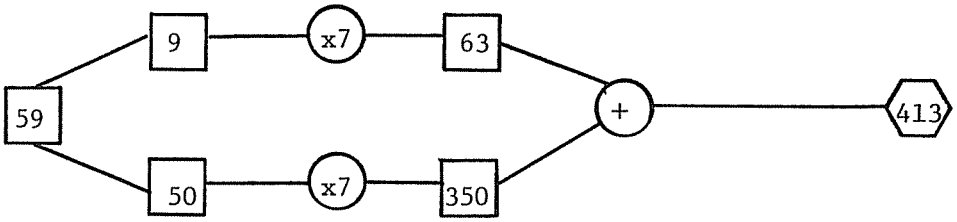
   Where are these numbers seen on the subtraction table?

MULTIPLICATION: FLOW CHARTS

Multiplication can be set out like this: 37 x 8

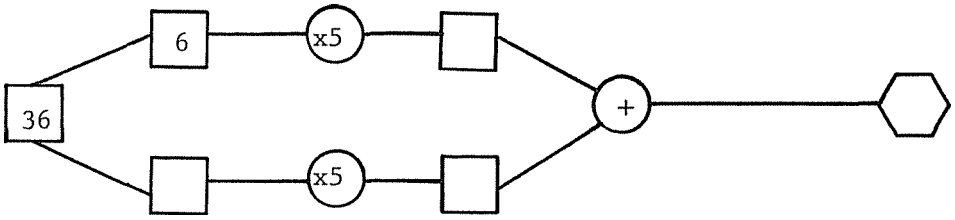


Here is another example: 59 x 7

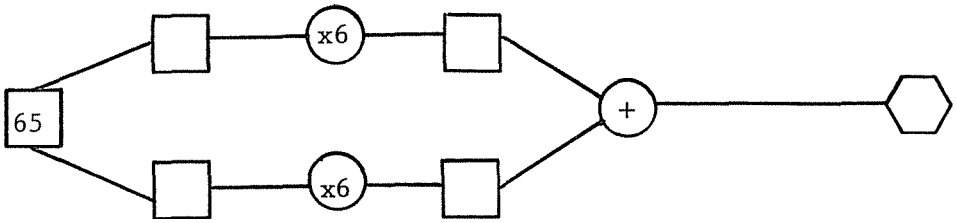


1. Copy and complete these diagrams:

(a) 36 x 5



(b) 65 x 6



2. Do these in the same way, drawing your own diagram for each.

(a) 84 x 8 (b) 97 x 6 (c) 88 x 8 (d) 90 x 5

WHAT DAY OF THE WEEK WAS IT?

Assign these numbers to the months.

January	1	April	0	July	0	October	1
February	4	May	2	August	3	November	4
March	4	June	5	September	6	December	6

(On leap years, use 0 for January and 3 for February.)

To figure a day:

1. Choose a day in the twentieth century.
2. Write down the last 2 figures of the year in which it occurred.
3. Divide this number by 4 and disregard remainders.
4. Find the key number for the month. Record it.
5. Write the day of the month.
6. Add the numbers in 2, 3, 4, and 5 above.
7. Divide the sum by 7.
8. Use the key below to find what day of the week it fell on.

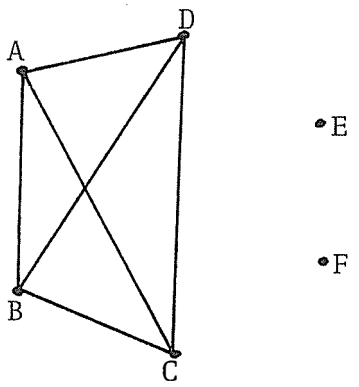
KEY: 1 - Sunday
2 - Monday
3 - Tuesday
4 - Wednesday
5 - Thursday
6 - Friday
0 - Saturday

All dates before the last day of 2100 and after September 15, 1752 may be computed. For those not in the 20th century, however, an adjustment must be made after step 6. For years in the 1700's add the number 4, for the 1800's add 2, for the 2000's add 6, for the 2100's add 4.

VERTICES AND EDGES

For the points A, B, C, and D there are six line segments which have these points as endpoints.

(a) Draw line segments from E to A, B, C, and D. How many new line segments are there? What is the total number of line segments for these five points?



(b) How many more line segments will there be if point F is used? What is the total number of line segments having six points as endpoints?

(c) Find a pattern and complete the table to show the number of line segments which have the given numbers of points as endpoints.

Number of points	2	3	4	5	6	7	8	9	10	20
Number of segments										

(d) You probably recognize the numbers 1, 3, 6, etc., as being the triangular numbers.

The nth triangular number is $n(n+1)/2$.

Use this formula to find the 98th triangular number.

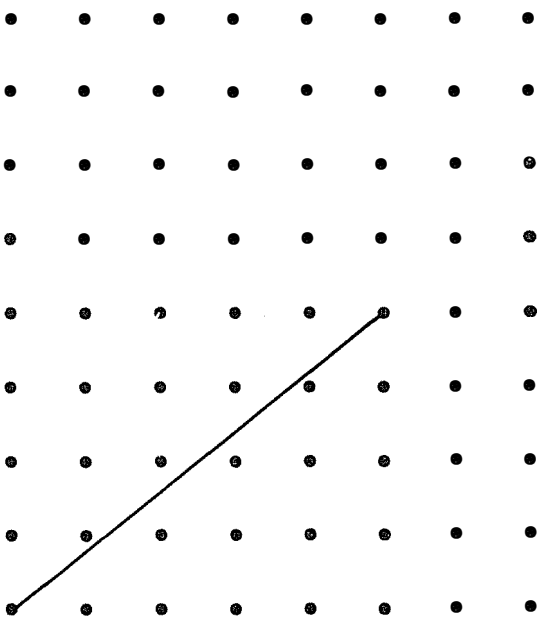
(e) In 1884 Ezra T. Gilliland devised a mechanical system that would allow 15 subscribers to reach each other without the aid of an operator. How many line segments are needed to connect 15 points? (105)

(f) In 1891 Almon B. Strowger patented a dial machine which connected up to 99 subscribers. How many different two party calls does this permit? (4851)

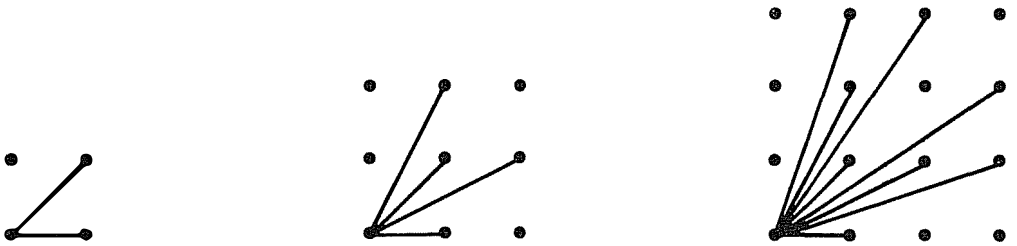
SLOPES ON GEOBOARDS

1. A rectangular geoboard has rows and columns of pegs. Line segments can be formed by stretching rubber bands between the pegs. The line segment on the geoboard has a run of 5 and a rise of 4. Its slope is 4/5.

   How many line segments with different non-negative slopes can be formed on this geoboard?



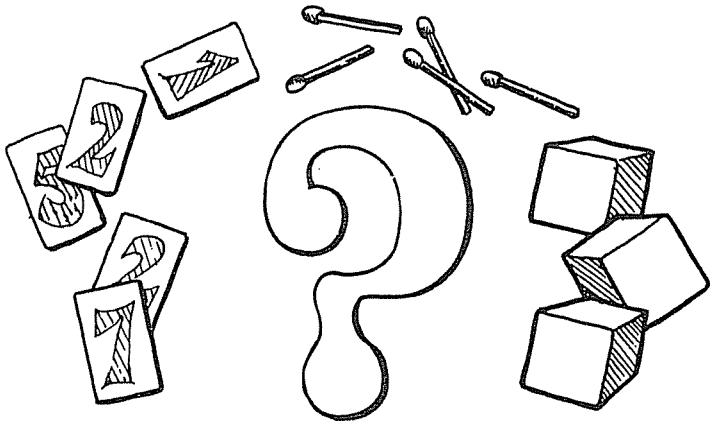
2. For any size geoboard the number of line segments with different non-negative slopes is even. Here are examples of the first three geoboards. Explain why the number is always even.



INVESTIGATIONS: HOW MANY?

In the following questions, particular numbers and other details are given, but these are mostly arbitrary and the investigations should extend to other cases. Where a question is ambiguous it is probably worth exploring the alternative interpretations.

- A classroom has four electric light switches. How many different ways may lights be put on?
- A set of five cards is made, each with one digit written on it. The digits used are 1, 2, 2, 5, 7. How many different numbers can be shown with the set of cards?
- How many ways can a cube be painted with two colours?
- Using only whole numbers and addition, write as many different expressions for the number 5 as possible.
- On a geoboard make as many different shapes with an area of 2 cm^2 as possible.
- Make a connected network (it need not be closed) with five matches. How many different networks are possible?
- Make a row of four different objects. How many different orders of the objects are possible?
- How many odd numbers are there smaller than 100, say, without the numeral 3 occurring in them?



CODES, CIPHERS AND CRYPTOGRAMS

John Scott, Mathematics Consultant, Ward 10

Statistics as taught in grades 9 and 10 can help with the "cracking" of certain kinds of ciphers or cryptograms. A cipher is defined, for our purposes, to be any system designed and intended to conceal the true meaning of any message. A code may conceal meaning from some but is not specifically intended for that purpose. For example, Morse Code is a mystery to some people but others can read it very well. Ciphers have been used to conceal messages from enemies since at least the time of Julius Caesar. This workshop examines the solving of certain types of ciphers using statistics as a starting point and links "codebreaking" to History.

Assumptions

When this material is presented to students, it is assumed that they have done a unit of statistics which includes a discussion of frequency tables or distributions, means, modes and data collection.

ENCIPHERING SYSTEMS

The methods used to encipher messages are as varied as one's imagination. They range from the simple replacement of any letter in a message by the letter of the alphabet which occurs a fixed distance away, to the incredibly complicated machine systems of the Second World War to the computerized systems likely in use today.

In this workshop we concentrate on the solution of substitution systems in which a given letter is always replaced by the same other letter. However, we first look at some other methods of enciphering which have been used over the years.

1. Transpositions

A transposition cipher is one in which the letters of the message are rearranged or transposed in order to conceal the true meaning of the message. Of course there are many ways in which to rearrange or transpose a message to conceal its meaning. Obviously, the number of possibilities goes up with the number of letters in the message.

For example, suppose we wished to send the message

MEET ME AT SIX BEHIND X OPERA X

(The two X's are nulls to make a "nice" number of characters, 24)

We then write the message into a 6 by 4 grid going down the

columns one at a time from the upper left. The message is then read out going across the rows and we end up with

MAEO ETHP ESIE TINR MXDA EBXX

as our message. This method has the advantage that enciphering and deciphering are both relatively easy tasks. The size of the message and the way in which the letters are written onto the grid play important roles in deciphering such messages.

2. The ADFGX Cipher

This is an example of a relatively simple system which is much more secure than the transpositions above, but very clever. It was invented by German Cryptographers during World War One. In this cipher the letters of the alphabet are written into a 5 by 5 matrix in some order and the letters A, D, F, G, and X are written at the top of each column and to the left of each row. To make 26 letters fit into the 25 slots in the grid I and J were taken to be equivalent.

	A	D	F	G	X
A	A	F	L	Q	V
D	B	G	M	R	W
F	C	H	N	S	X
G	D	I	O	T	Y
X	E	K	P	U	Z

To encipher a messaage, each plaintext letter is replaced by the letters at the left of its row and the top of its column, in that order. For the matrix above the message SEND HELP would be encoded as follows:

S	E	N	D	H	E	L	P
FG	XA	FF	GA	FD	XA	AF	XF

While this system as the disadvantage that the size of every message is doubled, it has the advantage that each of the letters A, D, F, G and X is a very distinctive sound in Morse Code which minimizes sending errors.

3. Concealment Ciphers

There are many ways to conceal a message so that it is part of some "cover". The letters of a secret message may be indicated in a newspaper clipping by the use of invisible ink (lemon juice works well, reappearing with the application of heat) or pin pricks in the paper. A "cover story" may be written and the secret message indicated by the first or any other letters of the words in the story.

4.Polyalphabetic Cipher Systems

Much History is to be learned by delving into the solution of the German and Japanese cipher systems during the Second World War. Briefly, these systems involved polylalphabetic substitutions which were done mechanically by a system of wheels and gears in a "black box" connecting two identical typewriters. At the beginning of each day the wheels were set to some predetermined position which set the substitutions for the day. A code clerk with a message to encode, sat down at one of the typewriters and typed the *plaintext*. The *ciphertext* appeared on the other typewriter automatically. When an enciphered message was received, the code clerk typed the *ciphertext* and the *plaintext* appeared on the other machine!

In Britain, a group of Mathematicians working with Alan Turing figured out how the coding was done and constructed their own "black box" to decode the messages of the German High Command. At the same time and working independently, an American group led by the William F. Friedman accomplished the same task for the Japanese code machine which had been adapted from a German model. The opening chapter of David Kahn's The Codebreakers details the American achievements.

Systems such as these are far beyond the grasp of most of us. However, there is no reason why they cannot be discussed in the light of the mathematical achievements of the solvers and the moral dilemmas faced by Winston Churchill and others in the use of information obtained from enemy ciphers.

STATISTICS AND SUBSTITUTION CIPHERS

The simplest of the substitution ciphers is the Caesar Cipher which originated in the time of Julius Caesar nearly two thousand years ago. This is a substitution cipher which simply shifts the letters up or down the alphabet a constant amount. For example, if we take the plaintext word CRYPTOGRAMS and shift every letter down one, we get the ciphertext word DSZQUPHSBNT. A different shift would give a different result. These are not difficult to break. Once it is determined that we have a Caesar Cipher, we simply write the alphabet below each character starting at each ciphertext letter. Eventually the solution becomes apparent. At most twenty-six letters must be written in each column. Caesar Ciphers can be made more difficult to solve by writing the figures of the date above each letter of the plaintext repeated as often as necessary and then using the digit above each letter as the shift.

Other substitution ciphers involve random, but constant replacements; some use a key word to determine the replacements for the first few letters of the alphabet and others simply reverse the alphabet using A for Z, B for Y, etc. Yet no substitution cipher is particularly difficult to break, provided that we know some statistical facts about the language in which

the original message was written and that the message uses the language in a "normal" fashion. We shall stick to English although the same methods can be used for any language if similar characteristics are known.

The facts below relate to "normal" English and are taken from the Gardner book cited in the bibliography, but could have come from just about any book on Cryptography. However, they can almost all be verified by students. The labourious method would be to give each student a page of prose on which to count and then record the letter frequencies. A class average for the percentages of each letter is a good calculation exercise. A better way would be to have a student (the class "hacker") write a computer program to do the job. That way a much larger sample could be counted with much less labour! The input to the program could well be word processor files which the students have already composed. The percentage frequencies may differ slightly from the accepted values, but the order of the letters ought to stay about the same.

Some Facts About the English Language

1. E is the most common letter followed in order of frequency by T, A, O, N, I, R, S and H. E is also the most common letter in German, French, Italian and Spanish, but in Russian the most common letter is O.

2. The most common final letter of a word is E.

3. The most common initial letter is T.

4. A single-letter word is almost always A or I.

5. The most frequent two-letter word is OF followed by TO and IN.

6. The most frequent three-letter word is THE. The word AND is the second most frequent.

7. Q is always followed by U.

8. N is the most common letter to follow a vowel.

9. The most common double letters are LL, EE, SS, OO, TT, FF, RR, NN, PP, and CC (in order).

10. The most common four-letter word is THAT. (THAT is also a pattern word with the first and last letters the same.)

Let's look at the solution of a substitution cipher in which the word divisions have been preserved. (The word divisions provide valuable clues to the solution!)

Historical fact:

VZB MXCVBT AVNVBA AHDKBT VZB GNCX LHTD HJ VZB FNYNXBAB XNKS CX VZB ABLHXT PHEDT PNE. VZCA YUDNSBT NX CGYHEVNXV EHDB CX VZB NGBECLNX KCLVHES NV VZB TBLCACKB WNVVDB HJ GCTPNS.

To get started on the solution we copy the cipher onto squared paper, writing on at most every third line. Then we tally the characters to make the frequency table which is shown below.

A	7	N	14
B	19	O	0
C	11	P	3
D	5	Q	0
E	6	R	0
F	1	S	4
G	4	T	8
H	9	U	0
I	0	V	16
J	2	W	1
K	4	X	10
L	5	Y	3
M	1	Z	7

TOTAL 140 Letters

When we examine the table of frequencies carefully, we see that the cipher letter B is the1 most frequent. In addition, the ciphertext word VZB occurs five times. Taken together with the information above about most frequent letters and most common three-letter words is is worth a guess that VZB represents THE. If we go through and fill in these guesses we get the following:

```
VZB MXCVBT AVNVBA AHDKBT VZB GNCX LHTB HJ VZB FNYNXBAB
THE    TE   T TE      E  THE         E    THE      E E

XNKS  CX  VZB  ABLHXT  PHEDT  PNE.   VZCA  YDNSBT  NX
          THE  'E                     TH       E

CGYHEVNXV EHDB CX VZB NGBECLNX KCLVHES NV VZB TBLCACKB
     T  T    E    THE   E         T     T THE  E     E

WNVVDB HJ GCTPNS.
  TT E
```

The next most common letters in the message are N at 14 and C at 11. Since A and O, at almost equal frequency, have yet to be even tentatively identified in the cipher let's try on or the other of them. In the ciphertext word NV, we have tentatively decided that V is plaintext T. Thus NV could be AT or perhaps IT. We need to try one of them to work towards a solution. If we were to try N as I we would come up with the unlikely sequence of IT THE in the last line. Let's try N as A and see what we get:

```
VZB MXCVBT AVNVBA AHDKBT VZB GNCX LHTB HJ VZB FNYNXBAB
THE    TE   TATE      E  THE  A      E    THE  A A E E

XNKS  CX  VZB  ABLHXT  PHEDT  PNE.   VZCA  YDNSBT  NX
 A        THE   E              A     TH      A E   A

CGYHEVNXV EHDB CX VZB NGBECLNX KCLVHES NV VZB TBLCACKB
     TA T    E    THE A E   A     T    AT THE  E     E

WNVVDB HJ GCTPNS.
 ATT E        A
```

Now we can start looking for complete words to fill in and get more of the solution. The first possibility is in the third word of the message. The letter S here would make the word STATES in the plaintext:

```
VZB MXCVBT AVNVBA AHDKBT VZB GNCX LHTB HJ VZB FNYNXBAB
THE    TE  STATES S   E  THE  A      E    THE  A A ESE

XNKS  CX  VZB  ABLHXT  PHEDT  PNE.   VZCA  YDNSBT  NX
 A        THE  SE              A     TH S    A E   A

CGYHEVNXV EHDB CX VZB NGBECLNX KCLVHES NV VZB TBLCACKB
     TA T    E    THE A E   A     T    AT THE  E  S  E

WNVVDB HJ GCTPNS.
 ATT E        A
```

At this point we have identified only two of the vowels A and E. Looking for another vowel, it is a reasonable guess that C is one of them, and it is likely to be I from looking at the first word of the second sentence of the message.

```
VZB MXCVBT AVNVBA AHDKBT VZB GNCX LHTB HJ VZB FNYNXBAB
THE   ITE  STATES S   E  THE  AI     E    THE  A A ESE

XNKS  CX  VZB  ABLHXT  PHEDT  PNE.   VZCA  YDNSBT  NX
 A    I   THE  SE              A     THIS    A E   A

CGYHEVNXV EHDB CX VZB NGBECLNX KCLVHES NV VZB TBLCACKB
I    TA T    E I  THE A E I A   I T    AT THE  E ISI E

WNVVDB HJ GCTPNS.
 ATT E     I  A
```

Further guesses start to come very quickly at this stage since so much of the message is evident. Whole words seem to jump out at us. Guessing that the word before STATES is UNITED gives us the following:

```
VZB MXCVBT AVNVBA AHDKBT VZB GNCX LHTB HJ VZB FNYNXBAB
THE UNITED STATES S   ED THE  AIN   DE    THE  A ANESE

XNKS  CX  VZB  ABLHXT  PHEDT  PNE.   VZCA  YDNSBT  NX
NA    IN  THE  SE  ND      D   A     THIS    A ED  AN

CGYHEVNXV EHDB CX VZB NGBECLNX KCLVHES NV VZB TBLCACKB
I    TANT    E IN THE A E I AN  I T    AT THE  E ISI E

WNVVDB HJ GCTPNS.
 ATT E     I  A
```

Further intuition tells us that .A.PANESE is almost certainly JAPANESE and that HJ is likely OF:

```
VZB MXCVBT AVNVBA AHDKBT VZB GNCX LHTB HJ VZB FNYNXBAB
THE UNITED STATES SO  ED THE  AIN  ODE OF THE JAPANESE

XNKS  CX  VZB  ABLHXT  PHEDT  PNE.   VZCA  YDNSBT  NX
NA    IN  THE  SE OND   O  D   A     THIS    A ED  AN

CGYHEVNXV EHDB CX VZB NGBECLNX KCLVHES NV VZB TBLCACKB
I  O TANT  O E IN THE A E I AN  I TO   AT THE  E ISI E

WNVVDB HJ GCTPNS.
 ATT E OF  I  A
```

Now the complete solution flows out very quickly and easily.

```
VZB MXCVBT AVNVBA AHDKBT VZB GNCX LHTB HJ VZB FNYNXBAB
THE UNITED STATES SOLVED THE MAIN CODE OF THE JAPANESE

XNKS  CX  VZB  ABLHXT  PHEDT  PNE.   VZCA  YDNSBT  NX
NAVY  IN  THE  SECOND  WORLD  WAR.   THIS  PLAYED  AN

CGYHEVNXV EHDB CX VZB NGBECLNX KCLVHES NV VZB TBLCACKB
IMPORTANT ROLE IN THE AMERICAN VICTORY AT THE DECISIVE

WNVVDB HJ GCTPNS.
BATTLE OF MIDWAY.
```

The reader should note that not all cryptograms solve this easily! This particular message is a bit contrived to show the method. When one finds a cryptogram in the newspaper or in a puzzle both the letter frequencies are not likely to follow the table exactly. However, the frequency table will still provide clue and with a bit of "guess and check" most simple substitution ciphers can be solved with relative ease.

CRYPTOGRAMS TO SOLVE

The methods used above can be applied to any substitution cipher. It is always useful to have such clues as the word divisions, punctuation and some knowledge of the origins of the piece. The usefulness of guesses is not to be underestimated. I suggest the use of squared paper, writing the ciphertext at least triple spaced and using pencil only so that if you end up in a "blind alley" erasing is easy.

Each of the following is a simple (monoalphabetic) substitution cipher in which each ciphertext letter always stands for the same plaintext letter. Word divisions are shown and a "title" which provides some (oblique) clue is given. Good luck.

1. Restaurant patron to waiter:
   UX IRUX ISL PD VPMMSS? UI ILXISX SOLVING NUTS TSDPXSAS.
   Waiter:
   IRSA UI ZEXI JS ISL XUD. PED VPMMSS ILXISX NUTS IEDCSAIUAS.

2. Beggar to man he has accosted in the street:
   MOJ BVXZL NVX ZGRL MVFG FVRGN AV WR XRTVJAXRWAG TGZZVB
   BPV'M VXA VT BVJH? WZZ O PWKG OR APG BVJZL OM APOM ZVWLGL IXR.

3. Flight Plan:
   SPRHWY MPOFYB PS DS PZZHWY IDEE: HF HO LDXB FP
   OPDX IHFL YDAEYO ILYS QPK LDGY FP IPXR IHFL FKXRYQO.

4. Patient on couch to Psychiatrist:
   ETQ ISH FR XW QTOUSFOU? WFG XGUQ AT MSHHSOE: S LFGJHO'Q HF
   QVZQ -- QVTW ZIT ZJJ QVZQ SU VFJHSOE XT QFETQVTI.

5. Applied Baseball:
   CH YTVAYTOO SOTNADV UTK MTJA SCKUM MCWWADV, QMN UTK'W
   AJADNBKA? WMAK ATUM BH LV UBLOI IB ZLVW QMTW QA AKZBN
   TKI IB DATOON QAOO?

6. Quote from well known playwrite:
   ZUHOU DCUZZ UHOZS GZAEZ SOJKO EZAUC

(In the last cipher, the word divisions have been concealed to increase the challenge.)

BIBLILOGRAPHY

David Kahn, THE CODEBREAKERS, Macmillan, 1967. This is the definitive treatise on the subject. The unabridged version is long very mathematical, but very absorbing.

Norma Gleason, CRYPTOGRAMS AND SPYGRAMS, Dover, 1982. The author often contributes to the cryptogram page in GAMES Magazine.

Martin Gardner, CODES, CIPHERS AND SECRET WRITING, Simon and Schuster, 1972. The former "Mathematical Games" writer for SCIENTIFIC AMERICAN has put together a very good little book on the subject of cryptography.

Helen F. Gaines, CRYPTANALYSIS, Dover, 1956. Originally published in 1939, this book was used as a text to train codebreakers.

Laurence D. Smith, CRYPTOGRAPHY, THE SCIENCE OF SECRET WRITING, Dover, 1955. This is a simple and concise explanation of how to solve the various types of cryptograms. Many examples are included.