# 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"

Martin Gardner

# CODES, CIPHERS AND SECRET WRITING

Dover Publications, Inc.
New York

*For*

OSVVZ ZYTZC KJLQZ

Copyright © 1972 by Martin Gardner.
All rights reserved under Pan American and International Copyright Conventions.

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 unaltered republication of the work first published by Simon & Schuster, Inc., New York, in 1972.

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] 001.54'36 84-8024
ISBN 0-486-24761-9

# Contents

Introduction 7

1 Easy Transposition Ciphers 11

The Rail Fence Cipher • The Twisted Path Cipher • Scrambling with a Key Word

2 Easy Substitution Ciphers 21

Shift Ciphers • Date Shift Ciphers • Key Word Ciphers • The Pigpen Cipher • The Polybius Checkerboard • Random Substitution Ciphers • The Shadow's Code

3 How to Break Substitution Ciphers 35

4 Hard-to-break Polyalphabetic Ciphers 43

Porta's Digraphic Cipher • The Playfair Cipher • Lewis Carroll's Vigenère Cipher

5 Simple Code Machines 53

Typewriter Codes • A Telephone Dial Code • The

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 Crease Code • The Swizzle Stick Code

8 Codes for Other Worlds 87

References for Further Reading 94

Historical • Methods • Codebreaking • Cipher Cranks • Interplanetary Communication

# Introduction

Cryptography, the writing and deciphering of messages in secret code, and other forms of secret writing have always played, and still play today, vital roles in the history of every nation. It is necessary in this crazy world of ours for governments and spies to send special information in secret ciphers. It is just as necessary for every major nation to have a staff of expert cryptanalysts who work day and night, with electronic computers at their elbows, to crack the codes used by other countries. The history of cryptanalysis (so marvelously told by David Kahn in his comprehensive book *The Codebreakers*) is a fascinating one, filled with dramatic incidents in which the fates of empires and political leaders hinged on the success or failure of a small group of specialists in this ancient, curious kind of puzzle solving.

I say "small" because in earlier centuries such work was often done by only a few cryptanalysts, sometimes only by one man. Today, codebreaking is a vast and rapidly growing profession. No one knows exactly how many people are now engaged in codebreaking for the United States, but they certainly number in the tens of thousands and cost us more than a billion

dollars a year. During World War II, 30,000 persons in Great Britain alone were assigned to such work. It is probably our 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 secret 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



it is even more fun to break a code used by someone else. If you belong to a secret club, you and your friends may want to communicate with one another by one of the methods explained in this book. If you keep a diary, you may wish to protect it from prying eyes by using a code.

Many famous people have written all or parts of their diaries in code. When Franklin Delano Roosevelt was twenty-one, he used a cipher for four entries in a diary he was then keeping. In 1971 these entries were shown for the first time to several cryptographers, who had no trouble breaking the code. It was a simple substitution cipher using numbers for vowels and symbols for consonants. The translations proved to be so tame that one wonders why young Roosevelt bothered to put the entries in code.

If you are clever and diligent, you, too, can learn how to break secret codes. The solving of substitution ciphers is now a popular type of puzzle with enough fans to support a daily "cryptogram" in hundreds of newspapers throughout the country. There is even an American Cryptogram Association which publishes a bimonthly periodical called *The Cryptogram.* (If you are interested, you can write to the treasurer at 604 W. Monroe St., Mexico, Missouri 65265.) Chapter 3 will introduce you to the exciting art of solving cryptograms.

The main purpose of this book, however, is to teach you how to use the most important codes, and other methods of secret communication, that have been invented since ancient times. A selected list of references at the end of the book will provide more reading material about the unusual techniques that have been employed for making ciphers, and for breaking ciphers used by others.

I am indebted to David B. Eisendrath, Jr., for many excellent suggestions which I have followed in Chapter 6, and to David Kahn for writing *The Codebreakers,* my principal source of information.

MARTIN GARDNER

CHAPTER 1

# Easy Transposition Ciphers

A transposition cipher is one that does not change any letters of the original message. (Cryptographers call the original the "plaintext" but we will simply call it the "message.") It merely rearranges the letters, according to a secret system, so that anyone who knows the system can put the letters back in their proper order and read the message.

The simplest transposition cipher is made by just writing the message backward. AGENT 427 IS ON HIS WAY becomes YAW SIH NO SI 724 TNEGA. If the message happens to be a palindrome—a sentence that reads the same in both directions—the letters will be in exactly the same order when reversed. For example: PULL UP IF I PULL UP, or 'TIS IVAN ON A VISIT. This is not likely to happen, however, with any genuine message.

The main trouble with backward writing is that it is too easy to recognize. If you keep the original word order, but reverse the letters of each word separately, the reversal is a bit harder to spot, but not much. The following transposition ciphers are better and almost as easy to remember and use.

## [ 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 trifle lower on the page. The message will look something like a rail fence:

```
M E M T N G T X
 E T E O 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 O 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 ETEO IHQZ



Decoding the message is just as easy as encoding. First divide the cipher text exactly in half by a vertical line:

MEMT NGTX | ETEO IHQZ

Now read the original message by checking off the first letter of the left half, the first letter of the right half, the second letter of the left half, the second letter of the right half, and so on. Ignore the three nulls at the ends. It is easy to guess where the spacings belong between words.

You can vary the rail fence cipher, if you like, by copying the two rows in reverse order, or by copying one row forward and the other backward. The decoding procedure, which you can easily work out for yourself, has to be changed accordingly.

Other variations can be obtained by writing the letters in a zigzag of more than two lines. For example, a 3-line rail fence cipher would begin like this:

```
M   M   N   T
 E T E O I H Q Z
  E   T   G   X
```

And encode:

MMNT ETEO IHQZ ETGX

The best way to understand a cipher is to use it for decoding an actual message. Throughout the book you will find "Practice Riddles" with coded answers that can be read only by deciphering them. *Please* do not try to do this directly on the book's pages. Copy the coded answer on a sheet of paper, then do all your work on that sheet. In this way you won't deface the book and spoil the fun for the next reader (if it is a library book), or for a friend who may wish to borrow your book.

PRACTICE RIDDLE 1

What goes "Tee, he, he, he, he, plop!"?

AALU HNHS EDFY MNAG IGIH AOFZ

(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:

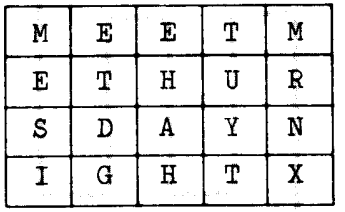
MEET ME THURSDAY NIGHT

The message has 19 letters. As before, we add enough nulls (in 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.



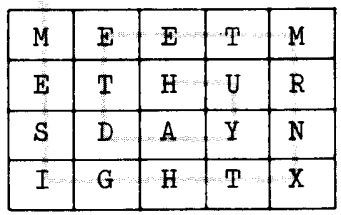



Copy the letters along the path, starting with the bottom cell on the right and following the curved line as it twists its way upward and leftward. The cipher text, written in groups of four, will be:

XNRM TUYT HAHE ETDG ISEM

To decipher, draw an empty 4–by–5 matrix, then fill in the cells with the letters of the cipher text. The first letter, X, goes in the lower right corner. N goes in the cell above it. Continue writing the letters along the same plow path that was used in coding the message. The message is read by taking each row from left to right, starting with the top row.

Another good path is a spiral. You can start the spiral at any corner cell and whirl inward, clockwise or counterclockwise, or you can begin at one of the central cells and spiral outward as shown below:



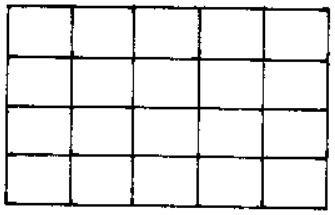

This spiral produces the cipher:

HUYA DTEE TMRN XTHG ISEM

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.

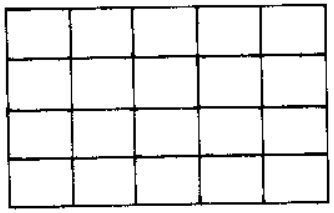
Of course you and whoever receives the code must agree beforehand on the exact method to be used, as well as on the dimensions of the matrix. If you wish to vary the size and shape of the matrix with each message, you can put one number at the beginning of the cipher to indicate the height of the matrix, 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:





Or you can follow a diagonal plow path:



Indeed, you can adopt any type of path you like as long as everyone who sends and receives the cipher knows exactly what kind of path (or paths) is being used.

**PRACTICE RIDDLE 2**

What is gray, lives in a tree, and is terribly dangerous?

INEG UNHT RIUQ SÀRH AMAC IWLE

(A 4-by-6 matrix was filled by writing left to right, from top to bottom. Then the answer was encoded along a counterclockwise spiral beginning at the lower left corner.)

## [ 3 ] Scrambling with a Key Word

This is a subtle and historically important variation of the previous transposition method. Instead of using regular paths, broken or continuous, a "key word" is employed for mixing up the columns of a matrix in a completely haphazard way.

We will explain how it works by using the same message as before and the same 4-by-5 matrix. First the message is written in the 20 cells according to an agreed-upon plan. Let's assume it is along a clockwise spiral:

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

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.

2 5 1 4 3
F R A N K

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

| 2 | 5 | 1 | 4 | 3 |
|---|---|---|---|---|
| M | E | E | T | M |
| Y | N | I | G | E |
| A | X | T | H | T |
| D | S | R | U | H |



The digits tell us the order to follow in copying the columns from top down. Copy first the column headed 1, then the column headed 2, and so on to column 5. The cipher text will be:

EITR MYAD METH TGHU ENXS

The person who receives the cipher knows that the key word is FRANK, from which he quickly derives the number 25143. He draws the empty matrix, puts the digits above the columns, then copies the cipher vertically in each column, in the order indicated by the digits. After filling columns 1 and 2, his matrix will look like this:

| 2 | 5 | 1 | 4 | 3 |
|---|---|---|---|---|
| M | | E | | |
| Y | | I | | |
| A | | T | | |
| D | | R | | |

When all the cells are filled, the message is read along the agreed-upon clockwise spiral path. The advantage of this method is that it does not use simple and regular paths which could be guessed by a clever enemy who might "intercept" (as cryptographers like to say) the cipher text. Instead, it furnishes a haphazard broken path which is hard to discover unless one knows both the system and the key word.

Key words are so easy to remember that you and your friends can change the cipher every week by just picking a new word. A rectangular matrix of any size or shape can be used, but of course the key word must have the same number of letters as there are matrix columns. Using key words, or key phrases, to "randomize" cipher texts is an ancient but valuable technique. It is still used today in many of the elaborate cipher systems employed by nations throughout the world.