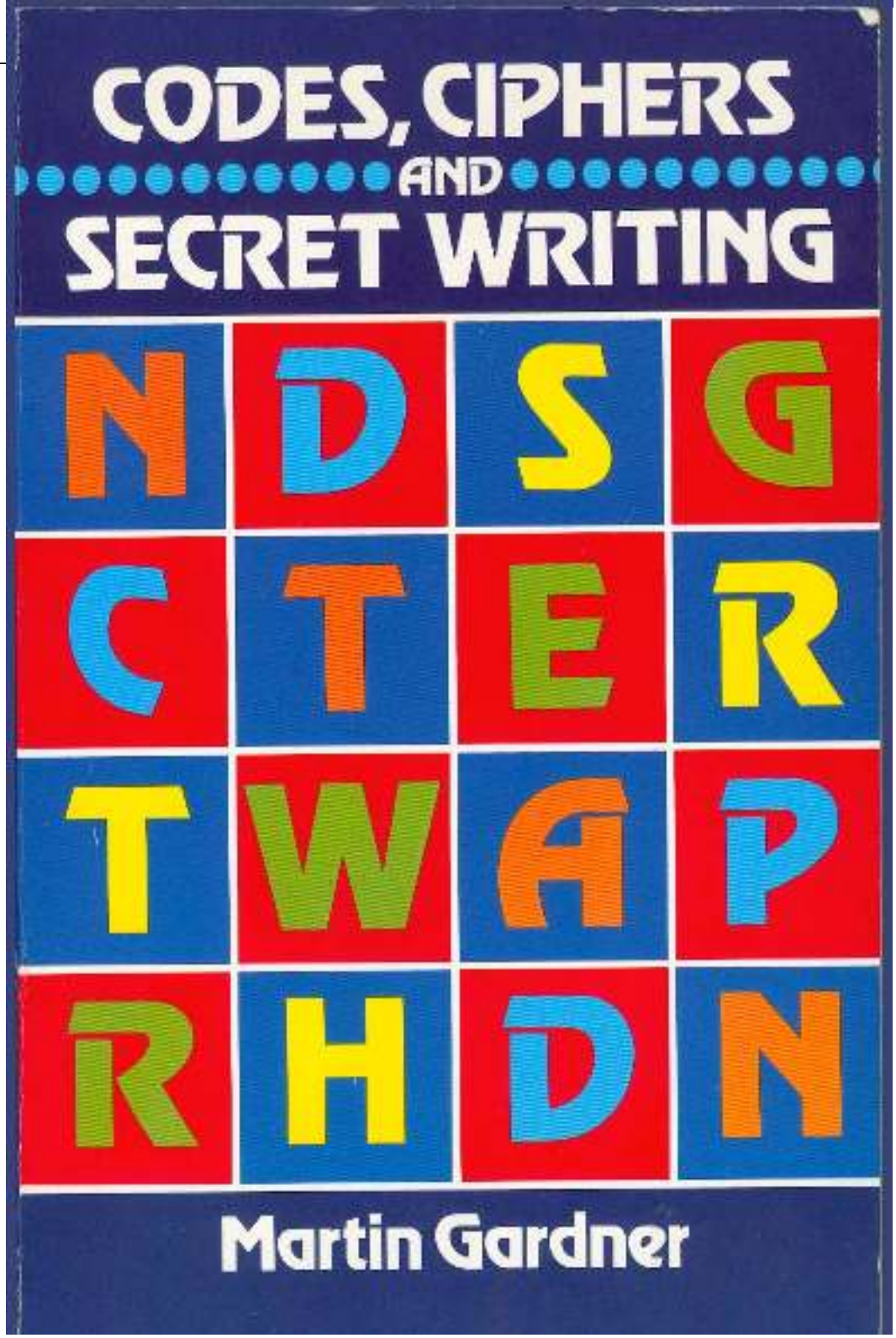
www.GetPedia.com

* More than 500,000 Interesting Articles waiting for you .
* The Ebook starts from the next page : Enjoy !

* Say hello to my cat "Meme"


CODES, CIPHERS
AND
SECRET WRITING
N D S G
C T E R
T W A P
R H D N
Martin Gardner

For

CHRIS ZYNC KING

Published in Canada by General Publishing Company, Ltd., 30 Lesmill Road, Don Mills, Toronto, Ontario.
Published in the United Kingdom by Constable and Company Ltd.

This Dover edition, first published in 1984, is an unabridged and corrected republication of the work first published by Simon & Schuster, Inc., New York, in 1975.

Manufactured in the United States of America.
Dover Publications, Inc., 31 East 2nd Street, Mineola, N.Y. 11501

Library of Congress Cataloging in Publication Data

Gardner, Martin, 1914-
Codes, ciphers, and secret writing.

Reprint. Originally published: New York : Simon & Schuster, c1972.
Bibliography: p.
1. Cryptography. 2. Ciphers. I. Title.
[Z103.G3 1984] 652'.8'03 84-9024
ISBN 0-486-24761-2

Content

Introduction

1 Easy Transpo
The Rail Fen
Scrambling

2 Easy Substitut
Shift Ciphers
Ciphers with
Checkerboard
The Shadow's

3 How to Break

4 Hard-to-break
Poe's Dipsy
Lewis Carroll

5 Simple Code
Typewriter C

Scytale • The Alberti Disk • Thomas Jefferson's Wheel Cipher • Grilles • The Triangle Code

6 Invisible Writing 71

Inks That Develop When Heated • An Ink That Turns Red • Inks That Glow in Blacklight • Inks That Appear When Powdered • Writing That Becomes Visible When the Sheet Is Wet • Writing That Can Be Seen in Slanting Light • Typing That Can Be Seen in Raking Light

7 Bizarre Methods of Message Sending 78

The Dot Code • The Knot Code • The Playing Card Code • The Red Blue Code • The Crayon Cover • The Cheese Code • The Swizzle Stick Code

8 Codes for Other Worlds 87

References for Further Reading 94

Historical • Methods • Codebreaking • Cipher Cranks • Interplanetary Communication

Introdu

Cryptography, the
secret code, and o
played, and still pl
nation. It is necess
rocess and spies to
It is just as necessa
expert cryptanalyst
computers at their
countries. The histo
David Kahn in his
is a fascinating one.
fates of empires an
failure of a small g
kind of puzzle solvi

I say "small" bu
often done by only
men. Today, codeb
fession. No one kn
gaged in codebreak
number in the hun

dollars a year. During World War II, 80,000 persons in Great Britain alone were assigned to such work. It is probably one government's most reliable method of gathering intelligence.

The United States Navy's great victory at Midway Island in 1942 was a direct consequence of our having learned the source of Japan's PURPLE machine code, a remarkable feat of codebreaking that will be described in Chapter 5. In the same war Germany's 1943 U-boat victories against Allied shipping were the result of Germany having broken the British merchant ship code. The tide did not turn until American and British cryptanalysts solved the cipher that was being used by German submarines.

The most sensational solution of a single coded message in recent history occurred during World War I. In 1917 Arthur Zimmermann, the German foreign minister, sent a cable to Mexico, using a diplomatic code called 0075. It announced Germany's plan to begin unrestricted submarine warfare. If America entered the war, the cable continued, Germany promised to give Mexico the states of Arizona, Texas and New Mexico if Mexico would only join in fighting against the United States. The cable was intercepted and the code broken by British intelligence, then passed on to President Woodrow Wilson.

America had been reluctant to enter the war. But news about the Zimmermann telegram so enraged Congress and the public that we declared war on Germany. Had we not done so, it is probable that Germany would have won the war. "Never before or since," writes Kahn, "has so much turned upon the solution of a secret message."

Interest in cryptography is not restricted to governments and professional spies. Everybody enjoys a secret. Surely that is one reason why so many young people like to send and receive coded messages even when there is no special reason for them to be secret. Coded messages are fun to encipher (put in cipher form) and decipher (translate back to the original), and

Easy Transpo Ciphers

A transposition cip
of the original mes
"plaintext" but w
merely rearranges t
that anyone who k
in their proper ord

The simplest tra
the message backw
comes YAW SIH
pears to be a palin
both directions—th
when reversed. To
'TIS IVAN ON A
ever, with any ger

The main troub
easy to recognize.
reverse the letters
but harder to spot,
ciphers are better

[1] The Rail Fence Cipher

Suppose you wish to encipher this message:

MEET ME TONIGHT

Count the number of letters. If the number is a multiple of 4, well and good. If not, add enough dummy letters at the end to make the number a multiple of 4. In this case there are 13 letters so we add three dummy letters, QXZ, to total 16. Such dummy letters are called "nulls." In a moment we will see why the nulls are added.

Write the message by printing every other letter a little lower on the page. The message will look something like a rail fence:

M E M T N G T X E T E C I H Q Z

Copy the top row, then continue by copying the lower row.

M E M T N G T X E T E C I H Q Z

Encoding and decoding is simpler and more accurate if you divide the cipher text into groups of four or five letters each, because it is easy to keep that many letters in your head when you write. Besides, this makes the cipher harder to "crack" by the "enemy" because the divisions between the words are not indicated. In this book we will use a 4-group system. That was why three nulls were added in the preceding message. By increasing the number of letters to 16, we make sure that the last group of letters in the cipher text will have four letters like all the other groups.

This is how the final cipher text will appear:

MEMT NGTX ETEC IHQZ

PRACTICE RIDDLE 1

What goes "Tee, he, he, he, ho, ple!"?

AALD HNHS EEFY MNAO IGTH AOEX

(This is a two-row, rail fence cipher. Read from left to right.)

[2] The Twisted Path Cipher

This is an elaboration of the letter-scrambling technique of the rail fence cipher. It uses a rectangular grid, or "matrix" as we will call it, which is simply a checkerboard of empty squares, or cells. Let's take a slightly longer sample message than the previous one:

MEET ME THURSDAY NIGHT

The message has 19 letters. As before, we add enough nulls (i.e. this case only one is needed) to make a multiple of 4. For the 20 letters it will be convenient to use a 4-by-5 matrix. The message, with a null X at the end, is written in the 20 cells, from left to right, taking the rows from top to bottom:

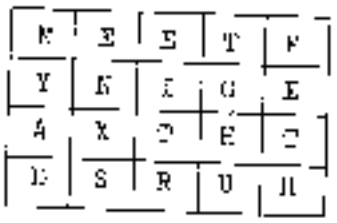
M	E	E	T	M
E	T	H	U	R
S	D	A	Y	N
I	G	H	T	X

The next step is to trace on the matrix a particular path, the shape of which is agreed upon in advance by everyone who will be using the code. It is not a good idea to start the path by moving horizontally along the top row, left to right, because your cipher text would start with MEET, which would be recognized as a word and provide a clue to your system. A good path, called a "plow path" because farmers use this pattern to plow their fields, is shown on the next page.

If you want to make this code even harder to break, you can combine two different paths. For example: Write the message in the matrix along a plow path instead of left to right by rows. Then encode it by taking the letters along a spiral path. To decode, write the letters of the cipher text along the spiral path, then read them along the plow path.

Of course you and whoever receives the code must agree beforehand on the exact method to be used, as well as on the dimensions of the matrix. If you wish to vary the size and shape of the matrix with each message, you can put one number at the beginning of the cipher to indicate the height of the matrix, and another number at the end to indicate its width. This might, however, tip off the enemy that you are using a matrix to scramble the letters. You could use a secret ink (see Chapter 6) to put 4–5 in a corner of the sheet, or to put dots over the fourth and fifth letters of the message, or some other system of your own invention.

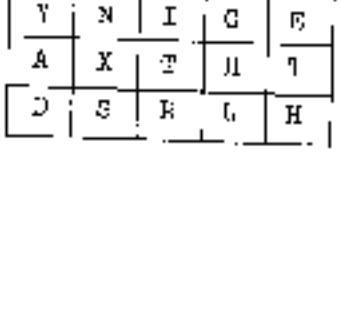
Paths do not have to be continuous. You can take the columns in order, from right to left, starting each column at the bottom, for example, and moving upward. Diagonals can also be used for paths, either broken or continuous. You can go up each diagonal from left to right:



We now wish to scramble the order of the columns. To do this, we could simply number the columns from 1 to 5, but mix up the digits. Our key number would be, say, 25143. Numbers, however, are not easy to remember, and that is where the key word comes in.

Any five-letter word, with no two letters alike, can serve as the key. Let's use the name FRANK. If we number these letters in the order in which they appear in the alphabet, A will be 1, F will be 2, K will be 3, N will be 4, and R will be 5.

In this simple way, FRANK produces the five-digit number 25143. Write the five digits above the columns of the matrix:



PRACTICE RIDDLE 3

What is gray and has four legs, a tail, and a trunk?

NDZG UEPT AANO CRZN SBGC

(This uses the matrix and the procedure just described, except the key word is JANET.)

Easy Substitu Ciphers

In the ciphers disc
of a message remai
of the letters is cha
letters stays the sar
perhaps some kind
substitution ciphers
letter of the messa
can be combined i
comes overly comp
encoding and deco
way, restrict the wo
words or phrases a
special codebook.
common practice o

Most of the fol
"monoalphabetic."
every letter, one an
If the code letter fo
cipher text it mean
mean T.

There is a big advantage in having a method of substitution that is easy to remember. If you and your friends have to carry around a complete alphabet key, someone might find it and steal it. He could then read all your coded messages. This has actually happened many times in history. A spy will manage to steal an alphabet key or make a copy of it. The secret cipher becomes, of course, totally worthless. But if the cipher system is kept only in your head, no one can steal it.

One of the simplest and oldest substitution ciphers is created by writing the alphabet forward, then underneath, the alphabet is written backward:

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

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

Each letter stands for the letter directly below (or above) it. A message such as MYRTLE HAS BIG FEET would be written:

NBIGVO SZH YRT UVVG

or, if you group the letters in quadruplets,

NBIG VOSZ HYRT UVVG

Note how the word "big" reappears near the beginning of the cipher text. It is just a coincidence, but amusing coincidences of this sort are very common in cipher writing. Sometimes they cause a lot of trouble for cryptanalysts because they are taken as clues. Of course they only lead the analysts off into false trails.

Another simple method is to number the letters of the alphabet forward (A = 1, B = 2, C = 3, and so on) or number them backward (A = 26, B = 25, C = 24, and so on). The numbers are used instead of letters. Dashes should go between the numbers to distinguish one-digit numbers from two-digit numbers.

Both these methods—the backward alphabet and the num-

bers in sequence—a
that your enemy is
minute or two to b
lution method was
much superior.

[1] Shift

These are often
Roman emperor Ju
ment messages. Th

A key number, k
which can be varie
shift a second alph
one. Suppose the k
now. Put your pen
the right, starting
Continue to the rig
go back to the beg
cipher will look lik

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

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

To encode a mes
stitute for it the
MYRTLE shifts f
To decode, find th
letter above it.

Needless to add
alphabet keys, yo
after you have enc
someone might fin
learn the secret of

Occasionally a w
word when it is sh

Try encoding it in a 5 shift cipher and you'll be surprised by what you get. What happens to PECAN in a 4–shift cipher? To SLEEP in a 9–shift? Try them and find out! It's fun to look for words that become other words in a shift cipher. Of course, the longer a word the less likely that a letter shift will produce another word. One of the longest of such words in English is ABJURER. In a 13–shift cipher it becomes NOWHERE.

PRACTICE: MIDDLE 4

What did Mr. MacGregor buy a roll of Scotch Tape for?

87207 23AGF

What did he *want* it for?

GRA FEA35

(This is a 13 shift cipher.)

[2] Date Shift Ciphers

To make a shift cipher harder to break, you can vary the amount of the shift from letter to letter. There are many ways to do this. One clever way is to use the date on which you send the message as your key.

For example, assume you wish to send a message on October 21, 1973. October is the tenth month of the year. The date can be written: 10 21 73. Eliminate the dashes and you have the number 102173. Write this number repeatedly over the message:

102173	102	173	1021
XYELE	HAS	BIG	FEET

To encode the message, shift X forward one letter. It becomes Y. (When the shift numbers are small, it is easy to learn how to make all the shifts in your head without having

[3] Key Word Ciphers

Here is a simple way to construct a substitution cipher alphabet by using a key word or phrase. Suppose you and your pals agree that the week's key word is JUPITER. Write the alphabet in a row. Underneath, write JUPITER, followed by all the *other* letters in alphabetical order:

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

Key words are easy to remember, and each word automatically produces a different substitution cipher. The procedures for encoding and decoding are the same as those of the previous ciphers in this chapter.

Note that V, W, X, Y, and Z are unchanged by this cipher alphabet. That is because JUPITER does not contain a letter which appears in the alphabet beyond U. If you use a key word that contains Y, it will change all the letters except Z. Of course your key word must not have duplicate letters.

If a key word is changed from week to week, sometimes it is not easy for everyone to get together to agree on the next key word. One way to avoid this is by using a book or a magazine to provide key words. If it is a book, everyone using the cipher must own or have easy access to a copy. If it is a magazine, pick a popular magazine, easily obtainable, and always use the issue currently on sale.

Select a good key word that appears somewhere in the book or magazine. Then write down the page number, the number of the line from the top of the page, and the number of the word in the line. These three numbers, separated by dashes, can be put at the end of your cipher text to let the receiver know how to find the key word in the book or magazine. If he sees 205 17–8 he turns to page 205, counts to the seventeenth line, and notes the eighth word in that line. The numbers will be meaningless to anyone who does not know what book or magazine is being used.

PRACTICE RIDDLE

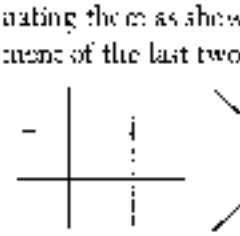
What flower's na
on a thumbtack?

(The key word is

[4] The

This cipher gets
separated by lines.
Masons' cipher bo
more than a hundr
to have used it duri

Draw two tic-tac
nating them as show
ments of the last two

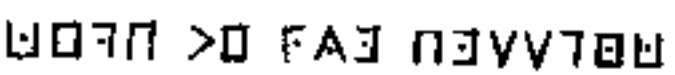


The alphabet is
Because this cipher
people, it is a good
usual order of letter

C	F	I
B	E	H
A	D	G

In the above syst
mum of the dictated
right), and number
bottom compartme

A message is encoded by substituting for each letter a tiny drawing of the compartment, with or without a dot, that contains the letter. This is how SEND ME TWO DOLLARS looks in the pigpen code:



PRACTICE RIDDLE 7

What's the end of everything?

[5] The Polybius Checkerboard

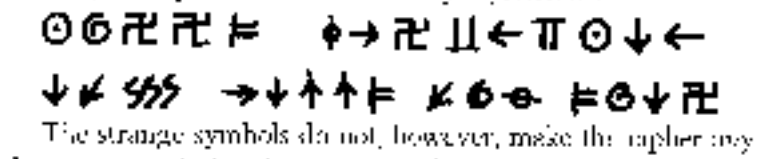
Polybius was an ancient Greek writer who first proposed a method of substituting different two-digit numbers for each letter. The alphabet is written inside a 5-by-5 square matrix which has numbered rows and columns:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y/Z

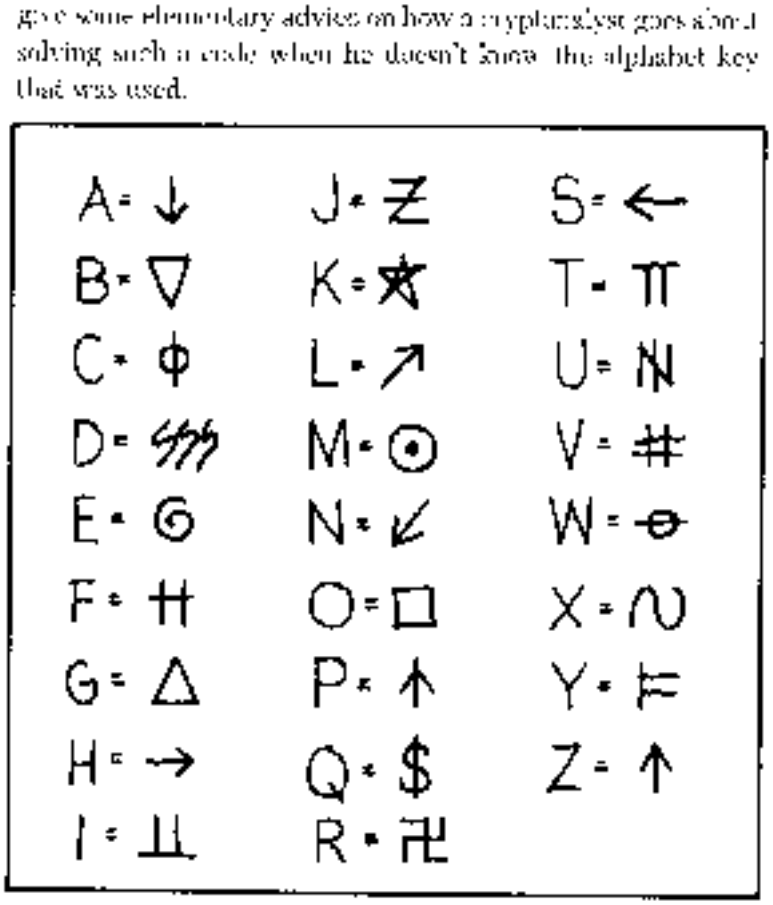
Note that both Y and Z are written in the last cell to divide the letters evenly. The context of the message should make it clear which of the two letters is intended.

To encode, substitute for each letter the numbers marking the row and column in which the letter appears. Always put

You can make up your own random cipher by writing the alphabet and pairing each letter with any sort of symbol you choose. The alphabet key shown below is typical. If you use it for encoding MERRY CHRISTMAS AND HAPPY NEW YEAR, the cipher text will look very mysterious:



The strange symbols do not, however, make the cipher any harder to crack than letters or numbers. The next chapter will give some elementary advice on how a cryptanalyst goes about solving such a code when he doesn't know the alphabet key that was used.



PRACTICE RIDDL

What goes "Yau

[7] The S

In the 1930's a

was the hero of a

popular radio show

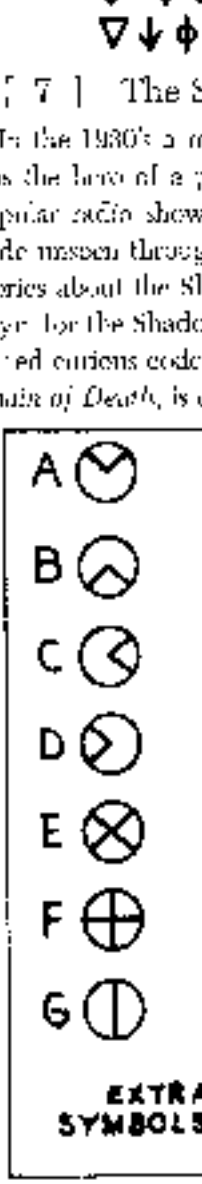
glide unseen throug

Stories about the Sh

anyone for the Shado

tained curious code

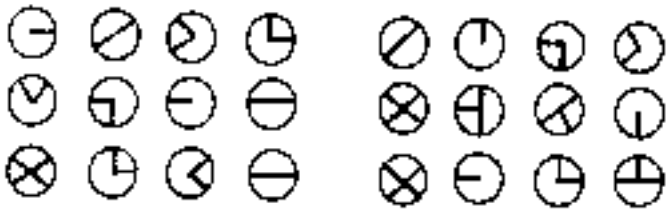
Chain of Death, is



In the alphabet key shown on the preceding page, note the four "extra symbols" at the bottom. These are inserted at any spot in the cipher text. Each symbol indicates how the sheet, on which the cipher text is written, is to be turned for encoding or decoding all the symbols that follow until the next extra symbol is reached.

Think of the line inside each extra symbol as a pointer that shows whether the top of the paper should be up, down, left or right. For example, if extra symbol 3 appears, the paper is turned upside down. Symbol 2 means that the page is turned so its top edge is on the right. Symbol 4 tells you to turn the sheet so its top edge is on the left. The first symbol means that the paper is in normal position, its top edge at the top.

The message: I AM IN DANGER. SEND HELP could look like this:



The first symbol tells you to give the page a quarter-turn clockwise before you decode the next four symbols. Then you come to another extra symbol which tells you to turn the page to normal position until you reach the next extra symbol. This constant turning of the sheet, while the alphabet key remains always in the same position, is a novel "twist" that makes this a most confusing cipher to any enemy who may intercept it.

PRACTICE RIDDLE 10

If two is company and three is a crowd, what are four, five, and six?

A message in the Da

"Why, Holmes,
Watson when he lo
torn from a notebo
mediately as a subst
ABE SLANEY. The
"I am fairly fam
Holmes declared, "a
graph upon the sub
sixty separate ciphe

5 3 ‡ ‡ †
) 4 ‡) ; 8
;J ‡ (; :
(; 8 8 *
* ‡ ? ; *
8 * ; 4 0
(‡ 9 ; 4
; 4) 4 8
; (8 8 ;
; : 1 8 8

The cryptogra

It was supposedly w
invisible ink on pare
The message, which

"A good
the devil
thirteen
twelve ba
shoot fro
head a b
the shot f

How
to Breal
Substitu
Ciphers

Solving simple subs
quires a great deal o
ter we will give a fe
solving the type of
puzzle in many new
time. Such cryptog
words. Punctuation
and so on—are also

First, some impo

1. The most ofte
frequency) by T, A
in German, French
languages it is not
used letter.)

2. The most comm

3. The most comm

4. A single-letter

5. The most freq
TO and IN.

6. The most used three-letter word is THE. The next most common is AND.

7. Q is always followed by U.

8. The consonant that most often follows a vowel is N.

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

10. The most frequently occurring four-letter word is THAT.

Note: THAT has the same letter at the beginning and at the end. When one or more letters appear more than once in a word, it is called a "pattern word." In solving a cryptogram, pattern words provide invaluable clues.

For example, suppose you saw the word XPP in a cryptogram. It is most likely to be a common word such as ALL, SEE or TOO, although it could be a less common word such as ODD, ADD, BOO, INN, EGG, ZOO and scores of others. As we have learned, XYZX is most likely to be THAT.

A five-letter pattern such as BDCKC is probably THERE, or WHERE, or THESE, although it could be hundreds of less common words, such as NIECE, ROSES, NOSES, OMAHA, or IRENE.

The pattern ABCDB is probably WHICH. RDMMRJ is a pattern word in which two letters, R and M, are repeated. LITTLE is the best bet. Much less likely possibilities include SNEESH, SWOOSH, and TWEETS.

A skilled solver of cryptograms will quickly recognize pattern words such as TOMORROW, PEOPLE, BANANA, BEGINNING, COMMITTEE, and many, many others. If the cryptogram is a quotation, followed by the author's last name, an old hand at solving cryptograms would immediately recognize RBKJDRLDKMD as SHAKESPEARE.

One of the most valuable of all tools for an amateur cryptographer is a table of the most common pattern words, arranged so that you can find a pattern quickly and learn the words that are most likely to fit. A brief list of this sort is in-

cluded in Fletcher
complete lists (for
in the programs of
eminent cryptanaly
mathematics at N
published a list of
nine letters. The w
tended in 1972 by
through sixteen lett
In 1937 Levine pub
pected Letters.

Another useful
dictionary" in whic
betized. For instan
you would look up
Brown, a professor
sylvania, directed
was published in 19
and Reverse English
entries. The set is
Commerce, Nation
Port Royal Road,
per volume.

It is hard to bel
also been publishe
Russia, Italy, and

The technique o
the best guesses yo
the letters through
make sense or if
letters. If the latter
and will have to try
an excellent descri
you will find more
Games (see Bibliog

Let's analyze a simple, well-known quotation from the work of a famous English author:

ZC HC UD CUZ ZU HO ZSGZ AE ZSO JKCOZAUC

This cryptogram is so short that we cannot rely on the fact that the most common letter in it is E. A good starting point is the pattern word ZSCZ. As we have learned, the most common four letter word is the pattern word THAT. Let's try it and see how it works out.

```
T       T   T       THAT
ZC HC UD CUZ ZU HO ZSGZ AE ZSO JKCOZAUC
```

We are probably on the right track because ZSO now has to be THE and ZU is almost certainly TO. Adding the new letters, E and O, gives us

```
TO  E O  OT  TO  E  THAT     THE     E T O
ZU HO UD CUZ ZU HO ZSGZ AE ZSO JKCOZAUC
```

The fourth word ends in OT. There are many possibilities. C, the first symbol of the word, cannot be H because H has already been used for another letter. Note that the last word of the cryptogram ends in C. TION is a very common ending for words. If we substitute TION on the last word, C becomes N and that would make CUZ translate as the common word NOT. Adding the new letters, I and N, continues to make good sense:

```
TO  E O  NOT  TO  E  THAT  /  THE    E TION
ZU HC UD CUZ ZC HC ZSGZ AE ZSO JKCOZAUC
```

AE cannot be IT, because T is already in our translation. IF doesn't fit well between THAT and THE, but IS does, so we add S to the solution:

```
TO  E O  NOT  TO  E  THAT  IS  THE    ESTION
ZU HC UD CUZ ZC HC ZSGZ AE ZSO JKCOZAUC
```

You will discover that, when you are working on a long cryptogram and trying out various hunches, you eventually reach a point at which you suddenly are absolutely sure that you are right and that it is only a matter of time until you complete the solution. This, in its small way, is not much different from the stronger emotion a scientist feels when he realizes there is enough evidence to make his new theory correct. The famous German philosopher and mathematician Gottfried Wilhelm Leibniz once observed that solving a cryptogram is very much like solving a problem in science. If a scientist has only two or three unrelated facts about nature that need to be explained by a theory, he can usually think of dozens of equally good theories, just as a cryptographer can think of dozens of solutions for one short word. But if there are a large number of facts to be explained, it is like having a long cryptogram to solve. It is not so easy to invent one theory to explain hundreds of different facts which were previously mysterious. When such a theory is invented, and it fits all these facts, it is probably correct for a reason that is curiously similar to the reason why a solution to a long cryptogram is probably correct if it fits all the symbols.

One of the greatest of recent scientific discoveries involved an artificial code used by nature: the genetic code. This code carries a plan for the development of an entire living creature along two intertwined DNA molecules in the nucleus of every living cell. The genetic code has an alphabet of only four symbols, each standing for a different chemical. The four chemicals are arranged along the DNA molecule in groups of three. These triplets are the "words" of an incredibly long "sentence" which tells every cell in a growing organism exactly what it is supposed to do.

In a metaphoric sense, the laws of science can be regarded as the "pattern words" of the universe. "Nature's great book," wrote Galileo, "is written in mathematical symbols." Scientists are like cryptographers engaged in the slow, progressive crack

ing of nature's code

I have given only
ple substitution ciph
sions are shown in
kinds of ciphers in
troductory book. If
cryptanalyst, I reco
Sinkov (see bibliog

Edgar Allan Poe,
cryptography, said
could construct one
may be right if we
tical cipher: that is,
encode and decode
must have a sufficie
sufficient time to wo
his theory has not y

So far in history,
moment our crypto
sage of the Soviet U
ing every one of ou

It is certainly p
ciphers that are m
Code-breakers devot
vented by an Amer
produces an incre
tographers call a "n
pletely random, and
In Kahn's excellent
Americans, he desc
and paper cipher a
World War II. It
often used? Becaus
plying new keys for
for general use.

Below is an illustration drawn by Rudyard Kipling for "The First Letter," one of five tales in his famous book for children *Just So Stories*. The picture shows an ivory tusk on which carved pictures tell a story about a girl named Taffimai. Kipling says that the strange symbols on the sides and at the bottom are magic Runic letters, but actually they are the symbols of a substitution cipher. Can you read Kipling's code?

Hints: There are many spelling peculiarities in the original text: YOU is represented by IU. W is either omitted or replaced by OU. F replaces V, and I is used instead of Y. In addition, A, C, O and T have two symbols each, and H has three.

The text on the left side begins: THIS IS THE STORY OF TAFFIMAI, ALL BITTEN OUT ON AN OLD TUSK.

Hard-to
Polyalp
Ciphers

The substitution c
the date shift ciph
for each letter. Suc
to solve, especially
has many messages
Force, State Depar
ment of any nation
first use ciphers t
monoalphabetic sub

These difficult
meaning *many*). T
different symbols
letter, and the sam
Polyalphabetic cod
tremely difficult to
be too complicated
code and decode
alphabetic ciphers

[1] Porta's Digraphic Cipher

A digraphic cipher is one in which pairs of letters, instead of individual letters, provide the basis of the cipher text. In the Porta Cipher, a single symbol is substituted for every pair of letters in the message. The method was invented by Giovanni Battista Porta, an Italian writer, scientist and magician. At the age of 28 he published (in 1563) a delightful book on ciphers, which included this one. It is the first known digraphic cipher.

To use the cipher you need an enormous 26-by-26 square matrix. The alphabet is written outside the border, once across the top and once down the left side. The 676 cells are filled in any way you like—letters, numbers, or symbols—as long as no two cells are the same. In the example (shown on the opposite page), numbers from 1 through 676 are used. Porta himself used strange-looking symbols. If you are curious, a copy of his matrix is reproduced on page 132 of *The Codebreakers*.

Suppose you wish to encode the word THEY. The first pair of letters is TH. Find T in the vertical alphabet, then move along its row until you reach the column headed by H. The number at this intersection is 502, so that is the first symbol of the cipher text. In a similar manner, find 129 at the intersection of row E and column Y, the next pair of letters in the message. The first letter of every pair always gives the row, and the second letter gives the column. The cipher text for THEY is written 502–129.

To decode, for each number in the cipher text, substitute the pair of letters heading the row and column in which the number appears, always getting down first the letter heading the row.

To make the cipher harder to break, it would be best not to fill the matrix with 676 numbers in sequence. The numbers should be put in the cells in a random order, or 676 different symbols could be used, as Porta did. Another scheme would