

# 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



Martin Gardner

CODES  
SECRET

Learn to use  
communication  
and cryptic, K  
and politics, K  
cryptology -

Beginning with  
world-famous  
complicated pa  
squares, trian  
typewriters and  
bricks and yee  
grow in shad  
possibilities of  
world.

Using this book  
used by Austr  
Can't be rate  
Cipher, The  
covered by auth  
Kidd and the S  
method of mess  
and more

Young cryptanal  
of intrigue and

... a stimulat

Cambridge Un  
published by S  
98pp, 5 1/2 x 8 1/2

UNIVERSITY  
CAMBRIDGE

---

C

For

GRACE ZYNG KUTAGG

Content

Introduction

- 1 Easy Transport  
The Bail Fee  
• Summing
- 2 Easy Substitution  
Shift Ciphers  
Ciphers • The  
Checkerboard  
The Shadow's
- 3 How to Break
- 4 Hard-to-break  
Porta's Dijkstra  
Lewis Carroll
- 5 Simple Code  
Typewriter C

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

Published in Canada by General Publishing, Commerce, Ltd., 50  
Lambton Road, Don Mills, Toronto, Ontario.  
Published in the United Kingdom by Constable and Company Ltd.

This Dover edition, first published in 1954, is an unabridged and  
unaltered republication of the work first published by Simon & Schuster  
Company, New York, in 1928.

Manufactured in the United States of America  
Dover Publications, Inc., 31 East 21st Street, Mineola, N.Y. 11501

Library of Congress Cataloging in Publication Data

Gardner, Martin, 1914-

Ciphers, ciphers, and secret writing.

Reprint. Originally published: New York: Simon & Schuster, c1972.  
1st. Typewritten.

1. Cryptography. 2. Ciphers. I. Title.  
QA769.G37 1984.      002.5439.      81-5024  
ISBN 0-486-24111-0

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 Be- comes Visible When the Sheet Is Wet • Writing That Can Be Seen in Slanting Light • Typing That Can Be Seen in Backlight	
7	Bizarre Methods of Message Sending	75
	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 • Code-breaking • Cipher Cranks • Interplanetary Communication	

## Introduc

Cryptography, the secret code, and o played, and still pl nation. It is necessa, rones and spies to It is just as necessa expert cryptanalysts computers at their countries. The histo David Kahn in his is a fascinating one. ldes of empires and hure of a small g kind of puzzle solvi I say "small" be often done by only men. Today, codeb fession. No one kno gaged in codebreak number in the time

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 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 1963 U-boat victories against Allied shipping were the result of Germany having broken the British merchant ship code. The code did not fall 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 there 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 if you belong to a secret society and can communicate with other members. This is the subject of this book. If you are interested, look for more from prying eyes here.

Many famous people have used secret codes. When Vera used a cipher for her secret messages to her husband in 1971 these codes were solved by cryptographers, who used a simple substitution cipher: each letter of the alphabet was replaced by a different symbol for communication. It is a code that one wonders how many people still use in their entries by code.

If you are clever you can break secret codes. This is a popular type of puzzle called a "cryptogram" in hobby magazines. There is even a magazine that publishes a bimonthly cryptogram. If you are interested in this subject, look for more on Monroe St. Meier's book, *Secret Codes and Ciphers*, available at your local bookstore or by mail.

The main purpose of this book is to use the most interesting and useful codes for communication. This is a selected list of codes that have been used in the past and more reading material that has been employed for communication and used by others.

I am indebted to many people for their kind suggestions and comments. I am especially indebted to David Kahn for his help and for his source of information.

---

## Easy Transpo Ciphers

A transposition cipher is a type of cipher that does not change the letters of the original message (the "plaintext") but merely rearranges them so that anyone who intercepts the message must rearrange them in their proper order to read it.

The simplest transposition cipher is the "columnar transposition cipher." The message "THIS IS A PALIN" becomes "YAW SIH". This cipher is a palindromic cipher, meaning it works both directions—the ciphertext "YAW SIH" when reversed, "HIS IVA N O N A", is the same as the original message "THIS IS A PALIN".

However, with any general transposition cipher, the main trouble is that they are easy to recognize. The letters are not in reverse order, but harder to spot, and transposition ciphers are better used for short messages.

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

M E E T M E T O N I G H T  
  Q X Z

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

M E M T N G I X E T E C J 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 these 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 NGCX ETEC IHQZ

Decoding the message is simple. Write the cipher text on a grid:

MEMT  
NGCX  
ETEC  
IHQZ

Now read the message by starting with the first letter of the left-hand column, then the second letter of the left-hand column, and so on, ignoring the spaces. The message will appear where the spaces go.

You can vary the number of rows by changing the two rows in the preceding example toward and the other way. The number of rows which you can easily remember is 10, so you can easily vary the number of rows accordingly.

Other variations of the rail fence cipher would be a zigzag of more than two rows. A zigzag of more than two rows would be a variation of the rail fence cipher which would be a variation of the rail fence cipher.

And finally:

MEMT  
NGCX  
ETEC  
IHQZ

The best way to find an actual message is to try the "Practice Riddles" by deciphering the messages on the back of the book's pages. Can you find the message? Then do all your work on a separate sheet of paper. Do not deface the book (and if it is a library book, do not deface the book).



**PRACTICE RIDDLE 1**

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

AALU HNHS LIFY MNAD IGTH AOEZ

(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	X
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  
cell on the right  
way upward and  
of four, will be:

XN=K

To decipher, dra  
cells with the let  
goes in the lower ri  
time writing the l  
used in coding (ie  
each row from left

Another good pa  
corner cell and wh  
er you can begin u  
as shown below:

This spiral pro

HUPA

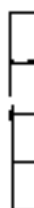
If you want to make this code even harder to break, you can combine two different paths. For example, write the message in the matrix along a plow path instead of left to right by rows. Then encode it by taking the letters along a spiral path. To decode, write the letters of the cipher text along the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



Indeed, you can  
as everyone who sees  
what kind of path

#### PRACTICE PADDY

What is gray, liv

HEX IN

(A 4-by-4 matrix  
top to bottom. The  
clockwise spiral be

#### [ 3 ] Scram

This is a subtle  
previous transposi  
broken or continu  
the columns of a m

We will explain  
as before and the  
written in the 20 c  
assume it is along

The digits tell us from top down, Column headed 2, and

EITH

The person who word is FRANK, 25143. He draws the columns, then copy the order indicated 2, his matrix will be

F	E	S	T	R
Y	K	I	G	E
A	X	D	E	D
L	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
F	R	A	N	K
Y	K	I	G	E
A	X	D	E	D
L	S	R	U	H

When all the colleagues upon a clock method is that it do could be guessed us cryptographer furnishes a haphaz unless one knows b

Key words are friends can change new word. A route used, but of course of letters as there key phrases, to "ran code technique. It cipher systems crop

---

### PRACTICE RIDDLE 3

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

MEEG UEFI AANO CEGM SEGC

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

## Easy Substitution Ciphers

In the ciphers discussed here, some or all of the letters of a message remain the same. In a simple letter-for-letter substitution cipher, each letter of the message is replaced by another letter. This can be combined in many ways. For example, you can come over to my house every evening and dress in a certain way, restrict the words you use to certain words or phrases, and use a special codebook. This is a common practice of

Most of the following are "monoalphabetic," meaning that every letter, one and the same, is replaced by the same letter. If the code letter for the letter A is T, then every A in the cipher text it means 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:

NRTGCV SZH YEC LVVG

or, if you group the letters in quadruplets,

NRIG CVSH YERT LVVG

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—that your enemy is a minute or two to be a substitution method was much superior.

## [ 1 ] Shift

These are often called Caesar ciphers. The Roman emperor Julius Caesar used them for his secret messages. The

A key number, k, which can be varied, shifts a second alphabet one. Suppose the key is 3. Put your pen to the right, starting at A, and count three letters. Continue to the right, and when you go back to the beginning of the alphabet, the cipher will look like

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  
 A B C D E F G H

To encode a message, substitute for it the letter three places to the right. MYRTLE shifts to NRTGCV. To decode, find the letter three places to the left of the letter above it.

Needless to add, the alphabet goes on after you have encoded a message. If someone might find out the secret of the key, you can change it.

Occasionally a word is shifted a certain number of places when it is sh-

Try encoding it in a 5-shift cipher and you'll be surprised by what you get. What happens to PEGAN 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 ABJURE. In a 13-shift cipher it becomes NOWHERE.

#### PRACTICE PUZZLE 4

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

8V2007 P3AGF

What did he want it for?

3RA P3AGF

(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  
 XYRTE HAS BIG FEET

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

to write down two zero distances, so it became U, and since if a shift carries you around,

The final cipher encoding the letters in green

FEET

To decode, write the same way you did encode in the alphabet above it. Whenever Z and continue the

Note that the cipher quadruplet, for example in "feet" are represented in CEFT represent

The date-shift cipher for 4, a cipher of the

You don't have to for a variable shift remember the key in Chapter 5, code

#### PRACTICE PUZZLE

What did Paul ride?

(Use the date of your.)

### [ 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 E F G H I K L M N O Q R 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 *not* changed 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 name  
 on a thumbstick?

(The key word is

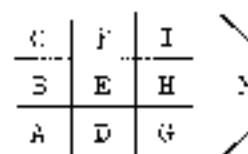
### [ 4 ] The Book

This cipher gets its name from the fact that the letters are separated by dashes. Because this cipher has been used more than a hundred times, it is thought to have been used during the

Draw two tick marks on each side of the dashes separating the *m* as shown in the diagram. The movement of the last two



The alphabet is used in the order shown. Because this cipher is not known to many people, it is a good one to use. The usual order of letters



In the above system, the letters are separated by dashes (right), and counted in the order shown in the diagram.

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 cipher code:

□○□□ >○ □▲□ □○□□□□

#### PRACTICE PUZZLE 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 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

the row number first. The word WATERBURY

53 - 41 - 45 -

To decode, simply look for the first number. The first number is 53, so the intersection of the 5th

#### PRACTICE PUZZLE 8

If you stand so close to the west, what is on your

21 - 24 -

### [ 6 ] Random

All the substitution ciphers we've looked at so far have a disadvantage: as we have seen, the alphabet key and the alphabet key are the same each time you encode or decode.

A random substitution cipher is not a plan. You make up a key for each letter you use, but any time you run the message through you run the message through a different substitution cipher. This is a simple system.

Dozens of Detectives is a book in which random ciphers are used. One of the best known is "The Adventure of the Hound of the Baskin's" by Edgar Allan Poe. In this story, the detective uses numbers and



You can make up your own random cipher by writing the alphabet and pairing each letter with any set 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:

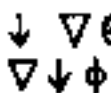
⊙ ⊙ Ꞥ Ꞥ Ꞥ    ϕ → Ꞥ ∟ ← ∟ ⊙ ↓ ←  
 ↓ ← ꙰꙰꙰    → ↓ ↑ ↑ Ꞥ    ↘ ⊙ ⊙ Ꞥ ⊙ ↓ Ꞥ

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.

A = ↓	J = ⚡	S = ←
B = ▽	K = ✱	T = ∟
C = ϕ	L = ↗	U = ∟
D = ꙰꙰꙰	M = ⊙	V = #
E = ⊙	N = ↘	W = ⊙
F = ∟	O = □	X = ~
G = Δ	P = ↑	Y = Ꞥ
H = →	Q = \$	Z = ↑
I = ∟	R = Ꞥ	

#### PRACTICE RIDDLE

What goes "Zazid?"



[ 7 ] The S

In the 1930's a man was the hero of a popular radio show who glide unseen through Stories about the Sh... ungr... for the Shado... tained curious code... Chain of Death, is c...

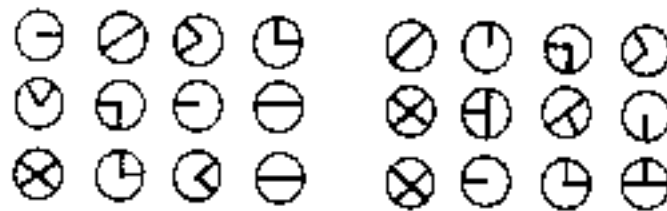
A	⊙
B	⊙
C	⊙
D	⊙
E	⊗
F	⊕
G	⊙

EXTRA SYMBOLS

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.

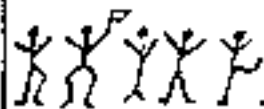
The message: I AM IN DANGER. SEND HELP could look like this:



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 Lullaby cipher.

"Why, Holmes, Watson when he has torn from a notebook immediately as a substitute for the word 'I AM SLANLY.' The

"I am fairly sure," Holmes declared, "in graph upon the subject sixty separate cipher-

5 3 + + +  
 ) 4 + ) : 8  
 J + ( : :  
 ( : 8 8 \* +  
 \* + 2 : \*  
 8 \* : 4 0  
 ( + 9 : 4  
 : 4 ) 4 8 5  
 : ( 8 8 :  
 : : I 8 8 :

The substituted

It was supposedly v  
 invisible ink on page  
 The message, which

"A good  
 the dead  
 thirteen a  
 make his  
 shoot from  
 head a l  
 the shot f

---

# How to Break Substitu- tion Ciphers

Solving simple substitution ciphers requires a great deal of patience. In this chapter we will give a few hints for solving the type of puzzle in many newsgroups. Such cryptograms, words, punctuation, and so on—are also

First, some input:

1. The most often used letter (frequency) by T, A, or E (in German, French languages it is not used letter.)
  2. The most common letter.
  3. The most common letter.
  4. A single-letter word.
  5. The most frequent letter.
- TO or c. 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, PP, 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, SEP or TOO, although it could be a less common word such as ODD, ADD, BOO, INN, FCC, ZOO and scores of others. As we have learned, XYZ is most likely to be THAT.

A five-letter pattern such as BDCCK is probably THERE, or WHFRE, or THESE, although it could be hundreds of less common words, such as NICEF, ROSLS, NOSES, OMAHA, or IRENE.

The pattern ABCDE 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 SNFESL, 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, you could hand at solving cryptograms would immediately recognize RBEJDRBDRMD 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's complete lists (found in the programs of eminent cryptanalysts in mathematics at New York University). He published a list of nine letters. The work was completed in 1972 by through sixteen letters in 1957. *Levine published Letters.*

Another useful volume is a "dictionary" in which the words are alphabetized. For instance, you would look up "B" and find "Brown," a professor at Columbia, directed to was published in 1957 and *Revised English* entries. The set is Commerce, National Port Royal Road, \$10 per volume.

It is hard to believe also been published in Russia, Italy, and Japan.

The technique of the best guesses you can make through the letters through make sense or if the letters. If the letter and will have to try an excellent description you will find more. Games 1500-5000.

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 JKOEZAUO

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 ZSGZ. 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 ZC HC UD CUZ ZU HO THAT ZSGZ AE TH ZSO JKOEZAUO

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 UD CUZ TO E THAT AE THE E T O JKOEZAUO

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, O 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 UD NOT TO E THAT IS THE E TION JKOEZAUO

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 UD NOT TO E THAT IS THE ESTION JKOEZAUO

At this point you TO BE OR NOT TO BE the famous line speaks the same name. Or solve. All our guesses false hunches that different possibilities general idea of how codes

Cracking cryptograms you solve, the better several pages to cry readers of this book (fortunately, not every There would be a cryptograms by writing the trouble to do we'd get to mark keep the book on it

The best plan, if is to ask a friend or with a code message the better. Whoever long message would the opposite is true would be impossible be any word of four

Claude L. Shannon founded a branch of information theory, wrote a paper in the *Journal*, October, 1948. The cryptogram has 80 or more one solution, but it's possible to find more than

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 actual 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 metaphorical 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 the cryptographers engaged in the slow, progressive crack-

ing of nature’s mystery.

I have given only a few simple substitution ciphers and shown only a few kinds of ciphers in this introductory book. If you are a cryptanalyst, I recommend you read *Cracking Codes and Ciphers* by Simon Singh (see listing).

Edgar Allan Poe, in his book on cryptography, said that a cryptanalyst could construct code words that may be right if selected ciphers that is, encodes and decodes must have a sufficient time to work. If his theory has not yet been tested.

So far in history, at the moment our cryptanalysts of the Soviet Union are using every one of our codes.

It is certainly possible to find ciphers that are more complex than the ones in *Cracking Codes* devoted by an American cryptanalyst, an American cryptanalyst call a “codebook” completely random, and it is possible to find a codebook in Kalin’s excellent *American Cryptography*, he described a codebook and paper cryptanalyst at World War II. It is often used? Because of the complexity of new keys for use for general use.

# Hard-to-Polyalphabetic Ciphers

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 Tattiloan. 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?

Hint: There are many spelling peculiarities in the original text: YOO is represented by U, W's 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 TATTILMAI, ALL BITTEN OUT ON AN OLD TUSK.



The substitution of the data shift cipher for each letter. Such to solve, especially has many messages. Fore, State Department of any nation first use ciphers. Monalphabetic substitution. These difficult meaning many. Different symbols letter, and the same. Polyalphabetic code. Tremendously 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 assigned 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 1569) 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 135 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's 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 putting 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

Z	26	52	78	104	130	156	182	208	234	260	286	312	338	364	390	416	442	468	494	520	546	572	598	624	650
Y	27	54	81	108	135	162	189	216	243	270	297	324	351	378	405	432	459	486	513	540	567	594	621	648	675
X	28	56	84	112	140	168	196	224	252	280	308	336	364	392	420	448	476	504	532	560	588	616	644	672	700
W	29	58	87	116	145	174	203	232	261	290	319	348	377	406	435	464	493	522	551	580	609	638	667	696	725
V	30	60	90	120	150	180	210	240	270	300	330	360	390	420	450	480	510	540	570	600	630	660	690	720	750
U	31	62	93	124	155	186	217	248	279	310	341	372	403	434	465	496	527	558	589	620	651	682	713	744	775
T	32	64	96	128	160	192	224	256	288	320	352	384	416	448	480	512	544	576	608	640	672	704	736	768	800
S	33	66	99	132	165	198	231	264	297	330	363	396	429	462	495	528	561	594	627	660	693	726	759	792	825
R	34	68	102	136	170	204	238	272	306	340	374	408	442	476	510	544	578	612	646	680	714	748	782	816	850
Q	35	70	105	140	175	210	245	280	315	350	385	420	455	490	525	560	595	630	665	700	735	770	805	840	875
P	36	72	108	144	180	216	252	288	324	360	396	432	468	504	540	576	612	648	684	720	756	792	828	864	900
O	37	74	111	148	185	222	259	296	333	370	407	444	481	518	555	592	629	666	703	740	777	814	851	888	925
N	38	76	114	152	190	228	266	304	342	380	418	456	494	532	570	608	646	684	722	760	798	836	874	912	950
M	39	78	117	156	195	234	273	312	351	390	429	468	507	546	585	624	663	702	741	780	819	858	897	936	975
L	40	80	120	160	200	240	280	320	360	400	440	480	520	560	600	640	680	720	760	800	840	880	920	960	1000
K	41	82	123	164	205	246	287	328	369	410	451	492	533	574	615	656	697	738	779	820	861	902	943	984	1025
J	42	84	126	168	210	252	294	336	378	420	462	504	546	588	630	672	714	756	798	840	882	924	966	1008	1050
I	43	86	129	172	215	258	301	344	387	430	473	516	559	602	645	688	731	774	817	860	903	946	989	1032	1075
H	44	88	132	176	220	264	308	352	396	440	484	528	572	616	660	704	748	792	836	880	924	968	1012	1056	1100
G	45	90	135	180	225	270	315	360	405	450	495	540	585	630	675	720	765	810	855	900	945	990	1035	1080	1125
F	46	92	138	184	230	276	322	368	414	460	506	552	598	644	690	736	782	828	874	920	966	1012	1058	1104	1150
E	47	94	141	188	235	282	329	376	423	470	517	564	611	658	705	752	799	846	893	940	987	1034	1081	1128	1175
D	48	96	144	192	240	288	336	384	432	480	528	576	624	672	720	768	816	864	912	960	1008	1056	1104	1152	1200
C	49	98	147	196	245	294	343	392	441	490	539	588	637	686	735	784	833	882	931	980	1029	1078	1127	1176	1225
B	50	100	150	200	250	300	350	400	450	500	550	600	650	700	750	800	850	900	950	1000	1050	1100	1150	1200	1250
A	51	102	153	204	255	306	357	408	459	510	561	612	663	714	765	816	867	918	969	1020	1071	1122	1173	1224	1275



- [Ciel et Espace, n°504 \(mai 2012\) online](#)
- [download online \*Testing the Limit: Derrida, Henry, Levinas, and the Phenomenological Tradition \(Cultural Memory in the Present\) online\*](#)
- [read To Catch a Bride \(Devil Riders, Book 3\)](#)
- [read Brand New Cherry Flavor: A Novel of the Occult pdf, azw \(kindle\)](#)
  
- <http://aseasonedman.com/ebooks/Ciel-et-Espace--n--504--mai-2012-.pdf>
- <http://growingsomeroots.com/ebooks/Baseball-Prospectus-2016.pdf>
- <http://pittiger.com/lib/Common-Space--The-City-as-Commons--In-Common-.pdf>
- <http://betsy.wesleychapelcomputerrepair.com/library/Test-Your-Emotional-Intelligence--Improve-Your-EQ-and-Learn-How-to-Impress-Potential-Employers.pdf>