

The Cryptoclub

Using Mathematics
to Make and Break
Secret Codes



Janet Beissinger and Vera Pless



The Cryptoclub

Using Mathematics to Make and Break Secret Codes



Janet Beissinger
Vera Pless

Daria Tsoupikova, Artist



A K Peters
Wellesley, Massachusetts

Editorial, Sales, and Customer Service Office

A K Peters, Ltd.
888 Worcester Street, Suite 230
Wellesley, MA 02482
www.akpeters.com

Copyright ©2006 by The Board of Trustees of the University of Illinois

All rights reserved. No part of the material protected by this copyright notice may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.



This material is based upon work supported by the National Science Foundation under Grant No. 0099220. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Library of Congress Cataloging-in-Publication Data

Beissinger, Janet.

The cryptoclub : using mathematics to make and break secret codes / Janet Beissinger, Vera Pless.

p. cm.

ISBN-13: 978-1-56881-223-6 (alk. paper)

ISBN-10: 1-56881-223-X (alk. paper)

1. Mathematics--Juvenile literature. 2. Cryptography--Juvenile literature.

I. Pless, Vera. II. Title.

QA40.5.B45 2006

510--dc22

2006002743

Book and cover design by Erica Schultz.

Set in ITC Officina and Agate SSK by A K Peters, Ltd.

Printed and bound in India.

10 09 08 07 06

10 9 8 7 6 5 4 3 2 1

Contents

Foreword	ix
Preface	xi
Acknowledgments	xiv

Unit 1 Introduction to Cryptography

Chapter 1 Caesar Ciphers	2
DO YOU KNOW? Little Orphan Annie and Captain Midnight	7
Chapter 2 Sending Messages with Numbers	8
DO YOU KNOW? Beale Ciphers and a Buried Treasure	18
Chapter 3 Breaking Caesar Ciphers	20
DO YOU KNOW? Navajo Code Talkers	26

Unit 2 Substitution Ciphers

Chapter 4 Keyword Ciphers	28
DO YOU KNOW? Dancing Men	33
Chapter 5 Letter Frequencies	34
DO YOU KNOW? Edgar Allan Poe Challenges	39

Chapter 6	Breaking Substitution Ciphers	40
	DO YOU KNOW? Poor Mary	50

Unit 3 Vigenère Ciphers

Chapter 7	Combining Caesar Ciphers	52
	DO YOU KNOW? The Civil War	61
Chapter 8	Cracking Vigenère Ciphers When You Know the Key Length	62
	DO YOU KNOW? Lewis and Clark	73
Chapter 9	Factoring	74
	DO YOU KNOW? Cicadas	83
Chapter 10	Using Common Factors to Crack Vigenère Ciphers	84
	DO YOU KNOW? The One-Time-Pad and Atomic Spies	98

Unit 4 Modular (Clock) Arithmetic

Chapter 11	Introduction to Modular Arithmetic	102
	DO YOU KNOW? How the United States Entered World War I	112
Chapter 12	Applications of Modular Arithmetic	114
	DO YOU KNOW? Non-Secret Codes	121

Unit 5 Multiplicative and Affine Ciphers

Chapter 13	Multiplicative Ciphers	124
	DO YOU KNOW? Passwords	131
Chapter 14	Using Inverses to Decrypt	132
	DO YOU KNOW? The German Enigma Cipher	142
Chapter 15	Affine Ciphers	144
	DO YOU KNOW? Atbash	152

Unit 6 Math for Modern Cryptography

Chapter 16	Finding Prime Numbers	154
	DO YOU KNOW? The Great Internet Mersenne Prime Search	165
Chapter 17	Raising to Powers	166
	DO YOU KNOW? Dead Men Can't Tell Passwords	172

Unit 7 Public Key Cryptography

Chapter 18	The RSA Cryptosystem	174
	DO YOU KNOW? Modern Uses of Cryptography	181
Chapter 19	Revisiting Inverses in Modular Arithmetic	182
	DO YOU KNOW? Jefferson and Madison: But Where Is the Key?	187
Chapter 20	Sending RSA Messages	188
	DO YOU KNOW? The British Public Key Ciphers	193
	Index	195
	Make Your Own Cipher Wheel	199

Foreword

The Cryptoclub is a wonderful introduction to cryptography for middle-school students. As a research mathematician with a long-standing interest in this subject, I am very favorably impressed by the accuracy, clarity, and relevance of the material presented. I believe that this book offers a great opportunity to introduce students to applications of mathematics that are both exciting and also play a major if sometimes hidden role in our daily activities. Encryption of information is used not only by students and governments to keep communications secret but also by banks and other businesses to secure sensitive information. With the growing number of transactions taking place over the Internet, cryptography is of ever-increasing importance.

Many people have the mistaken impression that mathematics is a static subject, one in which everything has been known for hundreds of years. Cryptography acts as a window to the open questions and evolving nature of mathematics and, in particular, to number theory, often considered an amusing playground for mathematicians with little relevance to the real world. In this book, we are shown why this view now has been completely reversed.

By incorporating various mathematical skills (factoring, exponentiation, modular arithmetic, etc.) and using them in a concrete way, the authors motivate students; by testing the efficiency of different encryption techniques, they stimulate critical algorithmic thinking and a sense of practicality. I believe that by telling a continuous story, the authors are able to engage the students and keep their interest throughout the entire project.

This book will without a doubt be a very attractive addition to the curriculum for middle-school students.

It certainly would have benefited me when I was in middle school.

Ronald L. Graham

University of California at San Diego

Preface

In the 1970s a new kind of code was discovered that changed the way people could send secret messages. It meant they didn't need to agree in advance about the details of the code they would use. This came at a good time because people were just starting to use the Internet, and this new kind of code, called a public key cipher, made it practical for businesses and for ordinary people to communicate securely.

One kind of public key cipher uses prime numbers. We were excited by the idea that kids could understand some of the topics involved in public key cryptography. Middle-grade students learn about prime numbers and factoring, so why not learn about how these topics are used today?

The more we thought about it, the more we realized there are many interesting ciphers that involve the kinds of mathematics middle-grade students know. One of these ciphers, which was used in battles long ago, involves nothing more than addition and subtraction. Another, the Vigenère Cipher, which was used during the Civil War and even into the twentieth century and was once believed to be unbreakable, can actually be cracked by today's middle-grade students (as long as the key isn't too long) by finding common factors of certain numbers.

We believe learning about cryptography will be an enjoyable way to explore mathematics. It appeals to the natural curiosity that people of all ages have for mysteries and secrets, and it comes with stories of how it has been used and misused throughout history. Along with the mathematics, we have included some of these stories—some tie in with what middle-grade students are learning in social studies and others simply are interesting to us.

We wrote this book so it could be used by teachers in classrooms and also by kids who want to learn about secret codes on their own or with friends. We tested it in Grades 5-8, in a variety of settings: regular math classes, gifted classes, remedial math classes, math clubs, after-school programs, a museum camp, and a cross-curricular class that integrated social studies, math, and language arts. Some students have read it on their own outside of school and some in a home-school setting. We found that students of all abilities enjoy the beginning chapters and advanced students and independent learners enjoy the challenge of the chapters near the end of the book.

If you don't have a class to work with, you can still read and enjoy this book. For class activities that involve sending messages to others or playing a game, you can substitute a friend for a class and send messages to each other. In some places, we give tips on how to modify the activities to do them alone, in case you can't find a friend who wants to work together.

Workbook and Teacher's Guide

A workbook is available to go along with this book. It contains the same problems as the book, but it gives you space to write your answers. We suggest using the workbook, since it avoids mistakes that might occur when you copy long messages onto your own paper.

A teacher's guide is available that contains suggestions for teaching and an answer key. For information about ordering a workbook or teacher's guide, contact the publisher, A K Peters, Ltd., at <http://www.akpeters.com>, or go to the Cryptoclub website.

Website

As we developed the book, we also developed a website to go with it:

<http://cryptoclub.math.uic.edu>

You can use the tools on the website to encrypt and decrypt messages. You can also collect data about the messages that will help you crack them. The computer will do the tedious work, and you can do the thinking. As you read a chapter, you should first solve the problems that are there. After you have worked with the short messages in those problems, you are ready to work with longer messages on the computer.

Besides tools for encrypting and decrypting, the website has an animated treasure hunt, message boards for sending secret messages, and programs for building factor trees and finding prime numbers. It will continue to grow, even after the book is published, so you should check back later for more activities and messages to crack.

The Cryptokids

The Cryptokids aren't exactly real kids, but some of the stories are based on things that really happened. Janet Beissinger's children are named Jenny, Dan, Tim, Abby, and Peter, and Vera Pless's grandchildren are named Evie, Lilah, Becky, and Jesse. A teacher really did read a note out loud to the class, to the dismay of one of the kids. The great-grandfather of Abby and Jenny's mother really did discover—and lose—silver along the Nipigon River (although he probably never wrote a secret message about it). Tim really did try to find an example for which $2 + 2$ is not always 4 , after being told he just had to accept the fact that some things are always true. And Jesse really did join the Cryptoclub after the rest of the kids—he was born while we were writing Unit 3.

As you read the book, listen to the conversations of the Cryptokids. They might ask each other some of the same things you are wondering about. You might imagine yourself talking with friends in the same way about how to solve problems. Their conversations reflect some of our own beliefs: that it is interesting to think about different ways to solve math problems and fun to look for ways to make problems easier. We enjoy working on a problem and solving it piece by piece. We feel good when we finish. We hope you will too.

Acknowledgments

The authors thank the following people for their help in the development of this book:

Artist

Daria Tsoupikova
School of Art and Design
Electronic Visualization Laboratory
University of Illinois at Chicago

Project Evaluators

Kyungsoon Jeon
Linda Schembari
Cynthia Mayfield

Website Developers

Rong Zeng
Yu Huang
Dov Kaufman

Mathematics Consultant

Jeremy Teitelbaum
Department of Mathematics,
Statistics and Computer Science
University of Illinois at Chicago

Mathematics Education Consultant

Andy Isaacs
Center for Elementary Mathematics
and Science Education
University of Chicago

Field Test Teachers

We thank the following teachers who tested drafts of various portions of the book and gave us feedback. Their suggestions have been very helpful.

Lynne Beauprez
Brooks Middle School
Oak Park, Illinois

Cathy Blake
Yeoukm Middle School
Belton, Missouri

Sharlene Britt
Carson Elementary School
Chicago, Illinois

Mary Cummings
Yeoukm Middle School
Belton, Missouri

E. Michael Einhorn
Nash Elementary School
Chicago, Illinois

David Genge
Stowe School
Chicago, Illinois

Katherine Grzesiak
Eastlawn Elementary School
Midland, Michigan

Deborah Jacobs-Sera
Greater Latrobe Jr. High
Latrobe, Pennsylvania

Jamae Jones
Foster Park Elementary School
Chicago, Illinois

Stacy Kasse
Taunton Forge School
Medford, New Jersey

Catherine Kaduk
Ranch View School and
River Woods School
Naperville, Illinois

Kristen Kainrath
Prairie School
Naperville, Illinois

John King
Henry Nash Elementary School
Chicago, Illinois

Erin Konig
Carson Elementary School
Chicago, Illinois

Susan Linas
George Washington Middle School
Lyons, Illinois

Reshma Madhusudan
Young People's Project
Chicago, Illinois

Robin Masters
Frances W. Parker School
Chicago, Illinois

Bridget Rigby
Tech Museum of Innovation
San Jose, California

Mary Rodriguez
Lara Academy
Chicago, Illinois

Kathryn Romain
Central Middle School
Midland, Michigan

Patricia Smith
Medill Elementary School
Chicago, Illinois

John Stewart
Carson Elementary School
Chicago, Illinois

Patricia Ullestad
River Woods School
Naperville, Illinois

Denise Wilcox
Fredrick Elementary School
Grayslake, Illinois

Noreen Winingham
Orrington Elementary School
Evanston, Illinois

Kam Woodard
Young Women's Leadership Academy
Chicago, Illinois

Students

The following students independently read and sent us comments on a draft of the book. We appreciate their suggestions.

Eva Huston

Adam Jacobson

Production

We thank Erika Larson who prepared several drafts of the book and workbook, and Henrique Cirne-Lima who drafted some of the figures.

We thank Carolyn Artin for her expert editing of the manuscript and for her several suggestions for improving it.

We also thank Klaus Peters and the staff at A K Peters, particularly Charlotte Henderson in the editorial department and Erica Schultz, the production manager. They have been a pleasure to work with.

Unit I



Introduction to Cryptography

Chapter 1



Caesar Ciphers

Abby wrote a note to her friend Evie. She folded it up tightly so no one else could read it and passed it to Evie when she thought nobody was looking. Unfortunately for the girls, their teacher was looking. She took the note away and read it out loud to the whole class.

Abby was mortified. If only she had known how to use cryptography! Then she could have sent the message in a secret code and avoided all of this embarrassment.

What Is Cryptography?

Cryptography is the science of sending secret messages. People have been sending secret messages for thousands of years. Soldiers send them so the enemy won't know their plans; friends send them when they want to keep their notes private; and, today, people shopping on the Internet use them to keep their credit card numbers secret.

People often use the term "secret code" to mean a method for changing a message into a secret message. A very simple secret code was used in Boston in 1776 to send a message to Paul Revere about how the British were coming. The code involved the number of lanterns hung in the church bell tower: "One if by land, two if by sea."

plaintext:	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
ciphertext:	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 C

Caesar cipher with a shift of 3.

PROBLEMS

(Workbook page W1)

1. Try it yourself!

a. Encrypt “keep this secret” using a Caesar cipher with a shift of 3.

b. Encrypt your teacher’s name with a shift of 3.

2. Decrypt the answers to the following riddles. They were encrypted using a Caesar cipher with a shift of 3.

a. **Riddle:** What do you call a sleeping bull?

Answer:

D EXOOGRCHU

b. **Riddle:** What’s the difference between a teacher and a train?

Answer:

WKH WHDFKHU VDBV

“QR JXP DOORZHG.”

WKH WUDLQ VDBV

“FKHZ FKHZ.”

In cryptography, the word **cipher** is used to mean a particular type of secret code that changes each letter of a message into another letter or symbol. One of the oldest ciphers is named after Julius Caesar, who used this type of cipher to exchange messages with his Roman generals more than 2,000 years ago.

In a **Caesar cipher**, the alphabet is shifted a certain number of places and each letter is replaced by the corresponding shifted letter. For example, shifting the alphabet 3 spaces to the left gives the Caesar cipher shown above.

This cipher changes **a** to **D**, **b** to **E**, and so on. For example, using this cipher, Abby’s name becomes DEEB:

Abby

DEEB

Changing a message to a secret message is called **encrypting**. Figuring out the original message from the encrypted (secret) message is called **decrypting**.

A message before it is encrypted is called the **plaintext**. An encrypted message is called the **ciphertext**. To avoid confusion, we will write plaintext in lowercase letters (except at the beginning of sentences or names). We’ll write ciphertext in uppercase letters.

 **Do Problems 1 and 2 now.**

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

Caesar cipher with a shift of 4.

To confuse anyone who might find your notes, you can shift the alphabet any number of spaces. The Caesar cipher above is a shift of 4 spaces.

Do Problems 3 and 4 now.

CLASS ACTIVITY: Play Cipher Tag

Choose someone to be “It”. “It” goes to the board, writes an encrypted name or message, and tells the class what shift was used for the encryption. The first person to decrypt the name becomes the new “It” and writes a new encrypted name or message on the board.

PROBLEMS (Workbook page W2)

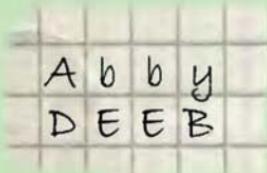
3. Decrypt the following note Evie wrote to Abby. She used a Caesar cipher with a shift of 4 like the one above.

WSVVC. PIX'W YWI GMTLIVW JVSQ RSA
SR.

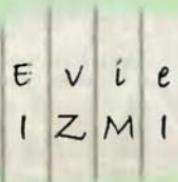
4. Use a shift of 3 or 4 to encrypt someone’s name. It could be someone in your class or school or someone your class has learned about. (You’ll use this to play Cipher Tag.)

★ TIP

You can use graph paper to write messages. Put one letter in each box.



Lined paper is good, too. Turn it sideways, and the lines make columns to write the letters in.



★ TIP: Using a Cipher Wheel

- Plaintext on outer wheel (lowercase)
- Cipher text on inner wheel (uppercase)
- Turn inner wheel counterclockwise

PROBLEMS (Workbook page W3)

5. Try it yourself!

- a. Encrypt “private information” using a cipher wheel with a shift of 5.
- b. Encrypt your school’s name using a cipher wheel with a shift of 8.

Use your cipher wheel to decrypt the answer to the following riddle:

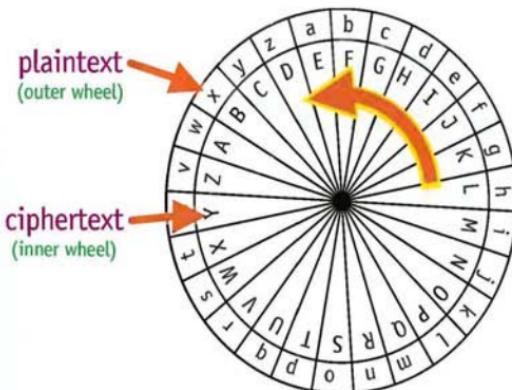
6. **Riddle:** What do you call a dog at the beach?

Answer (shifted 4):

E LSX HSK.

Cipher Wheels

To be able to change a cipher quickly, you can use a **cipher wheel**, like the one below. Then you can easily shift the alphabet any amount by turning the inner wheel.



A cipher wheel with a shift of 4.

CLASS ACTIVITY: Making a Cipher Wheel

Use the cipher wheel circles in the Workbook or on page 199 of this book, or make a copy of the circles on the inside back cover.

Cut out the circles to make a cipher wheel. Put the small circle on top and fasten the two circles together by putting a brad through their centers. (*Make sure the brad goes through the exact centers, or the wheel might not work very well.*)

Do Problems 5–9 now.

PROBLEMS (Workbook pages W3-W4)

Use your cipher wheel to decrypt the answers to the following riddles:

- 7. Riddle:** Three birds were sitting on a fence. A hunter shot one. How many were left?

Answer (shifted 8):

VWVM. BPM WBPMZA
NTME IEIG.

- 8. Riddle:** What animal keeps the best time?

Answer (shifted 10):

K GKDMRNYQ

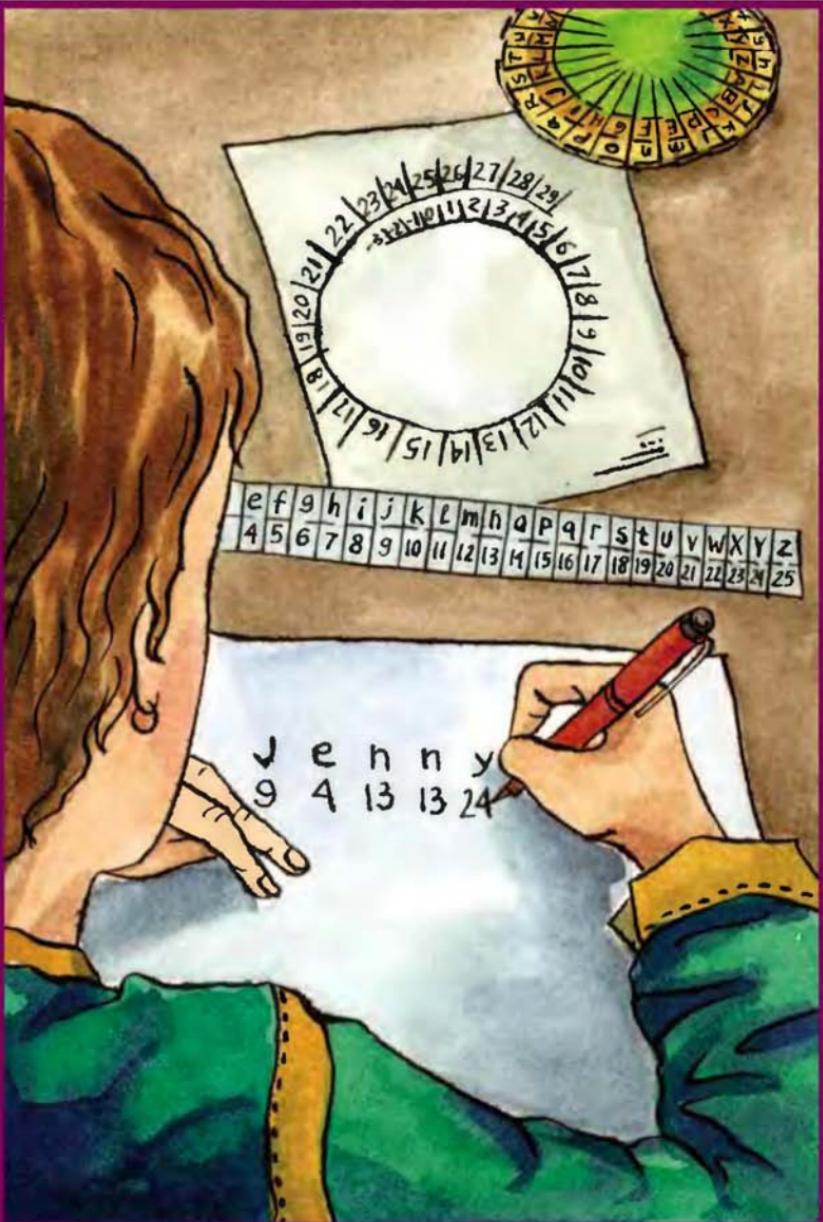
- 9.** Write your own riddle and encrypt the answer. Put your riddle on the board or on a sheet of paper that can be shared with the class later on. (Tell the shift.)

DO YOU KNOW? Little Orphan Annie and Captain Midnight

In the late 1930s, kids gathered around their radios after school to hear the latest stories about Little Orphan Annie, a red-headed orphan who had many exciting adventures, accompanied by her dog Sandy. The episodes continued from one day to the next, and if you wanted to know what would happen in the next episode, you could decode clues using the Little Orphan Annie decoder, which she called a Code-O-Graph. This was a cipher wheel, like the one in this book, which you could get by sending in labels from boxes of Ovaltine.

After Little Orphan Annie went off the air, the Ovaltine company sponsored a radio show about the crime-fighting Captain Midnight. Captain Midnight's helper also had a Code-O-Graph, which he used to send messages to Washington. Listeners who sent away for the Code-O-Graph became members of Captain Midnight's Secret Squadron of crime fighters. They could decrypt messages broadcast by the show's announcer about the next program.

Chapter 2



Sending Messages with Numbers

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cipher strip.

Other kids in school sent secret messages. Jenny was one of them. She liked to encrypt messages by changing letters to numbers. She let **0** represent **a**, **1** represent **b**, **2** represent **c**, etc.

Changing letters to numbers, Jenny encrypted her name like this:

J e n n y
9 4 13 13 24

CLASS ACTIVITY: Pass the Hat

- Use the number method to encrypt your teacher's name. Compare your answer with the rest of the class.
- Use the number method to encrypt your name. Put your encrypted name in a "hat" that your teacher provides.
- Pass the hat around and pull a name from it. Decrypt the name and return it to its owner.

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
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2

Cipher strip with a shift of 3.

PROBLEMS

(Workbook page W5)

1. Decrypt the following riddles using Jenny's method.

- a. **Riddle:** What kind of cookies do birds like?

Answer:

2, 7, 14, 2, 14, 11, 0, 19, 4
2, 7, 8, 17, 15

- b. **Riddle:** What always ends everything?

Answer:

19, 7, 4

11, 4, 19, 19, 4, 17 6

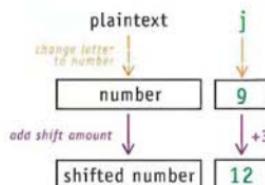
2. a. Encrypt "James Bond" using the cipher strip on page 9.
 b. Encrypt "James Bond" using the cipher strip above that is shifted three places.
 c. Describe how you can use arithmetic to get your answer to 2b from your answer to 2a.

Do Problem 1 now.

Jenny used her number method to encrypt messages for a while, but then she realized it would be very easy for someone else to figure out her method. When she heard about Caesar ciphers, she decided to combine them with her number method. She shifted the numbers on her strip three places and got the cipher shown above.

Do Problem 2 now.

Jenny realized that she didn't need a cipher wheel to use Caesar ciphers with numbers—all she needed was arithmetic. To encrypt the letter j, she followed this flowchart:



To encrypt her brother's name, Daniel, with a shift of 4, Jenny changed letters to numbers and added 4:

plaintext:	D	a	n	i	e	l
numbers:	3	0	13	8	4	11
shifted numbers:	7	4	17	12	8	15

Do Problem 3 now.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

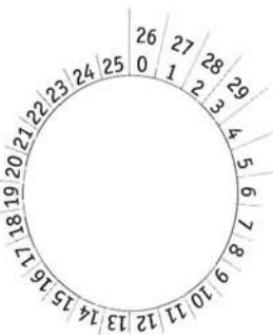
0 1 2

Numbers Greater than 25

Jenny started to use addition to encrypt her name with a shift of 3, but the **y** gave her trouble. She saw that **y** corresponds to 24, but $24 + 3 = 27$. “What do I do now?” she wondered. “My strip doesn’t have 27 on it.” The cipher strip shifted 3 on page 10 shows that **y** should be encrypted as 1.

“I get it,” said Jenny. “On the strip, the numbers only go up to 25. Then they start again with 0, 1, and so on. So 27 must be the same as 1.”

It helped Jenny to think of the numbers as wrapping around a circle:



Numbers that wrap around the circle to the same position are **equivalent**, or **congruent**, to each other. So, 26 is equivalent to 0, 27 is equivalent to 1, and so on.

Do Problems 4–6 now.

PROBLEMS

(Workbook page W6)

3. Encrypt each word with the given shift.
 - a. Lincoln; shift 4
 - b. Luke; shift 5
 - c. experiment; shift 3

What is different about encrypting the letter **x**?

4. What numbers between 0 and 25 are equivalent to the following numbers?
 - a. 28
 - b. 29
 - c. 30
 - d. 34
 - e. 36
 - f. 52

5. Describe an arithmetic pattern that tells how to match a number greater than 25 with an equivalent number between 0 and 25.

6. Encrypt each word by adding the given amount. Your numbers should end up between 0 and 25.
 - a. x-ray; add 4
 - b. cryptography; add 10

PROBLEMS (Workbook page W7)

7. Here is how Jenny encrypted the name of one of her friends by adding 3:

14, 11, 14, 3, 10.

Decrypt to find the name.

8. **Riddle:** Why doesn't a bike stand up by itself?

Answer (encrypted by adding 3):

11, 22, 21, 22, 25, 17

22, 11, 20, 7, 6

9. **Riddle:** What do you call a monkey who loves to eat potato chips?

Answer (encrypted by adding 5):

5, 7, 12, 13, 20

17, 19, 18, 15

10. **Riddle:** What is a witch's favorite subject?

Answer (encrypted by adding 7):

25, 22, 11, 18, 18, 15, 20, 13

11. **Challenge.** This is a name that was encrypted by adding 3:
22, 11, 15, 15, 1.

a. Decrypt by subtracting.

b. What happens to the 1?
What can you do to fix the problem?

To decrypt her Caesar number messages, Jenny only needed to subtract. If she added three to encrypt, she could decrypt by subtracting three. For example, she would decrypt 12 as $12 - 3 = 9$, which corresponds to the letter j.

 **Do Problems 7–11 now.**

Negative Numbers

Abby encrypted her name by adding 6. (Encrypting the y gave her 30, but she replaced that with 4, which is equivalent to 30 when the numbers wrap around.)

A	b	b	y
0	1	1	24
6	7	7	30

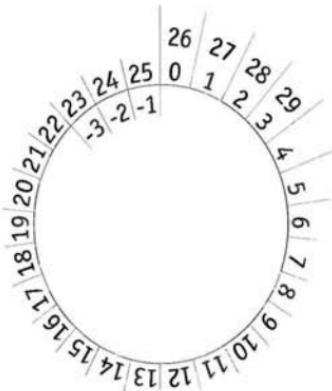
Jenny started to decrypt Abby's numbers by subtracting 6, but decrypting the number 4 gave her trouble. She subtracted:

$$4 - 6 = -2$$

"What do I do now?" she wondered. "What letter matches -2?"

Working with ciphers involves the numbers from 0 to 25. Numbers outside this range wrap around to match equivalent numbers between 0 and 25. This was true for numbers greater than 25, and it is also true for numbers less than 0.

Jenny knew that counting back two from 0 gives -2. Since 0 is equivalent to 26, she counted back two from 26 and saw that -2 is the same as 24. Since 24 matches **y** on the cipher strip, she concluded that the 4 in Abby's numbers decrypted to **y**.



Do Problems 12–16 now.

PROBLEMS (Workbook page W8)

- 12.** What numbers between 0 and 25 are equivalent on the circle to the following numbers?
 - a. 26
 - b. 28
 - c. -1
 - d. -2
 - e. -4
 - f. -10
- 13.** Describe an arithmetic pattern that tells how to match a number less than 0 with an equivalent number between 0 and 25.
- 14.** Decrypt by subtracting.
Replace negative numbers with equivalent numbers between 0 and 25.
 - a. 18, 11, 2, 2, 3 (subtract 3)
 - b. 3, 10, 7, 18 (subtract 10)
 - c. 7, 4, 13 (subtract 15)
- 15. Riddle:** What do you call a chair that plays guitar?
Answer (encrypted by adding 10):
10 1, 24, 12, 20, 14, 1
- 16. Riddle:** How do you make a witch itch?
Answer (encrypted by adding 20):
13, 20, 4, 24 20, 16, 20, 18
1, 24, 11 16

Making Calculations Easier

Abby and Jenny both agreed that decrypting was more of a bother when the subtraction gave negative numbers. They decided to look for a clever way to avoid this situation. They looked at the riddle from Problem 16 for an example of a calculation that had involved negative numbers.

Jenny reviewed the steps: "In the riddle about making the witch itch, the answer was encrypted by adding 20. So we decrypted it by subtracting 20. For example, to decrypt the number 13, we had to compute $13 - 20 = -7$."

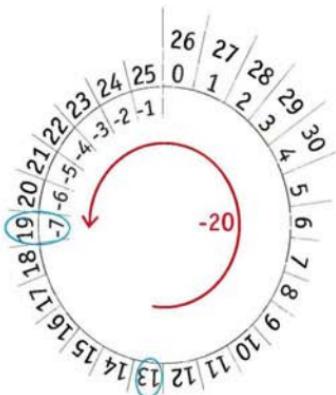
"I didn't like that," said Abby, "because, after subtracting, I had to do more work—I had to add 26 to get a number between 0 and 25."

"Work isn't so bad," said Jenny, "but I feel clever when I look for shortcuts."

"It might help to look at our numbers wrapped around on the circle," said Abby.

"Let's see," said Jenny. "We started at 13 and went back 20—that's counterclockwise—until we got to -7, which was the same as 19."

"I'm with you," said Abby. "Subtracting is like going counterclockwise around the circle."



"But we could also get from 13 to 19 by going the other direction—clockwise—around the circle. That is like adding." Jenny liked this idea.

"You mean we have a choice? We could add or subtract? How could that be?" asked Abby.

"It's because we're on a circle, not the regular number line."

"OK. So subtracting 20 is the same as adding 6—on a circle with 26 numbers." Abby was still a little cautious. "Let's try another example."

"Let's look at the word 1, 24, 11 in that 'witch itch' riddle," suggested Jenny. "To decrypt it, we could subtract 20 or add 6."

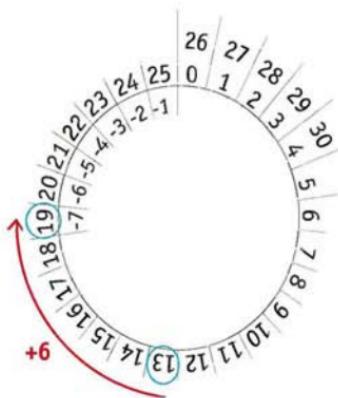
"But which should we do?" Abby wondered. "If we add 6, then it is easier to decrypt the 1 and 11, but it is harder to decrypt the 24."

"We don't have to do each letter the same way," said Jenny. "Decrypt the 1 and 11 by adding 6, but decrypt the 24 by subtracting 20. Both ways give us the same answer. For each letter we'll choose the method that makes our calculation easier."

 **Do Problems 17–23 now.**

CLASS ACTIVITY: Play Cipher Tag (see directions on page 5)

This time use messages with numbers, and choose a phrase or expression to encrypt instead of a name. For example, "Quick as lightning" or "A penny saved is a penny earned" would be good phrases to encrypt.



PROBLEMS (Workbook page W9-W10)

- 17.** **a.** To decrypt the riddle in Question 15, you could subtract 10. What number could you add to get the same answer as subtracting 10?
- b.** Decrypt the riddle in Question 15 again, adding or subtracting as necessary to avoid negative numbers and numbers greater than 25.
- 18.** **a.** Suppose that you encrypted a message by adding 9. Tell two different ways you could decrypt it.
- b.** This message was encrypted by adding 9. Decrypt by adding or subtracting to avoid negative numbers and numbers greater than 25.
- 5, 13 16, 9, 4, 13 14, 23, 3, 22, 12 9
1, 16, 23, 0, 2, 11, 3, 2.
- 19.** **a.** Suppose that you encrypted a message by adding 5. Tell two different ways you could decrypt it.
- b.** In general, suppose that you encrypted a message by adding an amount n . Tell two different ways you could decrypt it.

For Questions 20–23, add or subtract as necessary to make your calculations simplest.

- 20. Riddle:** Imagine that you're trapped in a haunted house with a ghost chasing you. What should you do?

Answer (encrypted by adding 10):

2, 3, 24, 25 18, 22, 10, 16, 18, 23, 18, 23, 16

- 21. Riddle:** Why must a doctor control his temper?

Answer (encrypted by adding 11):

12, 15, 13, 11, 5, 3, 15 18, 15 14, 25, 15, 3, 24, ' 4
7, 11, 24, 4 4, 25 22, 25, 3, 15 18, 19, 3
0, 11, 4, 19, 15, 24, 4, 3

PROBLEMS

(Workbook page W11)

- 22. Riddle:** What is the meaning of the word "coincide"?

Answer (encrypted by adding 7):

3, 14, 7, 0 19, 21, 25, 0 22, 11, 21, 22, 18, 11 10, 21

3, 14, 11, 20 15, 0 24, 7, 15, 20, 25

- 23.** Abby was learning about life on the frontier. "Peter," she said, "Where is the frontier?"

Decrypt Peter's reply (encrypted by adding 13):

6, 20, 13, 6, 5 13 5, 21, 24, 24, 11 3, 7, 17, 5, 6, 21, 1, 0 .

11, 1, 7 1, 0, 24, 11 20, 13, 8, 17 13 24, 17, 18, 6

17, 13, 4 13, 0, 16 13 4, 21, 19, 20, 6 17, 13, 4.

DO YOU KNOW?

Beale Ciphers and a Buried Treasure

Legend has it that in 1817 Thomas J. Beale and 29 others discovered and mined a large quantity of gold and silver north of Sante Fe, New Mexico. Beale buried it for safekeeping near Bedford, Virginia. Foreseeing the possibility that he might not return, he left a locked iron box with a friend named Robert Morrissey and instructed Morrissey to open it if he did not return in ten years. Morrissey waited twenty-three years, then finally opened the box. He found a letter from Beale in plain English and three pages of numbers believed to be encrypted messages. The letter told how the treasure was found and explained that the first page of numbers describes the location where Beale buried it, the second describes the treasure itself, and the third tells the names of the relatives of the men who should share the treasure.

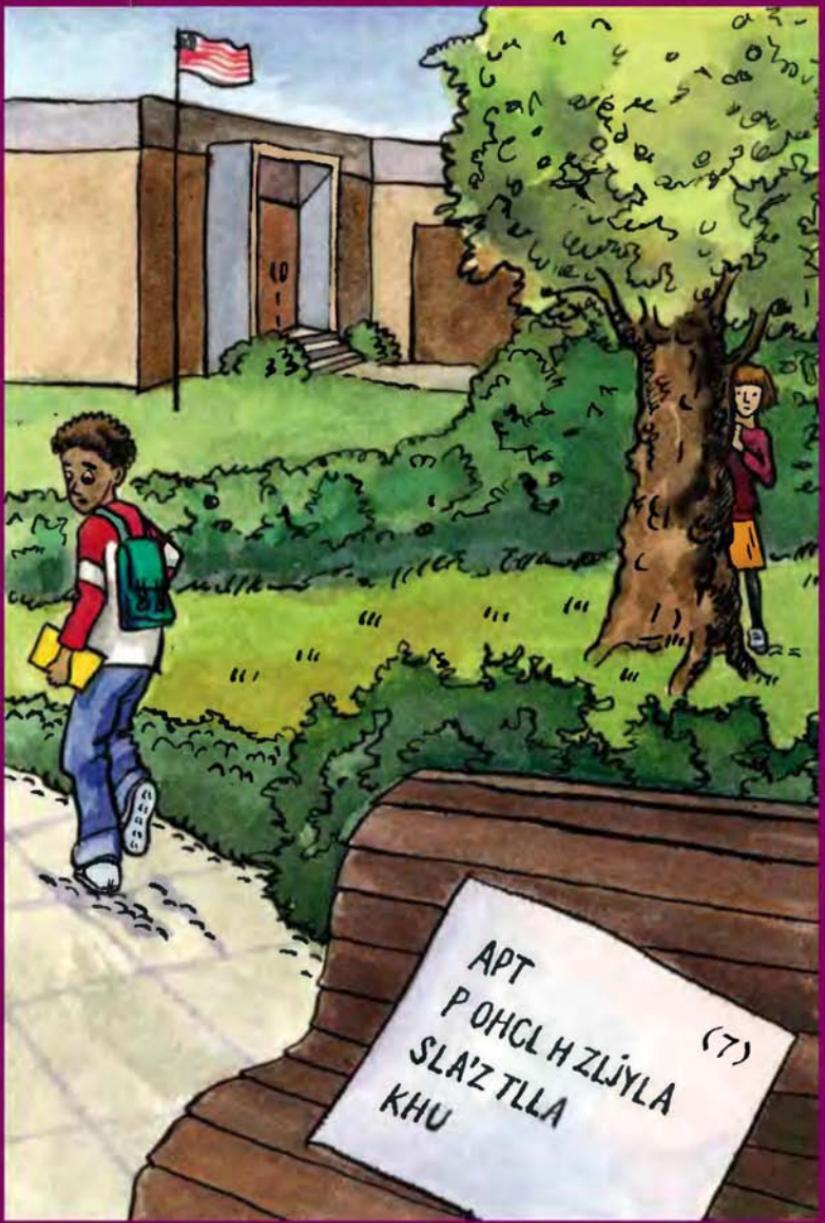
Morrissey tried for many years to decrypt the pages of numbers. Finally, in 1862, at the age of 84, he entrusted his secret to a friend. The friend then spent much of his life and money trying to decrypt the pages but he was only able to decrypt the second page, the one that lists the contents of the treasure. That page told of a first deposit that included 1014 pounds of gold and 3812 pounds of silver and a later deposit that included 1907 pounds of gold, 1288 pounds of silver, and jewels that Beale had obtained in exchange for some of the silver. Unfortunately, Morrissey's friend was unable to decrypt the page telling the location of this treasure. After years of frustration, he wrote an anonymous pamphlet describing

CONTINUED ON NEXT PAGE >

the ciphers and his decryption of the second page so that others could try to decrypt the remaining pages.

The mystery of the Beale Ciphers has generated a lot of interest over the years. Some people claim it is a hoax, but many people, including some professional cryptographers, think it is real.

Chapter 3

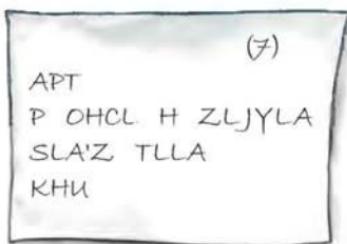


Breaking Caesar Ciphers

The idea of using ciphers to send messages spread around the school quickly. The kids thought this was a great way to pass notes that no one else would be able to read. Dan learned about Caesar ciphers and encrypted a message to Tim by shifting 7. He wrote the number 7 at the top of the note so that Tim would know how to decrypt the message.

Unfortunately, Evie found the note. She assumed they had used a Caesar cipher and she figured out that 7 was the shift amount. She used it like a key and unlocked their message. The boys realized they should keep their key secret. That way, someone who guessed that they had used a Caesar cipher to encrypt a message, wouldn't be able to decrypt it.

The kids had discovered a basic idea of cryptography: You might as well assume that anyone who finds your secret message will be able to guess the method you used to encrypt it. You need something else—a key—to keep the message secret. A cipher system really has two parts: the **algorithm** (method) for encrypting and a **key** that tells an extra detail to use in the algorithm. In a Caesar cipher system, the algorithm for encrypting is to shift the letters (or add) a chosen number of places. The key is the specific number of places to



Dan's note to Tim.

PROBLEMS (Workbook page W13)

1. Decrypt Dan's note to Tim.
2. Decrypt Dan's second note to Tim.

PROBLEMS (Workbook page W14)

3. Decrypt the answers to the following riddles by first figuring out the keys. Let the one-letter words help you.

a. **Riddle:** What do you call a happy Lassie?

Answer:

E NSPPC GSPPMI

b. **Riddle:** Knock, knock.

Who's there?

Cash.

Cash who?

Answer:

O QTKC EUA CKXK YUSK

QOTJ UL TAZ

c. **Riddle:** What's the noisiest dessert?

Answer:

W GQFSOA

4. Decrypt the following quotation:

HS RSX ASVVC EFSYX
CSYV HMJJMGYPXMIW
MR QEXLIQEXMGW,
M EWWYVI CSY XLEX
QMRI EVI KVIEXIV.

—Albert Einstein

shift. When you think someone has figured out your cipher system, you might not have to change your system entirely—you can simply change your key.

Dan and Tim changed their key and, confident that they could keep their messages private by keeping their keys secret, Dan sent another note to Tim.

M PMOI IZMI,
FYX HSR'X XIPP
LIV M WEMH WS.

Dan's second note to Tim.

Unfortunately for the boys, Evie was too clever for them. Even though Dan didn't include the key with his message, she was able to figure it out. She decrypted the whole message, but gasped when she read what it said.

Can you think how she might have figured out their key?

☞ **Do Problems 1 and 2 now.**

Breaking Caesar Ciphers

Evie realized that there were only a few letters that could be the one-letter word in Dan's message. (What letters can be one-letter words in English?) She figured out what shifts would give those letters and she tried those shifts as possible keys. When she got a few words that made sense, she knew she must have found the key.

☞ **Do Problems 3 and 4 now.**

Tim and Dan were determined to send messages the girls couldn't break, so they took out the spaces between the words:

EWWLHWLWJSFVEWLGFAYZLSLGMJKWUJWLHDSUW.

AZSNWKGEWLZAFYWDKWLGLWDDQGM.

The girls found the note.

"There aren't any spaces between words," said Lilah. "They took out the clues."

"Don't give up," said Evie. "We only have to match one letter—the wheel will tell us the rest. Once we know the letters, we can figure out where the spaces go."

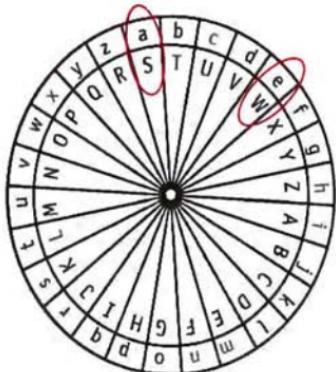
"Do we have to try every possible shift of the wheel?" Lilah wondered.

"No. We can be more clever than that," said Evie. "I once heard that **e** is the most common letter in English. Let's find the most common letter in the message and match it with **e**."

She made a tally of the letters in the message (*right*).

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

Evie's alphabet tally.



The a-to-S wheel.

"W occurs most often," she said. "Let's turn the wheel so e matches W."

They did that and got the a-to-S wheel (left).

"Look! Here is the boys' message!" Evie said.

Meet peter and me tonight at our secret place.
I have something else to tell you.

"We can read it even without the spaces."

Evie's method works, but not always. If matching e with the most common letter doesn't give a message that makes sense, you can try matching it with other common letters.

Do Problems 5–10 now.

PROBLEMS (Workbook page W15)

Decrypt each of the following quotations. Tell the key used to encrypt.

5. PKB KXN KGKI DRO LOCD ZBSJO DRKD VSPO YPPOBC SC DRO
MRKXMO DY GYBU RKBN KD GYBU GYBDR NYSXQ.
—Theodore Roosevelt
6. JAJS NK DTZ'WJ TS YMJ WNLMY YWFHP, DTZ'QQ LJY WZS TAJW
NK DTZ OZXY XNY YMJWJ.
—Will Rogers

PROBLEMS

(Workbook pages W16-W17)

Decrypt each of the following quotations. Tell the key used to encrypt.

7. RCAB JMKICAM AWUMBPQVO LWMAV'B LW EPIB GWC XTIVVML
QB BW LW LWMAV'B UMIV QB'A CAMTMAA.

—Thomas A. Edison

8. QBA'G JNYX ORUVAQ ZR, V ZNL ABG YRNQ. QBA'G JNYX VA
SEBAG BS ZR, V ZNL ABG SBYYBJ. WHFG JNYX ORFVQR ZR NAQ
OR ZL SEVRAQ.

—Albert Camus

9. OCPAQHNKHG'UHCKNWTGUCTGRGQRNGYJQFKFPQV
TGCNKBGJQYENQUGVJGAYGTGVQUWEEGUUYJGPVJGAICXGWR.

—Thomas Edison

10. Challenge.

16, 14, 23, 18, 4, 2 18, 2 24, 23, 14 25, 14, 1
12, 14, 23, 3 18, 23, 2, 25, 18, 1, 10, 3, 18, 24, 23
23, 18, 23, 14, 3, 8 23, 18, 23, 14 25, 14, 1
12, 14, 23, 3 25, 14, 1, 2, 25, 18, 1, 10, 3, 18, 24, 23.

—Thomas A. Edison

DO YOU KNOW?

Navajo Code Talkers

Navajo "Code Talkers" played an important role for the United States during World War II. A group of Navajo men developed a secret code based on the Navajo language. They first made up simple English words to represent military words, and then translated those words into Navajo. This way, "submarine" became "iron fish," which was translated to "besh-lo." Other words were spelled out using words instead of letters: the letter "a" could be represented by the English word "ant," then translated into "wol-lachee." They used this code to communicate secret messages by radio and telephone among American troops. The Navajo language was only spoken by a few people besides the small number of Navajos, so it worked well.

The Code Talkers took part in every assault the U.S. Marines conducted in the Pacific from 1942 to 1945. They grew in number from 29 to 400. They were so valuable that each was given a bodyguard for protection. High-ranking military officers have said that without the Navajos, there would not have been a U.S. victory at Iwo Jima and World War II might have had a different outcome. After the war, the Japanese said they had been able to decipher the codes used by the U.S. Army and the Army Air Corps, but they were never able to crack the code used by the Marines.

Because of its potential for future use, the Navajo code was kept secret until 1968. The code talkers received little recognition at the time for the important role they had played in World War II. However, their story was finally made public. In 1982, the United States Government designated August 14 "National Code Talkers Day." In July 2001, more than fifty years after the war had ended, the twenty-nine Navajos who developed the code were honored with the Congressional Gold Medal. It was presented by the president of the United States to four of the five living developers and to the families of the others.

Unit 2



Letter	Relative frequency
A	6.5
B	1.9
C	1.9
D	1.9
E	1.9
F	1.9
G	1.9
H	1.9
I	1.9
J	1.9
K	1.9
L	1.9
M	1.9
N	1.9
O	1.9
P	1.9
Q	1.9
R	1.9
S	1.9
T	1.9
U	1.9
V	1.9
W	1.9
X	1.9
Y	1.9
Z	1.9

Substitution Ciphers

Chapter 4



Keyword Ciphers

Dan was very excited. He had heard that the Outdoor Club was planning a ski trip. But he worried that if his sister Jenny and her friends signed up first, there would not be enough spaces for his friends. He decided to reserve a spot for his sister but not tell her about it until after his friends had signed up.

In the meantime, he needed to send a message about the trip to his friends. He wanted to encrypt it so Jenny couldn't read it. But what cipher should he use? He remembered how Evie had broken his Caesar cipher and decrypted the embarrassing message he had sent to Tim. All she had to do was figure out one letter and she would know the size of the shift. He decided that the addition pattern in Caesar ciphers made them too easy to break.

"I want a cipher with no pattern at all," said Dan. "I'll scramble up the letters so no one can figure out my cipher."

Dan made the table below, which has no obvious pattern. It is a substitution cipher. In a **substitution cipher**, each letter of the alphabet substitutes for another letter. The Caesar cipher in Chapter 1 is also a substitution cipher, but its shift pattern makes it easy to break.

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

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

Keyword **DAN**, key letter **h**.

"The trouble with my substitution cipher is that it is too clumsy to use," said Dan. "How do I tell my friends what my substitutions are so they can decrypt my messages? I would have to write the whole table out for them."

Then Dan read about keyword ciphers and realized they would help with this problem. A **keyword cipher** is a type of substitution cipher whose substitution table uses a keyword. It has a pattern that lets it be described easily, but the pattern doesn't involve numbers so it is not as easy to break as a Caesar cipher.

In a keyword cipher, the sender chooses a **keyword** and a **key letter**. He writes the keyword under the alphabet, starting under the key letter. Then he writes the unused letters, in alphabetical order, wrapping around the alphabet until all letters are used. If a letter appears more than once in the keyword, he only writes it the first time it appears.

For example, the table above shows a cipher with keyword **DAN** and key letter **h**. The keyword **DAN** begins under the **h**. The rest of the alphabet follows in order.

Sometimes Dan's friends called him Danny. To use "Danny" as a keyword, he would have to cross out the second **n** and use **DANY**—otherwise there wouldn't be room in the table for all letters of the alphabet. The table below shows a keyword cipher with keyword **DANNY** and keyletter **h**.

 **Do Problems 1–7 now.**

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

Keyword **DANNY**, key letter **h**.

PROBLEMS

(Workbook pages W19-W20)

The following riddles were encrypted with keyword ciphers.

Decrypt the answers.

1. Keyword: DAN, Key letter: h

Riddle: What is worse than biting into an apple and finding a worm?

Answer: YAFWAFZ DTCY T PGJE.

2. Keyword: HOUSE, Key letter: m

Riddle: Is it hard to spot a leopard?

Answer: OU. CVQJ LAQ MUAO CVLC GLJ.

3. Keyword: MUSIC, Key letter: d

Riddle: What part of your body has the most rhythm?

Answer: VHPL UXMLP FN

4. Keyword: FISH, Key letter: a

Riddle: What does Mother Earth use for fishing?

Answer: TDA MNQTD FMH RNUTD ONKAR

5. Keyword: ANIMAL, Key letter: g

Riddle: Why was the belt arrested?

Answer: ZEH NEBXIDA OF KNY FUDKJ.

6. Keyword: RABBIT, Key letter: f

Riddle: How do rabbits travel?

Answer: WS BVKZHDVFZ

7. Keyword: MISSISSIPPI, Key letter: d

Riddle: What ears cannot hear?

Answer: IXLN HS ZHLG

PROBLEMS

(Workbook pages W21-W22)

8. Decrypt Dan's message. (It is a long message, so you may want to share the work with a group.)
9. Write a message to another group and encrypt it using a keyword cipher. Tell them your keyword and key letter so they can decrypt the message.

Dan told his friends about keyword ciphers. He told them that he would use a keyword cipher to send them a message when the trip details were finally announced. He called the park every day waiting for the announcement. Finally word of the trip came out.

Dan encrypted the message below and passed it around to his friends at school. As he handed it out, he told them the keyword was **SKITRIP** and the key letter was **p**. He was pretty sure no one else knew about keyword ciphers so they wouldn't know how to decrypt the message, even if they knew the keys.

 **Do Problems 8 and 9 now.**

OLIL FIL ROL JLRFQWT ZM ROL ZPRJZZI HWPG'T TVQ
RIQS: ROL RBZ-JFD RIQS RZ SQYL XZPYRFQY BQWW GL
TFRPIJFD FYJ TPYJFD, ROL MQITR BLLVLYJ QY MLGIPFID.
ROL GPT BQWW WLFA L MIZX ROL SFIV'T OLFJKPFIRLIT
FR LQNOR FX FYJ ILRPIY FR RLY SX TPYJFD.
ILNQTRIFRQZY MZIXT FIL JPL GD YLCR MIQJFD SQHV
ROLX PS QY ROL SFIV ZMMQHL.
ROL RIQS QT WQXQRLJ RZ ROL MQITR RBLYRD BOZ
TQNY PS, TZ SWLFTL OPIID ZI ROLIL XQNOR YZR GL
LYZPNO TSFHL.

DO YOU KNOW?

Dancing Men

Sir Arthur Conan Doyle, the author of the Sherlock Holmes mysteries, was very interested in cryptography. In fact, he put secret ciphers into several of his stories. In "The Adventure of the Dancing Men," the villain, Abe Slaney, uses a substitution cipher made from stick figures of dancing men, with each man's arms and legs positioned differently to represent a different letter. He uses this cipher to send threatening encrypted messages to his childhood sweetheart, Elsie. The messages are brought to Holmes, who figures out the meaning of some of the dancing men.

Holmes is too late to prevent a murder but tricks Slaney into returning to the scene of the crime, where he is arrested, by sending him the following message:



This is an example of a substitution cipher made by using symbols instead of letters. You can decrypt Holmes' message if you know that the symbols correspond to letters as shown below and that the flags are added to indicate the end of words.

a =		c =		e =		h =		m =	
n =		o =		r =		t =			

Chapter 5



Letter Frequencies

Dan carelessly left his note in his pants pocket, and his mother found it when she did the laundry. She left it next to the washing machine, where Jenny found it later that day. Jenny knew immediately that it was something she wanted to read, so she tried to crack the code. She figured out that **L** occurs most often in Dan's note and decided that the letter **L** was probably the encryption of **e**. She set her Caesar wheel so **e** matched **L**, but then the other letters didn't make sense. She tried a few other settings for the wheel but got nowhere.

"This can't be a Caesar cipher," Jenny said to herself. "It's probably some other kind of substitution cipher—maybe a keyword cipher. I'm determined to crack it."

Even though most substitution ciphers are not as easy to crack as Caesar ciphers, cryptographers can break them fairly easily. Jenny did some reading and learned what to do. After some effort, she cracked Dan's cipher and read about the ski trip. She got her friends to sign up before it was too late.

Dan and his friends were puzzled. How could Jenny have cracked Dan's message? The letters were all scrambled up. "OK, you win," they told her. "But tell us how you did it."

"It wasn't as hard as you might think," Jenny said. "I counted the number of times each letter occurred in your message and then compared that with data on how often letters occur in plain English."

The boys realized that, to keep up with Jenny, they had better find out how often letters occur in English.

The word **frequency** describes how many times something occurs. For example, the frequency of the letter **b** in the expression **abcb** is 2. The frequency of **b** in **ababcacfaeghikvndswq** is also 2, but in this second expression **b** is a lot less common than in the first. The **relative frequency** of **b** is a ratio that compares or relates the number of occurrences of **b** to the total number of letters.

$$\text{relative frequency} = \frac{\text{number of occurrences}}{\text{total number}}$$

You can express relative frequency as a fraction, decimal, or percent. For example, the relative frequency of **b** in **abcb** is $\frac{2}{4}$ or $\frac{1}{2}$. This is the same as 0.5 and 50%. It tells us that **b** occurs half, or 50%, of the time.

The relative frequency of **b** in **ababcacfaeghikvndswq** is $\frac{2}{20}$ or $\frac{1}{10}$. This is the same as 0.1 and 10%.

You can use a calculator to convert to decimals. The relative frequency of **b** in **axqyhib** is $\frac{1}{8}$. Use a calculator to divide.

$$\frac{1}{8} = 1 \div 8 = 0.125$$

To change 0.125 to percent, we multiply by 100 and get 12.5%. (Do you remember an easy way to multiply by 100?)

Sometimes you may have to round an answer. For example, the relative frequency of **b** in **bghjiesrtasfgb** is $\frac{2}{14}$. We use a calculator to change this to a decimal and then round:

$$\begin{aligned}\frac{2}{14} &= 2 \div 14 \\&= 0.14285714286 \\&\approx 0.143\end{aligned}$$

To change 0.143 to percent, multiply by 100 and get 14.3%.

Dan and Peter decided to collect some data to learn about the relative frequency of letters in English. To share the work, they asked several friends to count letters in small samples of text and then combined it all into one big table.

CLASS ACTIVITY: Finding Relative Frequencies of Letters in English (Workbook pages W23–W24)

(Note: If you are working alone without a class, you can collect the data yourself. Choose a larger sample—around 500 letters. Then skip Parts 1 and 2 and enter your data directly into the table of Part 3.)

Part 1. Collecting data from a small sample.

- Choose about 100 letters from a newspaper or other English text.
- Work with your group to count the As, Bs, etc., in your sample.
- Enter your data in a letter frequency table.

Part 2. Combining data to make a larger sample.

- Record your group's data from Part 1 on your class's Class Letter Frequencies table. (Your teacher will provide this table on the blackboard, overhead, or chart paper.)
- Your teacher will assign your group a few rows to add. Enter your sums in the group table.

Letter	Frequency
A	10
B	2
C	3
D	5

Sample letter frequencies.

Letter	Class Letter Frequencies										Total for all groups
	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6	Group 7	Group 8	Group 9	Group 10	
A	10	9	6	5	8	8	10	12	4	6	78
B											
C											

Sample class data for letter A.

Discuss:

- What was the most common letter in your combined class data?
- Was this letter the most common for every group's data?
- What are other common letters? Do most groups have similar results?

		Relative Frequency		
Letter	Frequency	Fraction	Decimal (to 3 places)	Percent (%) (to nearest tenth)
A	78	$78/1059$.074	7.4
B				
C				
D				

Sample relative frequency of letter A (based on class letter total 1059).

Part 3. Computing relative frequencies.

Enter your class's combined data from the "Total for all groups" column of Part 2 into the "Frequency" column of the Relative Frequency table. Then compute the relative frequencies for the class data as fractions, decimals, and percents.

 **Do Problems 1–4 now.**

PROBLEMS (Workbook page W25)

1. a. What percent of the letters in the class sample were the letter T?
b. About how many Ts would you expect in a sample of 100 letters?
c. If your sample was about 100 letters, was your answer to 1b close to the number of Ts you found in your sample?
2. a. What percent of the letters in the class sample were the letter E?
b. About how many Es would you expect in a sample size of 100?
c. About how many Es would you expect in a sample of 1000 letters?
3. Arrange the letters in your class table in order, from most common to least common.
4. The table on the next page shows frequencies of letters in English computed using a sample of about 100,000 letters. How is your class data the same as the data in that table? How is it different? Why might it be different?

Letter	Relative frequency (%)
e	12.7
t	9.1
a	8.2
o	7.5
i	7.0
n	6.7
s	6.3
h	6.1
r	6.0
d	4.3
l	4.0
c	2.8
u	2.8
m	2.4
w	2.4
f	2.2
g	2.0
y	2.0
p	1.9
b	1.5
v	1.0
k	0.8
j	0.2
q	0.1
x	0.1
z	0.1

Letters in English.¹

¹ H. Beker and F. Piper. *Cipher Systems: The Protection of Communications*. Northwood Publications, London, 1982.

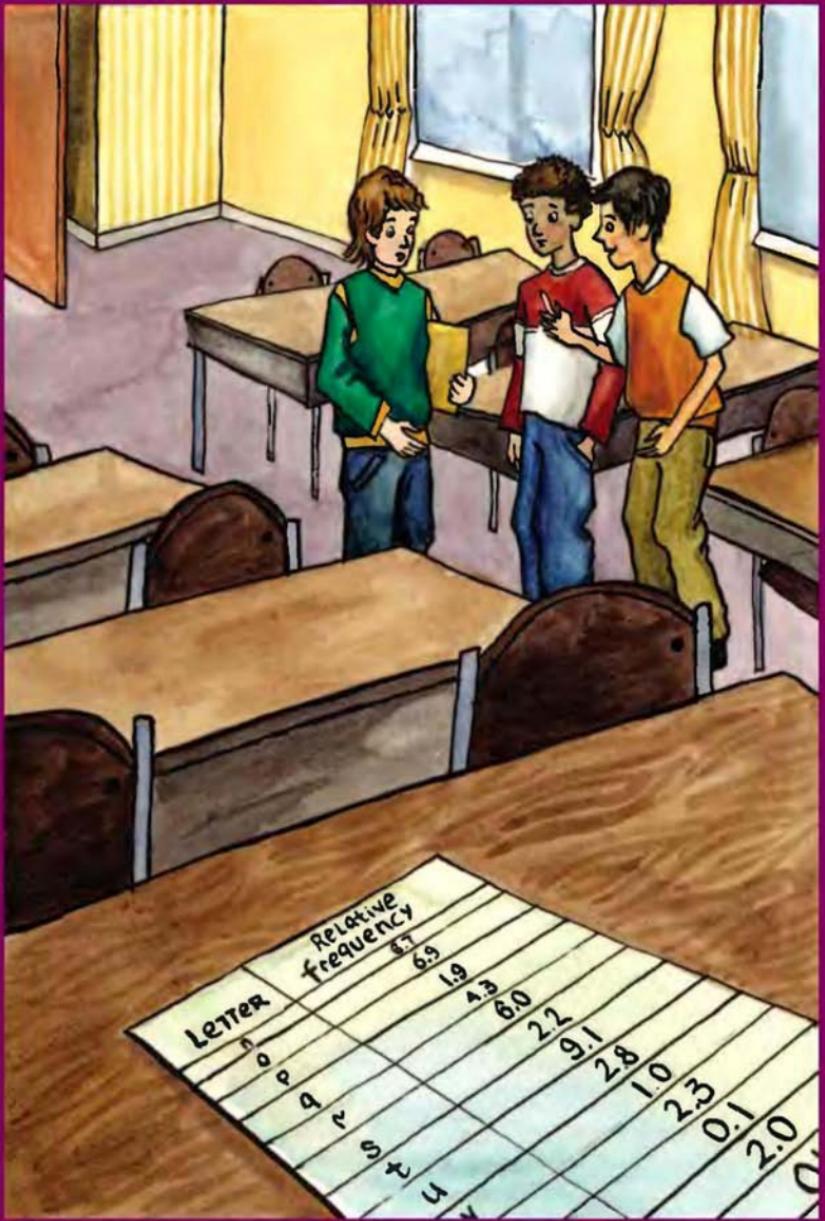
DO YOU KNOW?

Edgar Allan Poe Challenges

Edgar Allan Poe (1809–1849) is credited as the first author to write a detective story. He was also very interested in cryptography and wrote many articles about ciphers for a Philadelphia newspaper. Though he was not really a cryptographer, he was the first author to popularize the subject and, through his writings, he inspired many people to become interested in it. He even challenged his readers to send him messages encrypted by substitution ciphers and promised he would decrypt them all. He received hundreds of replies to his challenge. Although he needed nothing more than frequency analysis to decrypt the messages sent to him, the newspaper readers were amazed that he could do it. He gained the reputation as “the most skillful cryptographer that ever lived.”

The most popular of his stories, “The Gold Bug,” involves cryptography. In it, the main character decrypts a clue that was encrypted with a substitution cipher and discovers the buried treasure of the pirate Captain Kidd. This story won Poe a \$100 prize and made people even more interested in his work.

Chapter 6



Breaking Substitution Ciphers

"Now we know something about letter frequencies in English," said Dan. "I wonder how Jenny used that information to crack my cipher." Dan and Peter were ready to listen.

"Here is the table I found giving the relative frequencies of letters in English," Jenny told them.

"We didn't know you had used someone else's table," said Dan.

"We computed our own table!" exclaimed an exhausted Peter.

"Well, I bet you got similar results," Jenny assured them. "It turns out that the letter frequencies in most samples are about the same. That is why we can use the frequencies to break messages."

"So show us how you did it," Peter said.

Letter	Relative frequency (%)
a	8.2
b	1.5
c	2.8
d	4.3
e	12.7
f	2.2
g	2.0
h	6.1
i	7.0
j	0.2
k	0.8
l	4.0
m	2.4
n	6.7
o	7.5
p	1.9
q	0.1
r	6.0
s	6.3
t	9.1
u	2.8
v	1.0
w	2.4
x	0.1
y	2.0
z	0.1

Relative frequencies of letters in English.

"Well, first I found the frequencies and relative frequencies of the letters in your message," Jenny said.

Letter	Frequency	Relative Frequency		
		Fraction	Decimal (to 3 places)	Percent (%)
A	1	$\frac{1}{328}$.003	0.3
B	6	$\frac{6}{328}$.018	1.8
C	1	$\frac{1}{328}$.003	0.3
D	9	$\frac{9}{328}$.027	2.7
E	0	0	.000	0.0
F	24	$\frac{24}{328}$.073	7.3
G	6	$\frac{6}{328}$.018	1.8
H	4	$\frac{4}{328}$.012	1.2
I	27	$\frac{27}{328}$.082	8.2
J	13	$\frac{13}{328}$.040	4.0
K	1	$\frac{1}{328}$.003	0.3
L	41	$\frac{41}{328}$.125	12.5
M	9	$\frac{9}{328}$.027	2.7
N	5	$\frac{5}{328}$.015	1.5
O	18	$\frac{18}{328}$.055	5.5
P	15	$\frac{15}{328}$.046	4.6
Q	24	$\frac{24}{328}$.073	7.3
R	37	$\frac{37}{328}$.113	11.3
S	12	$\frac{12}{328}$.037	3.7
T	18	$\frac{18}{328}$.055	5.5
U	0	0	.000	0.0
V	5	$\frac{5}{328}$.015	1.5
W	9	$\frac{9}{328}$.027	2.7
X	8	$\frac{8}{328}$.024	2.4
Y	18	$\frac{18}{328}$.055	5.5
Z	17	$\frac{17}{328}$.052	5.2
Total	328			

Frequencies of letters in Dan's message (from page 32).

"Next, I used the frequencies to put the letters of the message in order from the most common to the least common letter. Then I did the same for the letters of regular English (right)."

"I decided to decrypt the most common letters first since that would give me the most progress. I figured a good first guess was to match **L**, the most common letter in the message, with **e**, the most common letter in English. Another choice would have been to match **R** with **e**, since **R** is the second letter on the list. But the message has a lot of three-letter words that start with **R**—I couldn't think of many three-letter words that start with **e**, so I decided **R** wasn't a good match for **e**.

"I went with my first guess and wrote **e** above all the **L**s in the message—in pencil because I knew I might change my mind later. Here are the first few lines:

Letters in Dan's Message

Letter	Relative frequency (%)
L	12.5
R	11.3
I	8.2
F	7.3
Q	7.3
O	5.5
T	5.5
Y	5.5
Z	5.2
P	4.6
J	4.0
S	3.7
D	2.7
M	2.7
W	2.7
X	2.4
B	1.8
G	1.8
N	1.5
V	1.5
H	1.2
A	0.3
C	0.3
K	0.3
E	0.0
U	0.0

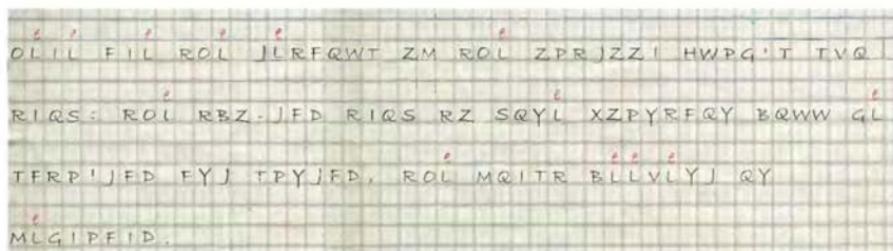
most common

Letters in English

Letter	Relative frequency (%)
e	12.7
t	9.1
a	8.2
o	7.5
i	7.0
n	6.7
s	6.3
h	6.1
r	6.0
d	4.3
l	4.0
c	2.8
u	2.8
m	2.4
w	2.4
f	2.2
g	2.0
y	2.0
p	1.9
b	1.5
v	1.0
k	0.8
j	0.2
q	0.1
x	0.1
z	0.1

least common

Comparing relative frequencies.



"Next, I thought about **t**. If I match **t** with **R**, then the word **ROL** would be **t_e**. That's possible. And if I match **O** with **h**, then **ROL** becomes **the**. That's a word that makes sense. I wrote both those substitutions above the letters.

he e e the et the +
OLIL FIL ROL JLRFQWT ZM ROL ZPRJZZI HWPG'T TVR
the + t t t e e +
RIRS: ROL RBZ-JFD RIRS RZ SQYL XZPYRFQY BQWW GL
the + t e e +
TERPIJFED FYJ TPYJFD ROL MRITR BLLVLYJ QY
e
MLGIPFID.

"The whole time I was working on this, I was also keeping track of the substitutions. I wrote the plaintext letters in the top row and the ciphertext letters in the bottom row.

"Here are my substitutions so far:

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
e	h	t																							

"Next I looked at other short words in the message. Unfortunately, there weren't any one-letter words. That was too bad because one-letter words are usually either **a** or **I**, so that would have been a good clue. But there was a two-letter word, **RZ**. I already knew that this was of the form **t_**. I thought this must be **to**, so I matched **Z** with **o**. Then I saw the two-letter word **ZM**. If **Z** is **o**, then this word is **o_**. It must be **on**. So I matched **M** with **n** and wrote these matches above the message.

he e e the et on the o t on
OLIL FIL ROL JLRFQWT ZM ROL ZPRJZZI HWPG'T TVR
t the t o t to e o t
RIRS: ROL RBZ-JFD RIRS RZ SQYL XZPYRFQY BQWW GL
the n t ee e
TERPIJFED FYJ TPYJFD ROL MRITR BLLVLYJ QY
e
MLGIPFID.

"I went back to the frequencies. The next most common unmatched letter was **I**. The first unmatched English letter in the list was **a**—the letters **I** and **a** even have the same relative frequencies (8.2%) in the tables. It seemed like a good match. But then the word **FIL** would be **ae**. That didn't look like a familiar word. Also, **ie** didn't look right. So I skipped **I** for a while.

"I decided to match **F**. The (relative) frequency of **F** is 7.3% in the message. The frequency of **a** in English is 8.2%, and the frequency of **i** is 7.0%. So either **a** or **i** would be reasonable matches for **F**. Then the word **FIL** would be either **a_e** or **i_e**. I thought maybe **a_e** was really **are**. So I guessed that **F** was **a** and that **I** was **r** and got two guesses for the price of one. I wrote those letters above the message and when I did that, the word **here** appeared. That encouraged me.

here are the eta on the o t oor
OLIL FIL ROL JLRFQWT ZM ROL ZPRJZZI HWPGIT TVQ
try the t o a tr to e o ta
RIQS: ROL RBZ-JFD RIQS RZ SQYL XZPYRFQY BQWW GL
sat r a a s a the n r st ee e
TFRP!JFD FYJ TPYJFD, ROL MQITR BLLVLYJ QY
we r ok
MLGIPFID.

"I noticed an apostrophe followed by one letter. That letter could be a **t**, as in words like **can't** and **don't**, but I already matched **t** with **R**. It could also be an **s**, because possessives end with 's. That suggested I match **T** with **s**.

here are the eta s on the o t oor s s
OLIL FIL ROL JLRFQWT ZM ROL ZPRJZZI HWPGIT TVQ
try the t o a tr to e o ta
RIQS: ROL RBZ-JFD RIQS RZ SQYL XZPYRFQY BQWW GL
sat r a a s a the n r st ee e
TFRP!JFD FYJ TPYJFD, ROL MQITR BLLVLYJ QY
we r ar
MLGIPFID.

"I saw a word that looked familiar. The word sat_r_a might be **saturday**. If that were true, then **P** should be **u**, **J** should be **d**, and **D** should be **y**. I filled in those letters.

Here are the details on the outdoor n s s
OLIL FIL ROL JLRFQWT ZM ROL ZPRJZZI HWPG'T TVQ
tr the to day tr to e on ta e
RQS: ROL RBZ-JFD RQS RZ SQYL XZPYRFQY BQWV GL
SATURDAY A D SUNDAY THE F RST E E A
TFRPIJFB FYJ TPYJFD, ROL MQITR BLLVLYJ QY
FEBRUARY
MLGIPFID.

"But then I saw a problem. The letters **saturday a_d su_day** must be **saturday and sunday** so **n** must be the match for **Y**. But I already matched **n** with **M** when I thought the word **ZM** was **on**. I must have been wrong. **ZM** could be **of** instead, so I erased the match of **M** with **n**. Instead I matched **M** with **f** and **Y** with **n**. It's a good thing I used pencil.

Here are the details of the outdoor n s s
OLIL FIL ROL JLRFQWT ZM ROL ZPRJZZI HWPG'T TVQ
tr the to day tr to e on ta e
RQS: ROL RBZ-JFD RQS RZ SQYL XZPYRFQY BQWV GL
SATURDAY A D SUNDAY THE F RST E E A
TFRPIJFB FYJ TPYJFD, ROL MQITR BLLVLYJ QY
FEBRUARY
MLGIPFID.

"Everything fell into place. **F**ebruary was missing the letter **b**, so I matched **G** with **b** and got **February**. **M**Q**I****T****R** was **f**irst. That was probably **f**irst, so I matched **Q** with **i**. **B**L**L****V****L****Y****J** had to be **w**eekend, so I matched **B** with **w** and **V** with **k**.

here are the details of the outdoor club's sri
OLIL FIL ROL JLRFQWT ZM ROL ZPRJZZI HWPGIT TVQ
trip: the two day trip to pine mountain will be
RIQS: ROL RBZ-JFD RIQS RZ SQYL XZPYRFQY BGWW GL
saturday and sunday the first weekend in
TFRPIJFD FYJ TPYJFD. ROL MQITR BLLVLYJ QY
february.
MLGIPFID.

"At this point I didn't need frequencies. I could see what the message probably said. So I decided: **W** must be **l**, **H** is **c**, **S** is **p**, and **X** is **m**. Here was the message:

here are the details of the outdoor club's sri
OLIL FIL ROL JLRFQWT ZM ROL ZPRJZZI HWPGIT TVQ
trip: the two-day trip to pine mountain will be
RIQS: ROL RBZ-JFD RIQS RZ SQYL XZPYRFQY BGWW GL
saturday and sunday the first weekend in
TFRPIJFD FYJ TPYJFD. ROL MQITR BLLVLYJ QY
february.
MLGIPFID.

"These are the substitutions I've used in these lines:

w	y	a	b	c	r	d	e	f	h	u	i	t	p	s	k	l	m	n	o					
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	U	V	W	X	Y	Z

"This was just the first few lines of the message. I continued with the rest of the message in a similar way."

★ TIP: Using Frequency Analysis to Decrypt Messages

- Match the most common letters first—you'll make faster progress.
- Use relative frequencies to help, but don't expect them to match exactly.
- Once you know some letters of a word, try to guess others until you have a word that makes sense.
- Look for familiar short words. One-letter words are usually **a** or **I**. Two and three letter words such as **in**, **of**, **at**, **and**, and **the** are helpful.
- Let punctuation help—for example, what letters can follow an apostrophe?
- Look for pairs of letters, called **digraphs**, that often occur together. Among the digraphs most common in English are TH, HE, IN, ER, ED, AN, ND, AR, RE, and EN. Common groups of three letters, called **trigraphs**, are THE, AND, ING, HER, THA, ERE, GHT, and DTH.

Using the frequencies, Jenny was able to make some intelligent guesses that helped to decrypt the message. The box on the left shows some of the ideas she used.

After decrypting Dan's message and learning that the boys had tried to keep the information about the ski trip secret from the girls, Jenny was mad. So when she heard that a local radio station was giving away tickets to the circus, she decided to tell only the girls. She encrypted a message to tell her friends.

"The boys will have to do some work if they want to figure out what I have written," she said.

Here is Jenny's message:

Y XTNDQ DNQYS EFNFYSU JKLM
NUUSGUPTQ FXTL JYII WYHT
NJNL VDTT PYDPGE FYPCTFE FS
FXT VYDEF FJTUFL-VYHT ATSAIT
JXS PNII YU. YF ESGUQE IYCT
VGU. ITF'E NII PNII NUQ WS
FSWTFXTD.



Do Problems 1 and 2 now.

PROBLEMS

(Workbook pages W26-W28)

1. Use frequency analysis to decrypt Jenny's message:

- Find the number of occurrences (frequency) of each letter in the message. Then compute the relative frequencies.
- Arrange the letters in order from the most common to the least common.
- Now decrypt using the frequencies to help you guess the correct substitutions.

2. Here is another message to decrypt using frequency analysis. The relative frequencies of the letters in the message are shown in the table on the right.

Message 2:

BQGKNJG SDKT CDQ MGVLQETD
BQGKNSLK G CGKNSLJD KDW SCEQT
MLQ CES REQTCNGY. UKMLQTUKGTDIY,
ET CGN G SEZD MLUQTDDK ALIIGQ
GKN TCD RLY CGN G SEZD SEXTDDK
KDAH. CD NUTEMUIIY WQLTD CDQ,
"NDGQ BQGJJY, TCGKHS CDGOS. E'N
WQETD JLQD RUT E'J GII ACLHDN
UO."

Letter	Relative frequency (%)
D	11.4
G	9.8
Q	8.3
T	7.8
C	6.7
K	6.7
E	6.2
L	5.7
N	5.7
S	5.2
I	3.6
U	3.6
J	3.1
M	2.6
Y	2.6
A	1.6
B	1.6
H	1.6
R	1.6
W	1.6
O	1.0
Z	1.0
V	0.5
X	0.5
F	0.0
P	0.0

DO YOU KNOW?

Poor Mary

If you want to send a secret message, you had better be careful. Mary Queen of Scots was beheaded in 1587 because her cipher was cracked and her messages revealed.

Mary was the Catholic Queen of Scotland and her cousin Elizabeth was the Protestant Queen of England. Mary had many troubles in Scotland and finally had to look for a safe place elsewhere. To avoid danger, she went to England, hoping that her cousin Elizabeth would help her, but that was a mistake. Elizabeth was afraid that Mary would try to become queen of England – the English Catholics believed Mary had more of a claim to the throne than Elizabeth – so when Mary arrived in England, Elizabeth promptly arrested her and kept her imprisoned for eighteen years.

Catholics loyal to Mary sent her letters that described a plot to free her, assassinate Elizabeth, and incite rebellion. In desperation, Mary agreed to the plot, but she made a mistake. She sent secret messages about details of the plot using a cipher that was not complex enough. The cipher that she used was not exactly a substitution cipher, but was quite similar to one. Elizabeth's spies stole the messages and used frequency analysis to decrypt them. Then, pretending to be Mary, Elizabeth's people sent a message that asked for the names of the others involved in the plot. With this trick, they were able to learn whom to arrest.

Elizabeth's advisors had suspected that Mary was plotting to take over the English throne, but they could not convince Elizabeth of this without proof. Unfortunately for Mary, the decrypted messages gave just the proof they needed. Elizabeth agreed to Mary's execution.

Unit 3



Vigenère Ciphers

Chapter 7



Combining Caesar Ciphers

Jenny and Abby found a box of their grandfather's papers up in the attic.

"What's this?" asked Abby, picking up one of the papers. "It looks like a message but it is not written in any language I have ever seen."

"Maybe it is encrypted!" Jenny exclaimed.

"Why would it be encrypted?" said Abby in disbelief. "What secret messages would Grandfather want to send?"

"Who knows? But maybe it is important."

"Let's get to work and figure out what it says."

The girls started working on the message. They tried all the ciphers they knew, but couldn't crack it. They tried frequency analysis but even that got them nowhere.

"I thought when we learned about frequency analysis that we would be able to crack anything," said a discouraged Jenny. "Boy, was I wrong."

"I agree," said Abby. "Let's take this to the next meeting of the Cryptoclub. Maybe somebody else will have an idea." By now, cryptography had become very popular in their school, so they had started a club for anyone who wanted to learn more about it.

A VNNS SGIAV GVDJRJ! WG OOF AB GZS UAZYK
PRZWAV HUW HESRVFU CGGG GB GZS AADVYCA
JWIWF NL HUW BBJHUWFA LWC GT YSYR KICWFVGF.
JZWYJW VVCWAY, W SGIAV GBES FZWAQ GGGBRK.
ZNLSSEA PEGITZH GZSZ LC N ESGSZ
RPDRJH GG VNNS GZSZ SDCJOVKSQ. KIEW SAGITZ,
HUWM NJS FAZIWF—VF O IWFL HIEW TBJA.
GZSEW AHKH OW ABJS—V OWYD FRLIEF OAV
GGSYR S QYSWZ.

Grandfather's message.

DISCUSS

Examine Grandfather's message.

- Do you agree with Jenny and Abby that it has unusual letter patterns?
- Do you think it could have been encrypted with a simple substitution cipher? Why or why not?

The girls took their grandfather's message to the very next Cryptoclub meeting. Lilah brought a new club member.

"Hey, everyone, this is Jesse," Lilah said. "He just moved in next door to me. He learned some cryptography in his old school."

"Welcome," said Jenny. "You've come at just the right time. We've tried and tried to crack this cipher with frequency analysis but we're stuck. Maybe you have an idea."

"There are ciphers that can't be cracked with frequency analysis. We learned about one called the Vigenère cipher. When Lewis and Clark left in 1804 to explore the American West, President Thomas Jefferson recommended that they use it to send him secret messages. For a long time people thought it was impossible to crack."

"Sounds like we ought to learn about it," said Abby. "Maybe that is the cipher used in Grandfather's note."

"Could be," said Jesse. "It was still used for serious purposes in the early 1900s."

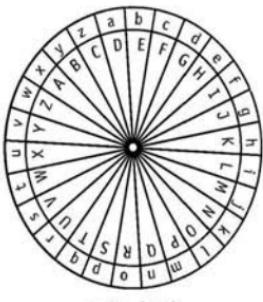
The Vigenère Cipher

You can think of a **Vigenère cipher** as being made from different Caesar ciphers, one for each letter of a keyword. (Note: This is not the same as the keyword cipher in Chapter 4.)

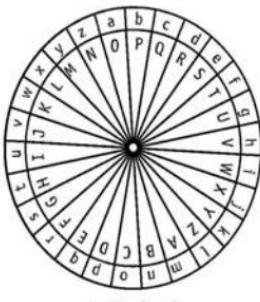
To use a Vigenère cipher, write the keyword repeatedly above the letters of the message. (Don't write anything above the spaces between words or above punctuation or other symbols.) Then, for each letter of the message, find the letter above it. Use the Caesar cipher that matches a with that key letter to encrypt or decrypt.

For example, to encrypt the message "Welcome to the Cryptoclub, Jesse" using the keyword **DOG**, first write the keyword again and again above the message. (Note: Don't write anything above the spaces between words or above punctuation.)

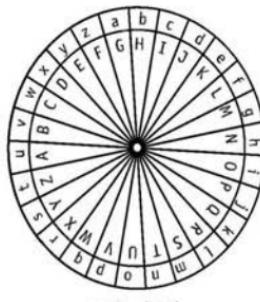
Use the wheel that matches **a** with **D** (page 56) to encrypt all letters that have **D** above them. The first letter is **w** and this wheel encrypts it as **Z**. The other letters with **D** above them are encrypted as shown.



a-D wheel



a-O wheel



a-G wheel

Wheels for a Vigenère Cipher with keyword **DOG**.

Use the wheel that matches **a** with **O** to encrypt all letters that have **O** above them. This wheel encrypts the letter **e** as **S**, and so on.

D	O	G	D	O	G	D	O	G	D	O	G	D	O	G	D	O	G	D	O	G	D	O	G	D	O	G		
Wel	c	o	m	e		t	o		t	h		e		C	r	y	p	t	o	c	l	u	b	,	J	e	s	s
Z	S	F	C	H	H	W	V		F	F	S	H	F	Z	E		X	V	G									

Use the wheel that matches **a** with **G** to encrypt all letters that have **G** above them. This wheel encrypts the letter **l** as **R**, and the other letters are encrypted as shown below.

D	O	G	D	O	G	D	O	G	D	O	G	D	O	G	D	O	G	D	O	G	D	O	G	D	O	G		
Wel	c	o	m	e		t	o		t	h		e		C	r	y	p	t	o	c	l	u	b	,	J	e	s	s
Z	S	R	F	C	S	H	H	U	W	V	K	F	F	E	S	H	U	F	Z	A	E		X	K	V	G		

Do Problems 1 and 2 now.

PROBLEMS (Workbook page W29)

- Encrypt “hidden treasure” using a Vigenère cipher with keyword **DOG**.
- Encrypt the message “Meet me tonight at midnight” using a Vigenère cipher with keyword **CAT**.

Decrypting Vigenère Ciphers

Jesse liked the welcome note. He sent the following reply, using the same keyword, **DOG**:

WVGQYY! JZGG HU ES NHFK

"We can decrypt this by going backward," said Lilah. She made a table like the one below and got to work.

keyword:	D	O	G	D	O	G		D	O	G	D	O	G	D	O	G			
plaintext:																			
ciphertext:	W	V	G	Q	Y	Y	!	J	Z	G	G	H	U	E	S	N	H	F	K

She used the first wheel, the **a-D** wheel, to decrypt the letters with **D** above them. She matched the ciphertext letters on the inner wheel to the plaintext letters on the outer wheel.

D	O	G	D	O	G		D	O	G	D	O	G	D	O	G	D	O	G
t	n	!	g	d	b	e												
W	V	G	Q	Y	Y	!	J	Z	G	G	H	U	E	S	N	H	F	K

She used the **a-O** wheel to decrypt the letters with **O** above them.

D	O	G	D	O	G		D	O	G	D	O	G	D	O	G	D	O	G
h	n	k	!	g	l	d	t	b	e	r								
W	V	G	Q	Y	Y	!	J	Z	G	G	H	U	E	S	N	H	F	K

Finally, she used the **a-G** wheel to decrypt the rest of the message.

D	O	G	D	O	G		D	O	G	D	O	G	D	O	G	D	O	G
t	h	a	n	k	s	!	g	l	a	d	t	o	b	e	h	e	r	
W	V	G	Q	Y	Y	!	J	Z	G	G	H	U	E	S	N	H	F	K

 **Do Problems 3 and 4 now.**

PROBLEMS (Workbook page W29)

3. Decrypt the Vigenère message below using keyword **CAT**.

QK, UWT PJEKG SACLE
YE FGEM?

4. Decrypt using a Vigenère cipher with keyword **LIE**:

L TMP KEY BVLDIW

PEWNALG ECWYYL

XSM AZZPO ELTTI EPI

EZYEP MD XYEBMYO

SY QXD ALZMW.

—Mark Twain

PROBLEMS

(Workbook page W30)

5. Use the Vigenère square—not a cipher wheel—to encrypt the message “top secret information” with keyword DOG.
6. Use the Vigenère square to decrypt the following message with keyword BLUE.

XSCGI XYXIZX HP JIY

MTEI CPMX?

7. Use either the cipher-wheel method or the Vigenère-square method to decrypt the following quotes from author Mark Twain.

a. Keyword: SELF

S TPWKSY HSRYTL

FP HGQQTJXLGDI

HNLLZZL

LTX GAY FHTCTNEW.

b. Keyword: READ

SI CDIIFXC EBRLX

RHRHIQX LEDCXH

EFSKV. PSU PRC DLV

SF D DMSSIMNW.

The Vigenère Square

“Sometimes I get mixed up using the wheels,” said Becky. “I don’t like it when the letters are upside-down. Is there another way to encrypt?”

“I like the wheels,” said Jesse, “but some people prefer to use the Vigenère square. I’ll show you how, then you can choose the method you like best.”

“The top row of the Vigenère square holds the plaintext (in lower case, as usual). Each row shows a shift of the plaintext alphabet, like a shift with a cipher wheel.”

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

The Vigenère square: encrypting t with row D.

Encrypting and Decrypting with the Vigenère Square

To encrypt or decrypt a Vigenère message using a Vigenère square, begin as you did with cipher wheels: write the keyword repeatedly above the message. For each letter of the message, find the key letter above it. Then encrypt or decrypt using the row that begins with that key letter.

- To encrypt using a given row: Begin in the top row with the plaintext letter to be encrypted. Follow its column down to the letter where it meets the given ciphertext row.
- To decrypt using a given row: Begin in the given row with the ciphertext letter to be decrypted. Follow its column up to the plaintext letter it meets in the top row.

"For example, to encrypt **t** using row **D**," said Jesse, "find **t** in the top row and follow it down to **W**, the letter where it meets row **D**."

"I get it," said Becky. "The plaintext **a** is encrypted as **D**, **b** as **E**, and so on. Using row **D** of the Vigenère square is like using the **a-D** wheel."

A larger Vigenère square is on the inside back cover.

☞ **Do Problems 5–10 now.**

★ TIP

Place a ruler or a piece of paper under the row you are using, to help line up the letters.

PROBLEMS

(Workbook page W31)

8. Use either the cipher-wheel method or the Vigenère-square method to decrypt the following quotes from Mark Twain. They were encrypted with the Vigenère cipher using the given keywords.

a. Keyword: CAR

CLNCYJ FO IKGYV.

TYKS NKLC IRRVIWA

SFOE GGOGNE RPD

RUTFPPIJJ TYG RVUT.

b. Keyword: TWAIN

BB YWH MALT GAA

TZHMD YWH WKN'B

UTRE BB KAMMZUAR

IARPHQAZ.

c. Keyword: NOT

PCNEOZR WL

ESLVGMNBVR HH SSTE,

ATFHXEM HS TXNF—

GBH TOGXAQX BT

YROK.

PROBLEMS

(Workbook pages W32-W33)

9. Use either the cipher-wheel method or the Vigenère square method to decrypt the following quotes.

- a. Keyword: WISE

DWF1OBQ MO BZI

BQJWP KZELBWV EV

LLA JGSG WX AEAWSI

—Thomas Jefferson

- b. Keyword: STONE

LAS ZEF PVB VWFCIIK

T ABYFMOVR TXUVRK

UM PEJKMVRY TKNC

KFOYP KMCAIK

—Chinese Proverb

10. Find a quote from a famous person. Encrypt it using a Vigenère cipher. Use it to play Cipher Tag.

CLASS ACTIVITY: Play Cipher Tag

Play Cipher Tag using messages encrypted with a Vigenère cipher.

Do Problem 11 now.

PROBLEMS (Workbook page W34)

11. **Challenge.** Explore how to describe a Vigenère cipher using numbers.

In Chapter 2, you worked with number messages. You described Caesar ciphers with arithmetic—by adding to encrypt and subtracting to decrypt. The Vigenère Cipher can be described with arithmetic too. Instead of writing the keyword repeatedly, change the letters of the keyword to numbers and write the numbers repeatedly. Then add to encrypt.

Example. The message “welcome” is encrypted below using keyword DOG. First change the message to numbers. Next, change DOG to numbers: 3, 14, 6. Write these key numbers repeatedly under the message numbers. Then add, replacing any number greater than 25 with the equivalent number between 0 and 25. Change the numbers back to letters. Note that this gives the same answer that the wheel method and the Vigenère-square method would give.

Plaintext	w	e	l	c	o	m	e
Numbers	22	4	11	2	14	12	4
Key numbers	3	14	6	3	14	6	3
Shifted numbers (between 0 and 25)	25	18	17	5	26 ₂	18	7
Cipher text	Z	S	R	F	C	S	H

Encrypt and decrypt your own message with this method.

DO YOU KNOW?

The Civil War

Both the North and the South used cryptography during the American Civil War. Unfortunately for the South, the North was better at it. Abraham Lincoln employed three cryptographers in their early twenties who were very good at cryptanalyzing the Confederate correspondences. The South, on the other hand, did not have good advisers and made several mistakes.

One mistake the South made was to let each commanding officer choose his own codes and ciphers. This resulted in at least one general choosing a Caesar cipher, which was very easy to break. The most common cipher used was the Vigenère cipher, but, although this seemed like a good choice, it turned out to be a big failure. One problem with the Vigenère cipher was that the messages were often garbled. If one letter was omitted during transmission, the keyword wouldn't match up and the message wouldn't make sense. Another problem was that the South made the huge mistake of using the same three keywords, MANCHESTER BLUFF, COMPLETE VICTORY, and COME RETRIBUTION for most of the war. Once Lincoln's young cryptographers figured them out, they were able to easily decrypt other messages.

To use the Vigenère cipher, Confederate soldiers used a cipher disk. It looked very similar to your cipher wheel except that it was made of brass.

Chapter 8



Cracking Vigenère Ciphers When You Know the Key Length

"Maybe Grandfather's note was encrypted using a Vigenère cipher. But we don't know the keyword. So how can we decrypt his message?" Jenny asked the rest of the Cryptoclub.

"We need to look at messages that somebody knows something about," said Abby.

"OK," said Jesse. "Let's send encrypted messages to each other and see if we can break them. If we get stuck, we can give each other hints about the keyword we used."

"Good idea," said Jenny. "We might notice something about how Vigenère ciphers work that will help break Grandfather's code. Let's make the messages long enough to see patterns."

So the boys got together and encrypted a message for the girls to work on. And the girls prepared one for the boys to work on.

Cracking the Boys' Message

Here is the boys' encrypted message.

KVX DOGRUXI OM R PHRH-KVBMRZ VFBVVGLZCG
NSGK HH KVX VRZV CY KVX CODV OGU MXCZXU,
"PHRH GLAUVF 99, VFAX SOVB. MHLF MZAX ZG NG."
PNK HAV PHRH WZRG'K FXKIKE. "PHRH GLAUVF 99,"
AV VHCZXISW RUTZB. "KVHNIB MF HAV RHTY
BDAXIUWTKSEP CK Z'ZE TVTIUX PCN FJXIHBDS."
"LFAXXKVBEU BJ KKFBZ, SCLJ," VBJ OLJWLKOOGK
GTZR. "PV CGCM ARJX 75 SCTKG. MYSKV WL EC
GLAUVF 99." MYS FRBTXSK KVHLUAK THI O
FFAXEH. "UFQM EIFSSK 66," YS RVZEVN. "TIS RFI
ARJBEU MICNSZX FIM KVXIS?"

The girls tried for a while to decrypt it, but they got nowhere.

"Frequency analysis of the entire message would be useless," said Lilah, "since a Vigenère cipher encrypts the same letter in different ways depending on which wheel is used."

"Yeah, but if we knew which letters were encrypted with which wheel, it might help," said Evie. "It would be like cracking several different messages separately."

"How would we know that?" asked Abby.

"We could figure out which letters go with which wheel if we knew how long the boys' keyword is," said Evie.

"Our keyword has length 3," said Tim. "Will that help?"

Evie took a pencil and wrote the number 1 under the first letter in the message and under every third letter after that.

"The letters with the 1s are the letters that were encrypted with the first wheel," she said. "We don't know yet what kind of wheel it was, but we can probably figure that out. I'll work on these letters."

"I get it," exclaimed Abby. She wrote 2 under the second letter and under every third letter after that. "The letters with the 2s were encrypted with the second wheel. I'll get to work on those."

"I'll work on the letters from the third wheel," said Jenny. She wrote 3 under each of those letters.

Here are the first few lines.

KVX DOGRUXI OM R PHRH KVBMZRZ VF BVVG LZC G
1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3

NSGK HH KVX VRZV CY KVX CODV OGU MX CZXU,
1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1

"PHRH GLAUVF 99, VFAX SOVB. MHLF MZAX ZG NG."
2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1

PNK HAV PHRH WZRG'K FXKIKE. "PHRH GLAUVF 99,"
2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1

Evie wrote down only the letters from the message with 1 underneath. They were:

KDRIRRVRFVZ
NKKVVVKCVCUC
RLVFSBLZZG
KVRZKKERLV
VCIRZVIFVT
DUKPZTIPFID
FKEJFSJJJKK
ZVCRSKYVE
LVYRXKLKI
FEFESYVVIF
REISFKI



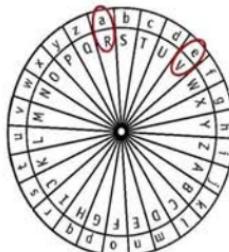
A	N 1
B	I 0
C	P
D	Q
E	XH I R XH
F	XH XH S XH
G	T
H	U
I	V XH XH
J	W
K	X XH
L	Y
M	Z XH

"These letters were all encrypted using the same wheel. Breaking this part of the message is the same as breaking a Caesar cipher. It is easier than breaking most substitution ciphers. I only have to figure out one letter and I'll know how to turn the wheel," she said.

"Let's see which letter occurs most often in this list," said Evie.
"Who wants to count?"

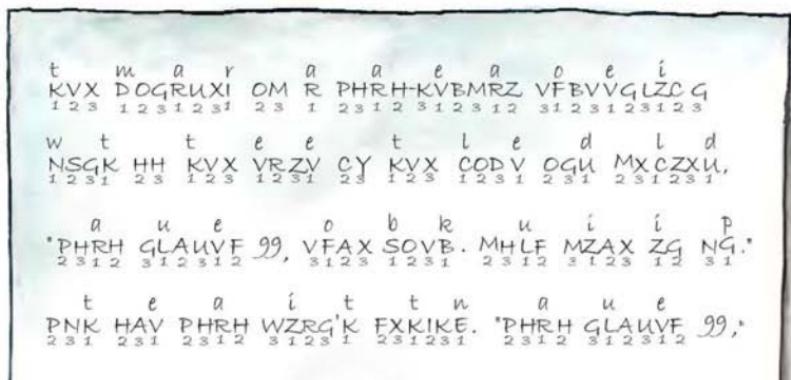
They made a tally of the letters in the list. Becky read the letters one by one as Evie made tally marks (left).

"V and K are the most common letters in this list. So either V or K is probably the encryption of e, since e is the most common letter in English. Let's turn the first wheel so e matches V. If this doesn't work, we'll try e with K." What they got was the a-R wheel (*right*).



The a-R cipher wheel.

They entered the letters from this wheel into the message. Here are the first few lines:



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

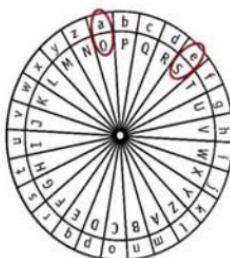
"I'll work on the part of the message that uses the second wheel," said Abby. "That is all the letters with 2 underneath."

She read off just those letters while Lilah made a tally (*left*).

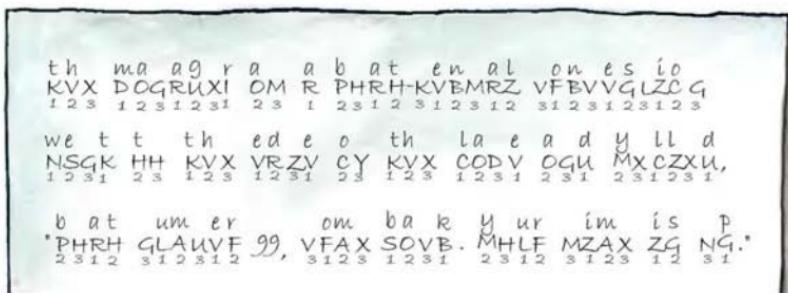
"**S** is the letter occurring most often in this list, and **H** is the second most common letter. I'll guess that the second wheel matches **S** with **e**. It could be **H** with **e**, but I'll only try that if my first guess doesn't work."

Abby turned the cipher wheel to match **S** with **e**. This gave the **a-O** wheel (*right*).

She used this wheel to decrypt the letters with 2 underneath.



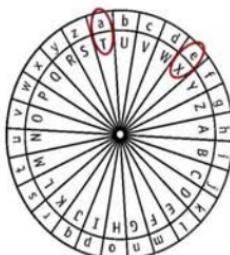
The **a-O** cipher wheel.



"I'll figure out the letters for the third wheel," said Jenny.

"Maybe I don't need to do a frequency analysis—I see a pattern that might make my job easier."

"Look at the message we have so far. The first word, **KVX**, is decrypted as **th**_. There aren't many three-letter words that start with **th**. I think this word is **the**. That would mean **X** should be decrypted as **e**. I'll match **X** and **e** on the wheel. That gives me the **a-T** wheel" (*right*).



The **a-T** cipher wheel.

Jenny started to substitute the letters on this wheel. "Look—we're getting a message that makes sense," she said. "We must have the correct substitutions."

The girls finished decrypting the boys' message:

the manager at a boat-rental concession
KVX DOGRUXI OM R PHRH-KVEMRZ VFBBVVLZCG
1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3

went to the edge of the lake and yelled,
NSGK HH KVX VRZV CY KVX CODV OGU MXCZXU,
1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1

"boat number 99, come back. Your time is up."
"PHRH GLAUVF 99, VFAX SOVB. MHLF MZAX ZG NG."
2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1

but the boat didn't return. "boat number 99."
PNK HAV PHRH WZRG'K FXKIKE. "PHRH GLAUVF 99,"
2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1

he hollered again. "return to the dock
AV VHCZXISW RHTZB. "KVHNIB MF HAV RHTY
3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1

immediately or i'll charge you overtime."
BDAXUWTKSEP CK Z'ZE TVTNUX PCN FJXIHBD'S.
3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2

"something is wrong, boss," his assistant
"LFAXKVBEN BJ KKFHZ, SCLJ." VBJ OLJWLKOGK
3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1

said. "we only have 75 boats. there is no
GTZR. "PV CGOM ARJX 75 SCTKG. MYSKG WL EC
2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2

number 99." the manager thought for a
GLAUVF 99. "MYS FRBTXSK KVHLLAK THI O
3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2

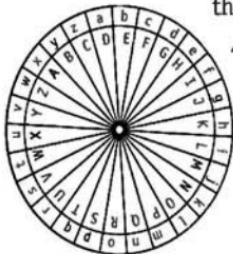
moment. "boat number 66," he yelled. "are you
FFAXEH. "UFOM EIFSSK 66." YS RVZEV. "TIS RFI
3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2

having trouble out there?"
ARJBEN MICNSZX FIM KVXIS?
3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2

"The three wheels you used were the **a-R** wheel, the **a-O** wheel, and the **a-T** wheel. From your wheels, we know that your keyword was ROT. Yuck. We wouldn't have guessed that."

Cracking the Girls' Message

"You were able to crack our message even though you only knew the length of the keyword," said Jesse. "Good job. Let's see if we can crack your message."



The **a-D** cipher wheel.

"Okay," said Abby. "Here it is. The key length is 4. Good luck."

The boys wrote numbers under the letters of the message so they could see which letters went with each wheel.

They found that **H** was by far the most common letter among the first wheel's encrypted letters, so they turned the wheel to match **e** with **H**. That gave the **a-D** wheel (*left*). They used the **a-D** wheel to decrypt the letters with 1 underneath. This meant that the first letter of the keyword was **D**.

t	e	a	t	o	m																						
W	P	Q	V	H	E	M	W	D	T	U	X	W	T	Q	F	R	G	Z	E	P	M	P					
1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	
e	.	t	i	y	t																						
N	H	A	E	!	.	W	P	Q	F	L	O	N	S	B	A	U	R	W	P	Q							
4	1	2	3	4	.	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3			
e	b	o	o	a	y	s																					
R	H	Q	S	L	E	W	D	L	R	W	P	G	R	V	E	D	V	F	P	B	B	Q	E	V	M	P	
4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
i	.	w	w	h	f	e	w																				
L	L	U	.	E	S	P	M	F	M	P	M	E	X	K	M	K	S	I	N	Q	V	H	L	T	M	P	
4	1	2	.	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	
o	b	e	n	e	d																						
1	0	L	R	Q	O	!	E	M	F	A	H	M	Z	E	Q	Q	O	O	H	T	M	R	G	!			
2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
m	.	s	l	s	k																						
P	P	P	M	.	V	I	V	A	Q	E	O	E	M	C	V	B	A	S	N	B	T	!					
3	4	1	2	.	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3		

w e - t l , w
 Q Q O O H T - M J W M D E O T , U X Z I E
 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3

i r . b o a e
 F L O S I U . B T I E Q S F R G E P D C S L H L
 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2

d g . o a t
 M R G T M Y J P Q H . R V Q H D G M J W M D
 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3

e g b h c , h
 N H A E I J Z M F E M P X K M Z M F S Q P , K Q E
 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3

a r k a e s ,
 J D B T I U B A S N P U Q D A U H H I Z H V I U H .
 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3

* j e , s y e i
 * M M E W H , B T S V M N S B A M V H U M O L V S
 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3

u y . h h y
 J X V A J B W G . X K M K X K Q Z O B W G
 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3

o w h m w h
 H R V ' F O Q W I X K M P M P M U W Z W D X K
 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1

e n n e . * s
 U A V H B T E Q B T I Q Q O O H T . * V I V A Q
 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3

r e d d , * t r
 K U Q Z R H L M R G A M M G . * L A R ' W E A V U G
 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2

d . o i s t
 P E G . Q W R R E I L L K T M V E A V W P
 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2

r t t t i ,
 Y S U M . N Y W Q R M W W A O W P Q H L U Q ,
 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3

(Message continues on next page.)

h	o	s	d	g	.	o
X KMK	A R C X H	V B A T	G W U R J	Q F.	W R	
4 1 2 3	4 1 2 3 4	1 2 3 4	1 2 3 4 1	2 3		4 1
i	o	c	t	o	r	*
N M V	L' D Q	G R T X I F B Q H	W M Z	H R T X E U A *		
2 3 4	1 2 3	4 1 2 3 4 1 2 3 4	1 2 3	4 1 2 3 4 1 2		

Next the boys worked on letters with 2 underneath. They made this table:



Frequency of letters with 2 underneath in girls' message.

CLASS ACTIVITY: Finish Decryption the Girls' Message (Workbook pages W35-W38)

(You can do this activity by yourself if you are reading without a class—it just will take longer to count the letters.)

Your teacher will assign your group 3 or 4 lines of the message.

1. **First wheel.** The letters of the first wheel are already decrypted. What letter was matched with a?
2. **Second wheel.**
 - a. Use the information in the table above to decide how to turn the second wheel. Then decrypt the letters with 2 underneath in your assigned lines.
 - b. What letter did you match with a?

3. Third wheel.

a. Find the number of As, Bs, Cs, etc., among the letters with 3 underneath. To save work, count the letters in your assigned lines only. Then share your data with the class to get a combined total.

b. Use the class data from **3a** to decide how to turn the third wheel. Then decrypt the letters with 3 underneath in your assigned lines.

c. What letter did you match with a?

4. Fourth wheel.

a. Use the partly decrypted message to guess how to decrypt one of the letters with 4 underneath. Use this to figure out what the fourth wheel must be. Then decrypt the rest of your assigned lines.

b. What letter did you match with a?

5. What was the keyword?

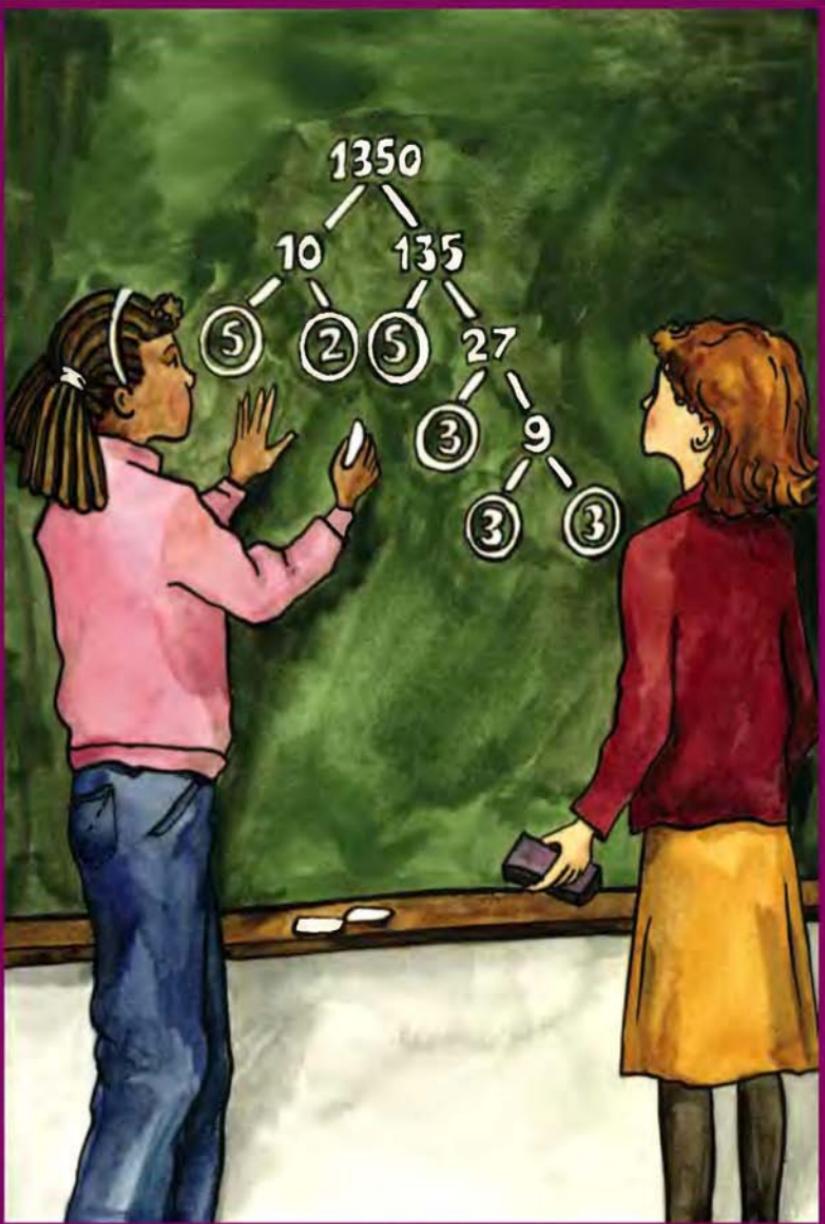
DO YOU KNOW?

Lewis and Clark

In 1803, President Thomas Jefferson sent Captain Meriwether Lewis and Captain William Clark on an important mission to explore the western portions of the continent and send back information about the terrain there. Jefferson knew there were governments who would not be happy about such an expedition. The ownership of the western territories was not yet determined, and England, Spain, and the United States were all trying to acquire them. In fact, Spain attempted to stop Lewis and Clark's expedition but never caught up with them.

Jefferson was afraid that the valuable information Lewis and Clark found would be lost if they were captured, so he asked them to send him regular reports. He expected that Native Americans and fur traders would be able to carry the messages back to him. He asked them to encrypt any messages that should be kept secret from other governments. He suggested they use the Vigenère cipher and described it to them in a letter. There is no evidence that Lewis and Clark actually used the cipher, but there is a sample message encrypted by President Jefferson with keyword ARTICHOKE.

Chapter 9



Factoring

"Jesse, you learned about Vigenère ciphers in your old school, didn't you?" asked Abby. "Do you have any suggestions about how we can crack Grandfather's message?"

"We did crack some Vigenère messages, but that was quite a while ago so I don't remember all the details," admitted Jesse. "But I think we looked for patterns in the messages. Then we found common factors of some numbers related to the patterns. That helped us figure out the key length."

"It sounds like we should review what we know about factoring," said Jenny.

"That's a good idea," said Abby. "Then we'll be ready to look at the message again."

The **factors** of a number are the whole numbers that can be multiplied to get that number. For example, 3 and 4 are factors of 12 since $3 \times 4 = 12$. Other factors of 12 are 1, 2, 6, and 12.

The **multiples** of a number are the numbers you get when you multiply it by whole numbers. The multiples of 3 are 3, 6, 9, 12, and so on. A number is a multiple of each of its factors.

PROBLEMS (Workbook page W39)

1. Find all factors of the following numbers:
 - a. 15
 - b. 24
 - c. 36
 - d. 60
 - e. 23
2. List four multiples of 5.
3. List all prime numbers less than 30.
4. List all composite numbers from 30 to 40.

A **prime number** is a number that has only two factors: 1 and itself. The first few prime numbers are 2, 3, 5, 7, and 11. A number that has more than two factors is a **composite number**. The first few composite numbers are 4, 6, 8, 9, and 10. The number 1 is unusual because it is neither prime nor composite.

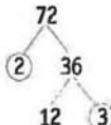
 **Do Problems 1–4 now.**

To factor a number means to break it into a product of its factors. There is often more than one way to do this. For example, 8×9 and 36×2 are both factorizations of 72. However, there is only one way to factor a number into prime factors, called its **prime factorization**.

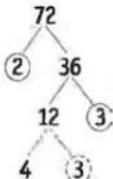
To find the prime factorization of a number, you can start with any factorization, then factor any parts of it that are not prime. One way to keep track of your work when looking for a prime factorization is to use a **factor tree**. Start with the number and break it into two factors. Circle any factors that are prime.



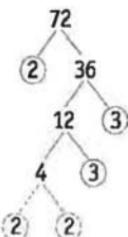
Factor each uncircled number into two factors: One way to factor 36 is 12×3 . Circle the 3 to show that it is prime.



Again factor any numbers that are not prime: One way to factor 12 is 4×3 . Circle the 3 since it is prime.

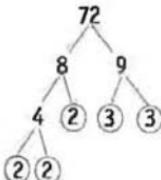


The final step is to factor 4 into 2×2 and circle the 2s.



The prime factorization of 72 is the product of all the circled numbers in the tree: $72 = 2 \times 2 \times 2 \times 3 \times 3$.

Here is another factor tree for 72. Although it is different, it gives the same prime factorization.



Do Problem 5 now.

PROBLEMS
(Workbook page W40)

5. Use a factor tree to find the prime factorization of each of the following numbers:
a. 24 b. 56 c. 90

"A number like 72 is easy to factor," said Becky. "I already know that $72 = 8 \times 9$ since that's one of the multiplication facts. But where do I start with a larger number like 1350 that isn't in the multiplication table? How do I know any of its factors?"

It helps if you can recognize when numbers are divisible by other numbers. One way to check divisibility is to divide on a calculator. For example, 299 is divisible by 23, since $299 \div 23$ is a whole number, 13, with no remainder.

"I remember once learning about divisibility patterns," said Evie.

"You can use these patterns to tell divisibility without a calculator. If you know which numbers divide your number, you already know some of its factors. Let's make a list of rules for divisibility."

They all got to work and made a list.

"These divisibility rules will help us factor," said Evie.

RULES FOR DIVISIBILITY

- A number is divisible by 2 if it ends in 0, 2, 4, 6, or 8.
Example: 148 is divisible by 2, but 147 is not.
- A number is divisible by 3 if the sum of its digits is divisible by 3.
Example: 93 is divisible by 3, since $9 + 3 = 12$, which is divisible by 3. However, 94 is not, since $9 + 4 = 13$, which is not divisible by 3.
- A number is divisible by 4 if its last two digits form a number that is divisible by 4.
Example: 13,548 is divisible by 4 since 48 is divisible by 4. But 13,510 is not divisible by 4 since 10 is not.
- A number is divisible by 5 if it ends in 0 or 5.
Example: 140 and 145 are both divisible by 5, but 146 is not.

- A number is divisible by 6 if it passes the tests for divisibility by 2 and by 3.

Example: 2358 is divisible by 6, because it is divisible by 2 (since it ends in 8) and by 3 (since $2 + 3 + 5 + 8 = 18$).

- A number is divisible by 9 if the sum of its digits is divisible by 9.

Example: The number 387 is divisible by 9 since $3 + 8 + 7 = 18$, which is divisible by 9.

- A number is divisible by 10 if it ends in 0.

Example: Both 90 and 12,480 are divisible by 10, but 105 is not.

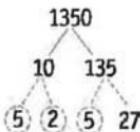
Do Problems 6–12 now.

"OK," said Becky. "Let's try factoring a big number like 1350. Where do we start?"

"You can see right off that 1350 is divisible by 10," said Evie, "so let's start a factor tree."



"Factor the 10 as 5×2 . As for the 135, I see that it is divisible by 5, so I divide 135 by 5 and get 5 and 27 as factors. After these steps, I circle all the primes: 5, 2, and 5.



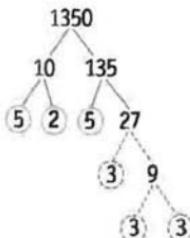
PROBLEMS

(Workbook pages W41–W42)

Use the rules for divisibility to answer the following questions.

- Which of the following are divisible by 2? Why?
a. 284 b. 181
c. 70 d. 5456
- Which of the following are divisible by 3? Why?
a. 585 b. 181
c. 70 d. 6249
- Which of the following are divisible by 4? Why?
a. 348 b. 236
c. 621 d. 8480
- Which of the following are divisible by 5? Why?
a. 80 b. 995
c. 232 d. 444
- Which of the following are divisible by 6? Why?
a. 96 b. 367
c. 642 d. 842
- Which of the following are divisible by 9? Why?
a. 333 b. 108
c. 348 d. 1125
- Which of the following are divisible by 10? Why?
a. 240 b. 1005
c. 60 d. 9900

"Next, I'll factor the 27 into 3×9 and, after that, the 9 factors into 3×3 . When I am done, I circle all the primes.



"Now I multiply all the circled numbers to get the prime factorization of 1350:

$$1350 = 5 \times 2 \times 5 \times 3 \times 3 \times 3.$$

"It is easier to read if we write the primes in increasing order:

$$1350 = 2 \times 3 \times 3 \times 3 \times 5 \times 5.$$

If the same prime appears many times in a factorization, it helps to use exponents. An **exponent** tells how many times to multiply a base number. If the base is 3, then

$$3^1 = 3$$

$$3^2 = 3 \times 3$$

$$3^3 = 3 \times 3 \times 3$$

$$3^4 = 3 \times 3 \times 3 \times 3$$

$$3^5 = 3 \times 3 \times 3 \times 3 \times 3$$

etc.

Using exponents, the prime factorization of 1350 is

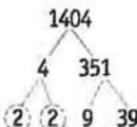
$$1350 = 2 \times 3^3 \times 5^2.$$

"Now it's your turn to find the prime factorization of a big number. How about 1404?" Evie said to Becky.

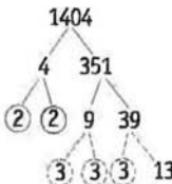
"I'll try," said Becky. "The last two digits are 04 so it is divisible by 4. I'll use that to start the tree."



"I factor the 4 into 2×2 and circle the 2s because they are prime. I see that 351 is divisible by 9 since $3 + 5 + 1 = 9$, which is divisible by 9. I divide 351 by 9 and get 39, so 351 factors into 9×39 .



"I factor 9 into 3×3 , and I circle each 3. I see that 39 is divisible by 3, since $3 + 9 = 12$, which is divisible by 3. So I divide 39 by 3 and get 13. Since these are prime numbers, I am done.



"I multiply all the primes together and get

$$1404 = 2^2 \times 3^3 \times 13.$$

Do Problem 13 now.

PROBLEMS
(Workbook pages W43-W45)

- 13.** Use a factor tree to find the prime factorization of each of the following numbers. Write each factorization using exponents.
- a. 2430 b. 4680
c. 357 d. 56,133
e. 14,625 f. 8550

A **common factor** of two or more numbers is a number that is a factor of each of them. For example, 3 is a common factor of 6, 9, and 15.

One way to find common factors is to list the factors of each number, then find all numbers on both lists. This works if there are not a lot of factors. For example, to find all common factors of 12 and 30, we could make two lists:

The factors of 12 are **1, 2, 3, 4, 6**, and 12.

The factors of 30 are **1, 2, 3, 5, 6, 10, 15**, and 30.

The numbers in bold are all the common factors. The **greatest common factor** is 6, the largest of all the common factors.

PROBLEMS

(Workbook pages W46–W47)

- 14.** Find the common factors of the following pairs of numbers:
 - a. 10 and 25
 - b. 12 and 18
 - c. 45 and 60
- 15.** Find the greatest common factor of each of the following pairs of numbers:
 - a. 12 and 20
 - b. 50 and 75
 - c. 30 and 45
- 16.** For each list of numbers, factor the numbers into primes and then find all common factors for the list.
 - a. 14, 22, 10
 - b. 66, 210, 180
 - c. 30, 90, 210

A second way to find common factors is to find the prime factorization of each number and multiply some or all of the common prime factors. Let's use the same numbers, 12 and 30, again.

The prime factorization of 12 is $2 \times 2 \times 3$.

The prime factorization of 30 is $2 \times 3 \times 5$.

The prime factorizations have 2 and 3 in common. If we multiply all the common prime factors together, we get the greatest common factor, $2 \times 3 = 6$. Other common factors are 1, 2, and 3.

For numbers with several factors, the second method—using the prime factorization—is usually quicker than listing all the factors of both numbers. Here is another example:

The prime factorization of 140 is $2 \times 2 \times 5 \times 7$.

The prime factorization of 60 is $2 \times 2 \times 3 \times 5$.

The common prime factors of 140 and 60 are 2, 2, and 5. We get the greatest common factor by multiplying *all* the common prime factors, $2 \times 2 \times 5 = 20$.

 **Do Problems 14–16 now.**

DO YOU KNOW?

Cicadas

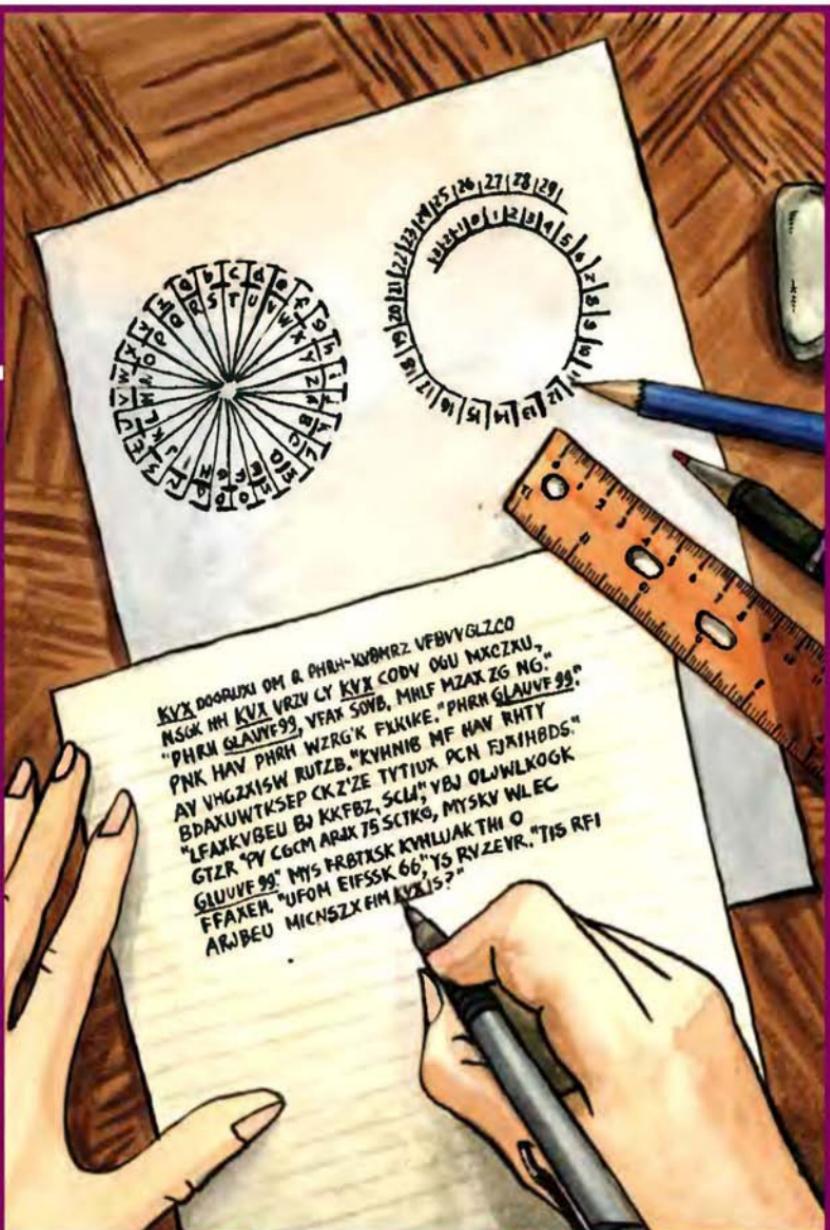
There are two types of cicadas, annual cicadas and periodical cicadas. Annual cicadas can be found every year, but periodical cicadas all mature at the same time, so they appear in cycles. Four species of periodical cicadas have 13-year life cycles and three have 17-year life cycles. They are sometimes called "13-year locusts" and "17-year locusts," but they aren't really locusts.

Cicadas stay underground for all but their last year of life. Then they come to the surface to mate, sing, lay their eggs, and then die. It is usually big news when they appear because it seldom happens. But when it does, they are hard to ignore because they are very noisy and seem to be everywhere you look.

Both 13-year and 17-year cicadas can live in the same area, but it would be very crowded if they all came up at the same time. Fortunately, this rarely happens. That's because the lengths of their life cycles don't have any factors in common — both 13 and 17 are prime numbers. Since $13 \times 17 = 221$, they only come out of the ground together once in every 221 years.

There are different types of cicadas in different parts of the country, so the particular year they immerge is different in different places. Illinois experienced a "cicada invasion" in 1990. In 2004, 17-year cicadas invaded Washington, D.C., and much of the Northeastern United States.

Chapter 10



Using Common Factors to Crack Vigenère Ciphers

"Well, we have figured out how to crack a Vigenère cipher when we know the key length. But if we don't know anything about the keyword, how can we know its length?" said Jenny.

"We're stuck," said Abby. "It looks like we'll never be able to decrypt Grandfather's message."

"Don't give up so easily," said Jenny. "Maybe there are some patterns we haven't seen yet. Let's take a look at the messages we just decrypted."

"In the boys' message, **KVX** appears 4 times," Evie observed. "It was decrypted as **the** each time." Evie underlined **KVX** each time it occurred.

"And look," said Abby, "**GLAUVF 99** appears 3 times. It was decrypted as **number 99** each time." She underlined **GLAUVF 99** each place it occurred.

"How could that be?" thought Lilah out loud. "I thought a Vigenère cipher encrypted and decrypted the same letters differently."

"Sometimes," said Jenny, "but not if the same letters of the keyword are above them. Let's look at an example."

ROT ROTROTR OT R	OTRO TROTRO
the manager at a boat-rental	
KVX DOGRUX! OM R PHRH-KVBMZRZ	
TROTROTROTROT ROTR OT ROT ROTR OT	
CONCESSION WENT TO THE edge OF	
VFBVVGLZCG NSGK HH KVX VRZV CY	
ROT ROTR OTR OTROTR OTRO	
the LARE AND YELLED. BOAT	
KVX CODY OGU MXCZXU. PHRH	
TROTROT TROT ROTR OTRO TROT	
NUMBER 99. COME BACK YOUR TIME	
GLAUVF 99. VFAX SOVB. MHLF MZAX	
RO TR OTR OTR OTRO TROT R	
IS UP. BUT TH BOAT didn't	
ZG NG. PINK H-V PHRH WZ-G'K	

In the boys' message (the first few lines are shown above), the word **the** appears several times. Whenever the keyword letters **ROT** are above **the**, the word **the** is encrypted as **KVX**. In the fifth line, however, the keyword letters **OTR** are above **the**, so it is encrypted differently.

"Isn't it just a coincidence when the same keyword letters line up above the same word?" asked Evie.

"Maybe it is more than a coincidence," said Jenny. "Maybe we can find a pattern." Jenny was always on the lookout for patterns.

"Look at this," said Abby. She divided the letters into blocks that had the same keyword letters above them (*facing page*).

"The keyword **ROT** fits exactly 13 times, from the first **the** to the second **the**. Since **ROT** has 3 letters, the first **the** and second **the** are $13 \times 3 = 39$ letters apart." Abby didn't have to count the letters—she multiplied instead.

"**ROT** fits exactly 3 times from the second **the** to the third **the**, so they are encrypted the same way. They are $3 \times 3 = 9$ letters apart."

ROT	ROT	ROTR	ROT	R	OTRO	TROT	ROT
the	man	wander	er	at	a	boat-	rental
KVX	DOGRUXI	I	OM	R	PHRH-	KVBM	RZ
TROT	TROT	TROT	ROTR	OT	ROT	ROTR	OT
concession	on	Went	to	the	edge	of	
YFBIVGLZCG	NSGK	HH	KVX	VRZV	CY		
ROT	ROTR	OTR	ROT	ROTR	ROT	OTRO	
the	Lake	and	yelled,	"boat	"	PHRH	
KVX	CODY	OGL	MXCZXU,	"			
TROT	TROT	TROT	ROTR	OTRO	TROT		
number	99,	come	back,	your	time		
GLAUVF	99,	VFAX	SOVB.	MHLF	MZAX		
RO	TR	OTR	OTR	OTRO	TROT	R	
is	up.	*but	the	boat	didn't		
ZG	NG.	*	PNK	HAV	WZRG.	K	

"The distance between repetitions of **ROT** is a multiple of 3," Jenny noticed. "So the letters of **ROT** will line up the same way above a repeated string of letters, such as **the**, if the distance between the strings is a multiple of 3."

"In other words," said Abby, "the letters line up the same way if 3 is a factor of the distance between the strings."

They had discovered something that would help them:

When the letters of the keyword line up the same way above a repeated string of letters, the distance between occurrences of the string is a multiple of the key length. In other words, the key length is a factor of the distance between occurrences of the string.

"The distance between **the** in the third line and **the** in the fifth line is 49, which is not a multiple of 3. So the blocks of 3 letters of **ROT** don't fit exactly between these occurrences. This is why **the** in the fifth line is encrypted differently from the rest."

★ TIP

To find the **distance** between repeated strings of letters, count the letters from the beginning of the first string up to (but not including) the beginning of the second. (Don't count punctuation or spaces.)

For example, in **XYZABCDXYZ**, the strings **XYZ** are a distance of 7 letters apart as counted here:

X Y Z A B C D X Y Z
1 2 3 4 5 6 7

 Do Problems 1 and 2 now.

PROBLEMS

(Workbook pages W49-W50)

These problems involve entries Meriwether Lewis wrote in his journal during the Lewis and Clark Expedition. (You might notice that the spelling is not always the same as modern-day spelling, but we show it as it originally was written.)

1. Sunday, May 20, 1804

"We set forward... to join my friend companion and fellow labourer Capt. William Clark, who had previously arrived at that place with the party destined for the discovery of the interior of the continent of North America.... As I had determined to reach St. Charles this evening and knowing that there was now no time to be lost I set forward in the rain... and joined Capt Clark, found the party in good health and sperits."

- a. Find all occurrences of **the** in the message above. Include examples such as "**there**" in which **the** occurs as part of a word.
- b. Find the distance between the last two occurrences of **the** in the last sentence. (Don't count punctuation or spaces.)
- c. Choose a keyword from RED, BLUE, ARTICHOKEs, and TOMATOEs that will encrypt in exactly the same way the last two occurrences of **the** in the last sentence of the message. Use it to encrypt:
"the rain... and joined Capt Clark, found the party"
- d. Choose a keyword from RED, BLUE, ARTICHOKEs, TOMATOEs that will encrypt in different ways the two occurrences of **the** in the phrase from **1c**. Then use it to encrypt:
"the rain... and joined Capt Clark, found the party"
- e. Of the keywords you have not used, which would encrypt the two occurrences of **the** in the phrase in the same way? In different ways? Give reasons for your answers.

PROBLEMS

(Workbook pages W51-W52)

2. Wednesday, April 7, 1805

"We were now about to penetrate a country at least two thousand miles [3,219 kilometers] in width, on which the foot of civilized man had never trodden; the good or evil it had in store for us was for experiment yet to determine, and these little vessels contained every article by which we were to expect to subsist or defend ourselves.... I could but esteem this moment of my departure as among the most happy of my life."

- a. Find the occurrences of **the** in the above message.
- b. Find the distance from **the** in the second line to **the** in the third line. List all keyword lengths that would cause these words to be encrypted the same way.
- c. Find the distance from **the** in the third line to **these** in the fourth line. List all keyword lengths that would cause **the** in these strings to be encrypted the same way.
- d. What keyword length(s) would cause all three occurrences of **the** described in **2b** and **2c** to be encrypted the same way?
- e. Choose the keyword from the following list that will cause all three occurrences of **the** described in **2b** and **2c** to be encrypted the same way:
PEAR, APPLE, CARROT, LETTUCE, CUCUMBER, ASPARAGUS,
WATERMELON, CAULIFLOWER
- f. Copy the message beginning with the last **the** in the second line and ending with **these** in the fourth line. Write your chosen keyword above this part of the message. Encrypt each occurrence of **the** (you don't have to encrypt the entire message).

"So far we have only looked at repeated strings of plaintext to understand what's going on," said Jenny. "We need to look for patterns in ciphertext if we are trying to crack a message."

"Maybe we can look at the distances between repeated strings in the message and work backward to figure out what the key length must be. We can factor the distances to see what the possibilities are," said Abby.

"Is the key length always a factor of the distance between repeated strings of ciphertext?" asked Tim.

"Let's look at another message and find out," suggested Evie. "The message we sent the boys had a different key length than theirs. Let's take a look at that."

 **Do Problem 3 now.**

PROBLEMS

(Workbook pages W54-W55)

3. a. Find strings of letters that repeat in the girls' message from pages 70–72.
b. Complete a table like the one below. Include the strings shown in the table as well as the strings you found in 3a.

Repeated Strings in the Girls' Message			
String	Distance between repetitions	Is key length a factor of distance?	Number of times keyword fits between repetitions
XKM	136	YES	34
XKM	68		
XKM	20		
XKM	100		

Z.MF (in line 13)

- c. Is the key length *always*, *usually*, or *sometimes* a factor of the distance between strings?

Cracking Grandfather's Message

After looking at messages they had encrypted, the Cryptoclub members wrote the following rule:

The distance between a pair of repeated strings in a Vigenère message is usually a multiple of the key length.

"The word 'usually' in our rule bothers me a little," said Abby. "Can't we find a rule that works every time?"

"No, but with other clues from the message we will know if we are on the right track," said Jenny. "Let's try to use this pattern to guess the keyword length in Grandfather's message."

First they looked for repeated strings of letters.

A VNNS SGIAV GVDJRI! WG OOF AB GZS UAZYK
PRZWAV HUW HESRVFU CGGG GB GZS AADVYCA
JWIWF NL HUW BBJHUWFA LWC GT YSYR KICWFVGF.
JZWYW VVCWAY, W SGIAV GBES FZWAQ GGGBRK.
ZNLSE A PEGITZH GZSZ LC N ESGSZ
RPDRJH GG VNNS GZSZ SDCJOVKSQ. KIEW SAGITZ,
HUWM NJS FAZIWF—VF O IWFL HIEW TBJA.
GZSEW AHKH OW ABJS—V OWYD FRLIEF OAV
GGSYR S QYSWZ.

Grandfather's message.

String that repeats	Distance between occurrences
VNNS	162
SGIAV	105
GZS (5 times)	30 90 24 51
GGG	76
SYR	162
HUW (4 times)	
IWF (3 times)	
IEW	
GITZ	
ZWA	

Repeated strings in Grandfather's message.

GZS occurs five times. The distance between the first and second occurrence is 30 letters, between the second and third is 90 letters, between the third and fourth is 24 letters, and between the fourth and fifth is 51 letters.

They expected that each of these distances is a multiple of the key length. That means the key length is a factor of each of the distances. To find the factors, they wrote the prime factorization of each of the distances:

$$\begin{array}{ll} 30 = 2 \times 3 \times 5 & 90 = 2 \times 3^2 \times 5 \\ 24 = 2^3 \times 3 & 51 = 3 \times 17 \end{array}$$

The only common factor is 3, so a good guess would be that the key length is 3.

"Wait," said Tim. "Three is probably the key length, but we might as well look at the other strings we found just to see if they are also multiples of 3."

In the table on the left are the strings they found and some of the distances between them.

 **Do Problem 4 now.**

PROBLEMS (Workbook pages W56-W57)

4. a. Find some of the strings that repeat in Grandfather's message. Include at least two strings whose distances aren't in the table. Then find the distances between occurrences of those strings.
- b. For each distance in the table and the distances you found, tell whether 3 is a factor.
- c. How did you determine whether 3 is a factor of a number?
- d. Do you think 3 is a good guess for the key length of Grandfather's message? Why or why not?

The kids decided that 3 was a good guess for the key length for Grandfather's message. They divided the letters of the message into three groups. Then they divided up the work so that they each worked on cracking the part of the message made from letters in one of the groups. They used a different cipher wheel to decrypt the letters in each group.

Wheel 1: the 1st, 4th, 7th, ... letter of the message

Wheel 2: the 2nd, 5th, 8th, ... letter of the message

Wheel 3: the 3rd, 6th, 9th, ... letter of the message

They counted the letters in each group to see which letters were the most common. They made the table on the right.

 **Do Problem 5 now.**

"I had swim team practice when you were figuring all this out," said Peter the next day. "Can somebody explain how you figured out Grandfather's key length?"

"Sure," said Abby. "We found the distances between strings of letters that repeat in the message. We assumed that most of those distances were multiples of the key length."

"In other words," said Jenny, "we assumed that the key length was a factor of most of the distances."

"Right," said Tim. "So we factored each distance and looked for common factors."

 **Do Problems 6–10 now.**

PROBLEMS (Workbook pages W58–W59)

5. Decrypt Grandfather's message. To save time, use the information in the table below. (It is a long message, so you might want to share the work.) What keyword was used?

	Most common letters
Wheel 1	W, G, Z, J
Wheel 2	S, W, H, I
Wheel 3	G, A, R, V
English	e, t, a, i

★ TIP

A good guess for the length of the keyword is a common factor of distances between repeated strings of letters.

PROBLEMS

(Workbook page W60)

In Problems 6–8, Grandfather's message is encrypted using a different keyword each time. The goal is to find the key lengths. (You don't have to decrypt the message since you already know it.) A table next to each message shows repeated strings and the distances between some of them. For each message:

- Find at least three pairs of repeated strings, including at least two whose distances are not in the table. Then find the distances between occurrences of those strings.
- Factor the distances in the table and the new distances you found.
- Make a reasonable guess about what the length of the keyword might be. Explain why your answer is reasonable.

6. O VLYK TZXTR DLRJPU! OH HDY WY WNS
SLRZD EKVTOQJ HSH ZFLGOBR SUGE RT HSH
TWALMCY UOJPU GH EKK BZUZVPUT HTS
UT WDQS DXVSCLUF. HKOZP KOYTQM, W
QRABO VUAP VNWB YHZQKG. WDZSC L
HFZXMVE WNSX WU O XHZOW HDDPUZ HZ
KGJP WNSX DVDCDOGPG. YICH KBZXMV,
EKKM LUK GTOBSC—LT O GHXM AXXS QRXA.
EKKFP PAGE EK AZUK—W HLRZ CHZICQ GBO
VZOVA G QWDQA.

Strings that repeat in message 6	Distance between occurrences
JPU	52
WNS (occurs 3 times)	120
HSH	
EKK (occurs 3 times)	120
WNSX	24
ZXMV	
LRZ	208

PROBLEMS

(Workbook pages W61-W62)

7. A LCMI YGYPU WBDZGI! MM OEU ZR MZI
JZPEK FGYMGV XJV XKSHKEK IGWV FR
MZI PZTBYS P IMOWV CK XAW RQIXAWVP
KMI GJ NROX KYRVVBGV. YYMEW LKBMGY,
M HFYGV WQDI LZMPP WMGRGJ. PTLIT Z
FKGYIYX MZIO KS T EIVRP XPTGIX MG LCMI
MZIO RTIJEKJIW. KYTV IGGYIY, XAWC CII
LAPXVV—BF E XVVR HYTV JHJQ. VYIKW
QWJX UW QQII—B OMNC VXLYTE EGV WVROX
S GNRMF.

Strings that repeat in message 7	Distance between occurrences
LCMI	162
MZI (occurs 4 times)	90
XAW (occurs 3 times)	114
ROX	162
MZIO	
YTV	
GYIY	
XVV	

8. I WPGI FDJYH SXAGIR! XI HES XC ELE
WXWPS QTSMNS ISI TGPOMV EZWT DC
ELE CXAMGDC CMVTG LX TWT YSRIWPVN
IXA SF APVI SJEPVIDG. HLIAT SMKXCR,
M FDJYH SDBP WHXCJ WTDCPW. LPIPV I
QGZYGWI ELEB IZ E MTILP EMEPVT ID SEVT
ISIM PEAVAXHHPH. SJGP INDJRL, TWTJ ERT
HTPVTG—TR A KTCC PJGP JOGB. ELEG T XYSI
QP QOGT—T AIAA CITJGY ENS HEEKT P
NPAXB.

Strings that repeat in message 8	Distance between occurrences
FDJYH	105
ELE (occurs 4 times)	90
ISI	130
VTG	120
TWT	
PVI	135
PVT	
JGP	
EPV	

PROBLEMS

(Workbook pages W64-W66)

9. Here is another message encrypted with a Vigenère cipher. Collect data to guess the key, then crack the message. Tell what keyword you used. *The workbook gives suggestions for sharing the work with your class.*

ECF DXS GHXM NOKJPU. ECF FXONNKRL YOUPQKFP
FODSHX. DPRVZP XYSO WU HSLTY EKGH HDY
WXSUGDLHZP. VU MZX YVZXRR MH BSCB VFZXJ. MZX
ICFOJ PP D YSNUKH LJKBE. PGMMH ECF VNCFQJ
HCB ECFU YYTORG ZQ ZVP EKOWH IWAKKFD. QUPZGE
VLV IFLFQSO WNSX BKH, MXZ WQ BUI OR, ECF
POUSW JWFDFUJPU G HCHGGFUK KZUVZ XLRZTRTG ZI
JCWOGFD.

10. Describe in your own words how to crack a Vigenère cipher when you do not know anything about the keyword.

The Rest of the Story

"Mom! Mom!" Jenny and Abby blurted out as soon as they got home.
"Grandfather found silver—we found a secret message he wrote, and we cracked it!"

"Oh, that," said their mother.

"What do you mean? Aren't you excited? Don't you believe us?"

"Oh, I believe you. But there isn't much we can do about it. He found it but lost it years ago. It's an old story that has been in the family for years."

"The note was probably from Grandfather's grandfather—he was quite an adventurer. When he was a young man, he joined the Canadian Coast Guard and was stationed on Lake Superior. Once, when he had shore leave, he went hiking along the Nipigon River, at the northern tip of the lake. There was a trading post there, but not much else at that time. He climbed the ridge up behind the trading post, but night came quicker than he expected and he couldn't return in the dark. So he spent the night in a cave.

"The next morning, he noticed some strange-looking rocks in the cave. He collected a few, then hurried back to his ship. When his ship arrived in Montreal, he had the rocks appraised and was told they were extremely valuable ore, very rich in silver. Everyone wanted to know where he had gotten them, but he put them away and kept the secret, always planning to return.

"Many years later, he returned with his son—my grandfather—to the Nipigon River on vacation. They spent three weeks searching where he remembered finding the silver—in the hills behind the trading post—but they found nothing. On the last day of their vacation, they met an old fisherman on the dock in front of the trading post, and Grandfather's grandfather mentioned he had been there 20 to 30 years before. The fisherman said, 'Oh, I guess you don't know about the fire. The trading post used to be on the other side of the river, but it burned down several years ago. They rebuilt it on this side of the river.'

"So they had spent their entire vacation looking for silver on the wrong side of the river! They didn't have time to go back and look again, and they never had a chance to return.

"The story stayed in the family, and when I was a little girl, my father took us to the Nipigon area on vacation, only to find that a high dam has been built there. All the landmarks are gone, and probably underwater. So your great-great-grandfather's treasure may never be found."

DO YOU KNOW?

The One-Time-Pad and Atomic Spies

If the keyword of a Vigenère cipher is as long as or longer than the message, there aren't any patterns, and the cipher is impossible to break. But it is important that the keyword be used only once, otherwise patterns can be found and the cipher can be broken.

When German diplomats began using this system in the 1920s, they put their keys on pads of paper with different keys on each sheet. When a sheet was used for a message, it was torn off the pad and never used again. The system became known as the one-time pad. It is still used today, since it is the only unbreakable cipher system.

The type of pads used in one-time pad ciphers varies. One Russian agent was captured with a booklet the size of a postage stamp. Some pads have been found in scroll form. Spies have had clever ways of hiding their one-time pads: Some spies have hidden several scrolls in the base of a cigarette lighter.

If the one-time pad is unbreakable, why doesn't everyone use it? One reason is that it is difficult to get the keys to the users, since a user needs a new key every time he or she sends a message. In wartime, hundreds of thousands of words are encrypted each day. It would be impossible to supply that many keys and to keep track of which ones have been used. But the one-time pad system is used by governments to communicate with their spies.

During a period in the 1940s, the Russians didn't follow the important rule that the keyword must be

CONTINUED ON NEXT PAGE >

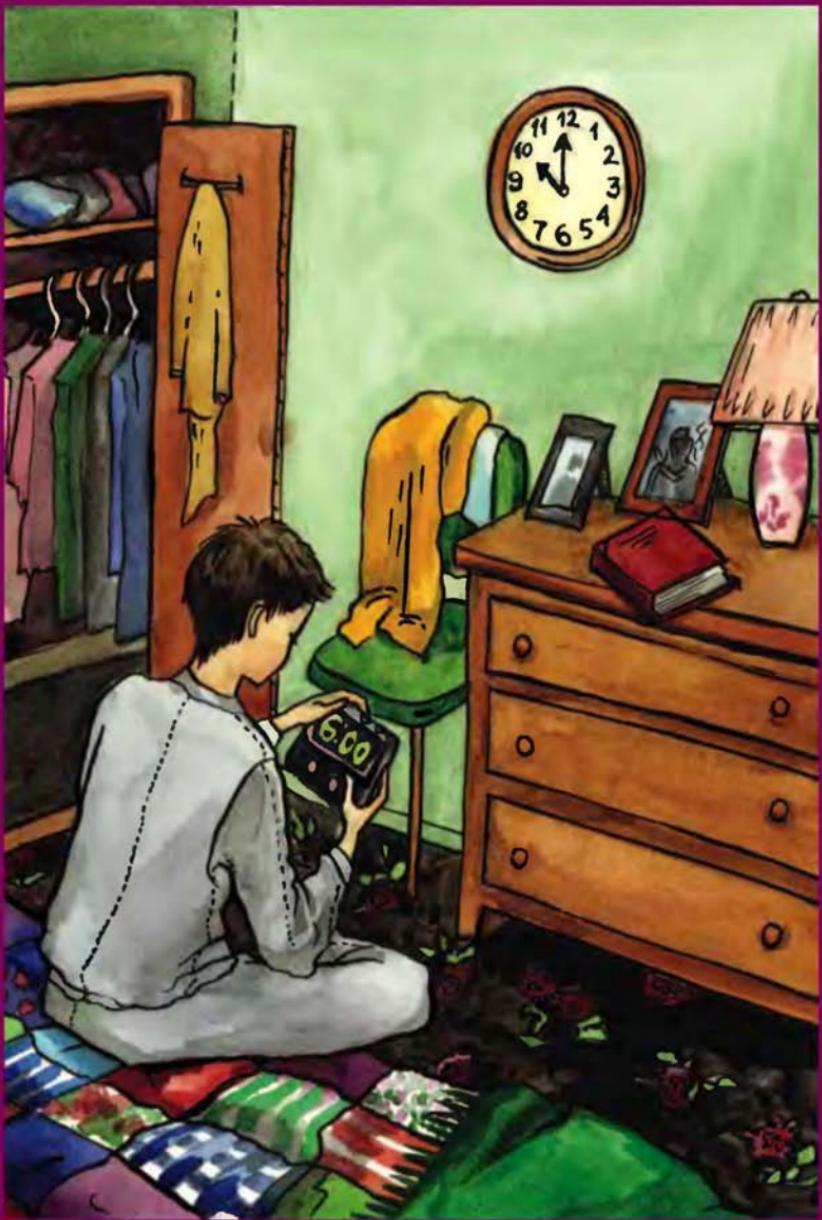
used only once. We don't know exactly why – maybe they had trouble getting new one-time pads to each other during wartime and had to reuse their old pads. Or maybe the manufacturer made a mistake and printed the same pad twice. Whatever the reason, whether knowingly or not, they sent out messages using the same keyword more than once. This put just enough patterns into their messages that American cryptanalysts were able to break some of the messages. By breaking these messages, the United States government learned the names of some important American and British spies who were giving atomic secrets to the Russians. The spies were arrested. This code-breaking effort was part of the VENONA program, which lasted from 1943 until 1980 and wasn't fully revealed to the public until 1995.

Unit 4



Modular (Clock) Arithmetic

Chapter 11



Introduction to Modular Arithmetic

Tim was always asking questions. He wondered about the reasons things are the way they are. He often asked, “Why?” Usually his teacher encouraged his curiosity, but one busy day she just didn’t have time. When Tim asked another one of his questions, she answered him in a frustrated way. “Tim,” she said, “some things are *always* true. You just have to accept that.” Then she continued, “2 plus 2 is *always* 4, 4 plus 4 is *always* 8, and 8 plus 8 is *always* 16.”

Instead of accepting what his teacher said, Tim took her words as a challenge. He was determined to think of an example to prove that the things she had listed are *not* always true. He started thinking about arithmetic, hoping to come up with an example. He was still thinking about it as he got ready for bed that night. “It’s 10 PM now,” he said. “If I want to sleep for 8 hours, I should set my alarm to wake me up at 6 AM.”

“That’s it! In clock arithmetic, $10 + 8$ hours = 6 AM. So $10 + 8$ is *not* always 18! My teacher said 8 plus 8 is *always* 16, but in clock arithmetic $8 + 8 = 4$. I can’t wait to tell her tomorrow!”



Tim reported his example to his class the next day. They all agreed that addition in clock arithmetic is pretty strange. When the sum is less than 12, clock addition is just like regular addition. For example, $6 + 3 = 9$. But when the sum is greater than 12, we start counting again with 13 equal to 1. For example, $6 + 7 = 1$ (in clock arithmetic).

Do Problems 1–6 now.

PROBLEMS
(Workbook page W67)

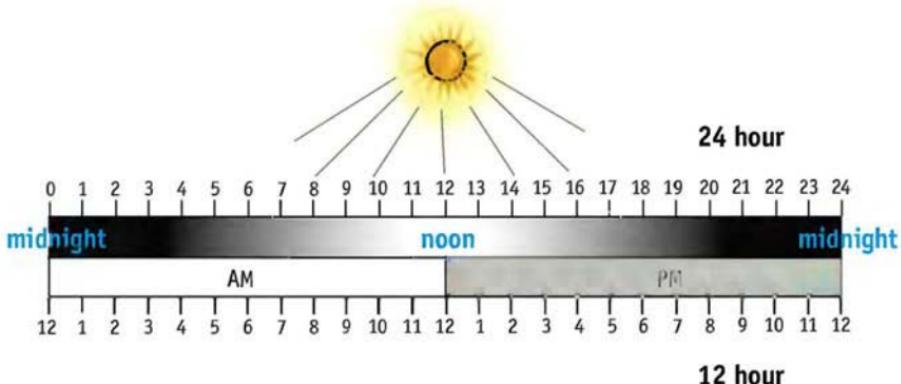
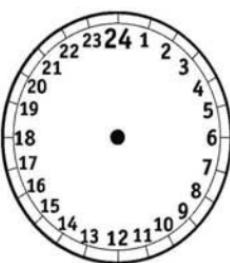
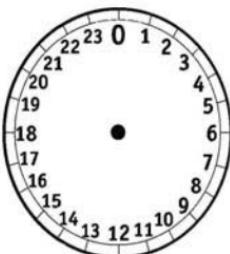
1. Lilah had a play rehearsal that started at 11:00 AM on Saturday morning. The rehearsal lasted three hours. What time did it end?
2. Peter was traveling with his family to visit their grandmother and their cousins, Marla and Bethany, near Pittsburgh. The car trip would take 13 hours. If they left at 8:00 AM, at what time would they arrive in Pittsburgh?
3. The trip to visit their other grandmother takes much longer. First they drive for 12 hours, then stop at a hotel and sleep for about 8 hours. Then they drive about 13 hours more. If they leave at 10:00 AM on Saturday, when will they get to their grandmother's house?
4. Use clock arithmetic to solve the following:
 - a. $5 + 10 = \underline{\hspace{2cm}}$
 - b. $8 + 11 = \underline{\hspace{2cm}}$
 - c. $7 + 3 = \underline{\hspace{2cm}}$
 - d. $9 + 8 + 8 = \underline{\hspace{2cm}}$
5. Jenny's family is planning a 5-hour car trip. They want to arrive at 2 PM. At what time should they leave?
6. In Problem 5, we moved backward around the clock. This is the same as subtracting in clock arithmetic. Solve the following subtraction problems using clock arithmetic. Use the clock, if you like, to help you:
 - a. $3 - 7 = \underline{\hspace{2cm}}$
 - b. $5 - 6 = \underline{\hspace{2cm}}$
 - c. $2 - 3 = \underline{\hspace{2cm}}$
 - d. $5 - 10 = \underline{\hspace{2cm}}$

24-Hour Time

Peter asked Abby one of his favorite old riddles. "What time is it when the clock strikes thirteen?" Abby thought about it, but had no idea of the answer—all of the clocks in her house only went up to twelve. "It is time to get a new clock," he said.

Peter's riddle assumes that a clock that has a 13 on it must be broken. But actually, there are clocks that have numbers for all of the 24 hours in the day.

On a **24-hour clock**, a different number is used for every hour. The hours before noon are numbered from 1 to 12 as usual, but the afternoon and evening hours are different—they are numbered from 13 to 24. So, 13:00 hours means 1 PM, 14:00 hours means 2 PM, and so on, up to 24:00 hours. Midnight can be numbered either 0 or 24.



With a 24-hour clock, you don't need to say AM or PM—you can tell whether the time is AM or PM simply by whether it is less than or greater than 12.

It is not hard to convert between 12-hour and 24-hour time. Morning hours are the same in both systems. To convert afternoon and evening hours, you just have to add or subtract 12.

For example, to convert 9 PM to 24-hour time, add: $9 + 12 = 21$. So, 9 PM is the same as 21:00 hours.

To find 16:00 hours in 12-hour time, subtract: $16 - 12 = 4$. So, 16:00 hours is the same as 4 PM.

The 24-hour system is widely used in Europe and is becoming increasingly common in the United States. It is often used for train and bus schedules to avoid confusion. Sometimes it is called “military time” because it is the system used by military agencies.

 **Do Problems 7–11 now.**

PROBLEMS

(Workbook pages W68–W69)

7. Write the following 12-hour times using the 24-hour system:
a. 3 PM b. 9 AM c. 11:15 PM
d. 4:30 AM e. 6:45 PM f. 8:30 PM
8. Write the following 24-hour times as 12-hour times, using AM or PM.
a. 13:00 b. 5:00 c. 19:15
d. 21:00 e. 11:45 f. 15:30
9. Use clock arithmetic on a 24-hour clock to solve the following:
a. $20 + 6 =$ _____ b. $11 + 17 =$ _____
c. $22 - 8 =$ _____ d. $8 - 12 =$ _____
10. Solve the following on a 10-hour clock:
a. $8 + 4 =$ _____ b. $5 + 8 =$ _____ c. $7 + 7 =$ _____
d. $10 + 15 =$ _____ e. $6 - 8 =$ _____ f. $3 + 5 =$ _____
11. **Challenge:** Is $2 + 2$ always 4? Find a clock for which this is not true.



Modular Arithmetic

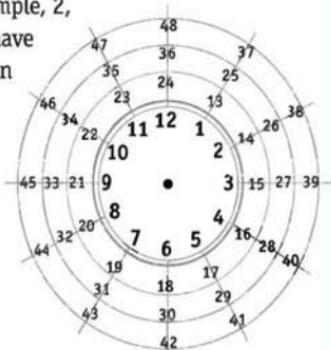
Tim wrote down the answers to some of his clock arithmetic problems. Abby saw his calculations.

"What has happened to you?" she said. "These answers are all wrong!"

"The answers aren't wrong," said Tim defensively. "I'm not using regular arithmetic. There must be some way to write these problems to make it clear that I did them in clock arithmetic."

Their teacher showed them a way. She told them that another term for clock arithmetic is **modular arithmetic**. The word "modulus," or the shorter word "mod," is used to show which size clock to use. For example, the expression "mod 12" means use a 12-hour clock, "mod 10" means use a 10-hour clock, and so on. We could write the answer to the problem $8 + 4 = \underline{\hspace{2cm}}$ as $8 + 4 = 2 \pmod{10}$ to make it clear that we used clock arithmetic.

To understand modular arithmetic, it helps to understand which numbers have the same position on your clock. For example, 2, 14, 26, and 38 all have the same position on the 12-hour clock.



Do Problems 12–14 now.

PROBLEMS

(**Workbook page W70**)

- 12. a.** The figure shows numbers wrapped around a 12-hour clock. List all numbers between 1 and 48 that have the same position on a 12-hour clock as 3.
b. If the number wrapping continues, what numbers between 49 and 72 would have the same position on a 12-hour clock as 3?
- 13. a.** List all numbers between 1 and 48 that have the same position on a 12-hour clock as 8.
b. If the number wrapping continues, what numbers between 49 and 72 would have the same position on a 12-hour clock as 8?
- 14. a.** How can you use arithmetic to describe numbers that have the same position on a 12-hour clock as 5?
b. What numbers between 49 and 72 have the same position on the 12-hour clock as 5?

There is a special term in modular arithmetic to describe numbers that have the same position on a clock. Two numbers are **equivalent mod n** if they differ by a multiple of n —in other words, if they have the same position on a clock of size n . For example, 37 and 13 are equivalent mod 12 because their difference, $37 - 13 = 24$, is a multiple of 12.

The symbol “ \equiv ” means “is equivalent to.” Using this notation,

$$37 \equiv 13 \pmod{12}.$$

This notation includes mod 12 in parentheses to tell us what clock the numbers are on.

The symbol “ \equiv ” reminds us of the equal sign “ $=$ ” but it is a little different. Equivalent numbers are alike because they have the same position on the clock, but they don’t have to be equal, so we use a slightly different symbol.

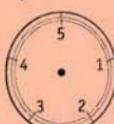
PROBLEMS

(Workbook page W71)

15. List three numbers equivalent to each number.
- $6 \pmod{12}$
 - $9 \pmod{12}$

16. List three numbers equivalent to each number.
- $2 \pmod{10}$
 - $9 \pmod{10}$
 - $0 \pmod{10}$

17. List three numbers equivalent to each number.
- $1 \pmod{5}$
 - $3 \pmod{5}$
 - $2 \pmod{5}$



Another term for “equivalent mod n ” is **congruent mod n** . You may have learned the word “congruent” in geometry. Congruent triangles are alike because they have the same size and shape. In both geometry and modular arithmetic, “congruent” means things are alike in certain specific ways.

You can find numbers equivalent, or congruent, to another number by adding multiples of the modulus. For example, 13, 25, 37, and 49 are all equivalent mod 12 to 1 since they are all 1 plus a multiple of 12.

$$1 + 1 \times 12 = 13$$

$$1 + 2 \times 12 = 25$$

$$1 + 3 \times 12 = 37$$

$$1 + 4 \times 12 = 49$$

Do Problems 15–17 now.

Reducing mod n

When we work mod n , we often use only the numbers from 0 to $n - 1$. If another number comes up, we **reduce mod n** , which means we replace it with the number between 0 and $n - 1$ that is equivalent mod n to it. This is the remainder when we divide by n .

For example, 37 is equivalent mod 12 to the numbers 1, 13, 25, and so on. Of these, the number in the range from 0 to 11 is 1, so reducing 37 mod 12 gives 1.

It is useful to have a notation that means reduce, or find the remainder. We will use mod n without parentheses for this. So 37 mod 12 means the remainder when we divide 37 by 12. Also, when we reduce, we use the equal sign and not the equivalence symbol. We write

$$37 \bmod 12 = 1.$$

Abby thought she understood modular arithmetic, but she wasn't sure she understood reducing.

Jesse said, "Let's work out a problem. Let's reduce 40 mod 12.

"Since we're working mod 12, we need to find the number from 0 to 11 that is equivalent to 40 mod 12. One way to do that is to subtract 12 repeatedly until we get a number between 0 and 11."

$$\begin{array}{r} 40 \\ - 12 \\ \hline 28 \\ - 12 \\ \hline 16 \\ - 12 \\ \hline 4 \end{array}$$

"We stop when we get to a number less than 12, in this case 4."

"Hmm," said Abby, "wouldn't it be faster to subtract a multiple of 12? The greatest multiple of 12 less than 40 is $3 \times 12 = 36$, and $40 - 36 = 4$."

"Yes," said Jesse, "and another way is to divide and find the remainder:

$$\begin{array}{r} 3R4 \\ 12 \overline{)40} \end{array}$$

"All these methods lead to the same answer: $40 \bmod 12 = 4$."

Negative numbers work in modular arithmetic, too, if you think about going backward on a clock. For example, $-3 \bmod 12 = 9$. We get this by counting back 3 hours from 12 on a 12-hour clock. Another way is to add 12 until we get a number between 0 and 11:

$$-3 + 12 = 9.$$

Do Problems 18–24 now.

PROBLEMS

(Workbook pages W72–W73)

18. Reduce each number.

- a. $8 \bmod 5$ b. $13 \bmod 5$ c. $6 \bmod 5$ d. $4 \bmod 5$

19. Reduce each number.

- a. $18 \bmod 12$ b. $26 \bmod 12$ c. $36 \bmod 12$ d. $8 \bmod 12$

20. Reduce each number.

- a. $8 \bmod 3$ b. $13 \bmod 6$ c. $16 \bmod 11$ d. $22 \bmod 7$

21. Reduce each number.

- a. $-4 \bmod 12$ b. $-1 \bmod 12$ c. $-6 \bmod 12$ d. $-2 \bmod 12$

22. Reduce each number.

- a. $-4 \bmod 10$ b. $-1 \bmod 10$ c. $-6 \bmod 10$ d. $-2 \bmod 10$

23. Reduce each number.

- a. $-3 \bmod 5$ b. $-1 \bmod 5$ c. $8 \bmod 5$ d. $7 \bmod 5$

24. Reduce each number.

- a. $-2 \bmod 24$ b. $23 \bmod 20$ c. $16 \bmod 11$ d. $-3 \bmod 20$

CLASS ACTIVITY: The Mod Game

- Divide the class into teams. (Four to seven teams is a good number.) Each team sends a representative to stand in a line facing the class.
- One of the teams chooses a number between 10 and 30. Students in the line “count off” 1, 2, 3,... up to that number.
- The student who calls out the last number wins a point for his team.

Sample: Suppose there are four teams, T1, T2, T3, and T4. If the number 11 is chosen, then the counting stops at T3 as shown below. Team 3 wins a point.

T1	T2	T3	T4
1	2	3	4
5	6	7	8
9	10	11	

- Another team chooses a number, and the counting is repeated.
 - After you have played for a while, divide the class into a different number of teams and play again.
-

DO YOU KNOW?

How the United States Entered World War I

When war broke out in Europe in 1914, the United States did not immediately get involved. Hoping to keep it that way, Germany's foreign minister, Arthur Zimmermann, came up with a plan to make sure that the United States was too busy at home to get involved with a war in Europe. He decided to convince the president of Mexico to invade the United States and reclaim the "lost" Mexican territories, including Texas, New Mexico, and Arizona.

Zimmermann described his plan in a secret message to the German ambassador in Washington, who was to pass it on to the Mexican president. Unfortunately for the Germans, he had to send the message through cables that touched Great Britain, and the British government intercepted it. They saw immediately that the message was encrypted at a level used only for top-secret communications, so they knew they had to decrypt it.

After British cryptographers decrypted the message, they wanted the Americans to know what it said so the Americans would join the war on their side. However, they didn't want the Germans to know they had broken the German code, so they devised a clever plan. The British knew the message would need to be decrypted before it was given to the Mexican president, so they sent a special agent to steal the message again, but this time, after it had been decrypted. This version of the telegram was given to the United States, and the British never had to tell anyone that they knew how to decrypt German messages. To make sure no one suspected them of intercepting the encrypted message

CONTINUED ON NEXT PAGE >

and breaking the code, the British even planted a newspaper story criticizing their secret service for not intercepting the Zimmermann telegram!

When President Woodrow Wilson read Zimmermann's message, he saw that Germany was encouraging direct aggression against the United States. On April 2, 1917, President Wilson asked Congress to declare war on Germany, and four days later they did.

Chapter 12



Applications of Modular Arithmetic

"I think we've been using modular arithmetic in our ciphers without knowing it," said Tim.

"I think you're right," agreed Lilah. "When we used Caesar ciphers, we wrote the letters as numbers and then added to encrypt. But if the sums were greater than 25, we substituted 0 for 26, 1 for 27, and so on. That's just like reducing mod 26."

Tim and Lilah were right. Using modular arithmetic, they could write

$$26 \bmod 26 = 0$$

$$27 \bmod 26 = 1$$

$28 \bmod 26 = 2$, and so on.

To reduce a negative number mod 26, you add 26 to get a number in the range 0 to 25.

$$-1 \bmod 26 = 25$$

$$-2 \bmod 26 = 24$$

$-3 \bmod 26 = 23$, and so on.

 **Do Problems 1–3 now.**

PROBLEMS (Workbook page W75)

1. Reduce the following numbers mod 26:

- a. 29 b. 33 c. 12
d. 40 e. -4 f. 52
g. -10 h. -7

Use multiplication to make a cipher. The rule for encrypting is given in the table below.

2. Encrypt the name "Jack" using the times-5 cipher. The first two letters are done for you.

Times-5 Cipher	J	a	c	k
change letters to numbers (use cipher strip)	9	0		
multiply by 5	45	0		
reduce mod 26	19	0		
change numbers to letters	T	A		

PROBLEMS

(Workbook page W75)

3. Encrypt “cryptography” using the times-3 cipher as described in the table below. The first two letters are done for you.

Times-3 Cipher	c	r	y	p	t	o	g	r	a	p	h	y
change letters to numbers (use Cipher strip)	2	17										
multiply by 3	6	51										
reduce mod 26	6	25										
change numbers to letters	G	Z										

154

- 26

128

- 26

102

- 26

76

- 26

50

- 26

24

$$154 \text{ mod } 26 = 24.$$

Tim and his friends decided to use what they called the times-11 cipher. They changed letters to numbers, multiplied by 11, and reduced mod 26. But multiplying by 11 gave some pretty large numbers. They had to figure out how to reduce these numbers mod 26. For example, to encrypt the letter **m**, which corresponds to 14, they computed $11 \times 14 = 154$. Then they needed to reduce 154 mod 26. How would you solve this problem?

Dan decided to subtract 26 over and over (*left*), until he got an answer less than 26.

Jenny decided to divide by 26, since the remainder is the desired answer. In this method, $154 \div 26 = 5 \text{ R } 24$, so $154 \text{ mod } 26 = 24$. You can divide using long division or using a calculator. (For tips on how to use a calculator to find the remainder, see the next section.)

Lilah decided to subtract a multiple of 26 from 154. Multiples of 26 are 26, 52, 78, 104, 130, 156, In this problem, 130 is the largest multiple you can subtract from 154. Since $154 - 130 = 24$, $154 \text{ mod } 26 = 24$. (If you subtract a smaller multiple of 26, for example, 104 instead of 130, you would have to keep subtracting until you get a number less than 26.)

Jesse decided to estimate the number of times 26 goes into 154 and subtract that many 26s from 154. He guessed 26 goes into 154 about 5 times, since he knew that 5×30 is 150. He calculated $5 \times 26 = 130$ and subtracted this from 154. If his guess had been too low, he could have subtracted more until his answer was less than 26.

All of their methods gave the same answer, $154 \text{ mod } 26 = 24$, which corresponds to the letter **Y**. In the times-11 cipher, **m** is encrypted as **Y**.

Do Problems 4 and 5 now.

Using a Calculator to Find Remainders

To find $154 \text{ mod } 26$, Tim and Abby wanted to divide and find the remainder. They could do this using long division, but instead they chose to use their calculators. With their calculators, they found that

$$154 \div 26 = 5.9230769$$

The calculator expressed the remainder as a decimal, but they wanted it expressed as a whole number. Tim and Abby used two different methods to find the whole number remainder from the decimal remainder.

Tim thought, “The calculator answer tells that there are 5 groups of 26 in 154, plus some left over. (The leftover amount is the decimal 0.9230769.) The 5 groups of 26 are $5 \times 26 = 130$. This leaves $154 - 130 = 24$ left over. Therefore $154 \div 26 = 5 \text{ R } 24$. So $154 \text{ mod } 26 = 24$.”

PROBLEMS (Workbook page W76)

4. Reduce each number.

- a. $175 \text{ mod } 26$
- b. $106 \text{ mod } 26$
- c. $78 \text{ mod } 26$
- d. $150 \text{ mod } 26$

5. Reduce each number. (Hint: Try subtracting multiples of 26 such as $10 \times 26 = 260$.)

- a. $586 \text{ mod } 26$
- b. $792 \text{ mod } 26$
- c. $541 \text{ mod } 26$
- d. $364 \text{ mod } 26$

Abby thought, "The calculator answer is 5.9230769. To get the decimal remainder, I'll subtract off the 5." (This is better than retyping the decimal part, since it saves the extra places stored in the calculator that help prevent round-off error.)

$$5.9230769 - 5 = 0.9230769$$

"I know that a decimal remainder is computed by dividing the remainder R by the divisor. In this case, the divisor is 26, so

$$\frac{R}{26} = 0.9230769.$$

"To solve this, I'll multiply both sides by 26:

$$26 \times \frac{R}{26} = 0.9230769 \times 26.$$

"This gives

$$R = 24."$$

Abby discovered that when she found remainders this way she didn't always get whole number answers for R . She knew that was because of calculator round-off during division. This didn't happen often, but when it did, she adjusted her answer by rounding it to the nearest whole number.

 **Do Problems 6–8 now.**

PROBLEMS

(Workbook pages W76–W77)

6. Use a calculator to help you reduce the following.
 - a. 254 mod 24
 - b. 500 mod 5
 - c. 827 mod 26
 - d. 1500 mod 26
 - e. 700 mod 9
 - f. 120 mod 11
7. Reduce each number.
 - a. 500 mod 7
 - b. 1000 mod 24
 - c. 25,000 mod 5280
 - d. 10,000 mod 365
8. Choose one of the numbers you reduced in Problem 6. Write how you would explain to a friend the way you reduced your number.

Shortcut For Multiplying mod 26

Tim wanted to encrypt his name using the times-11 cipher. He started to multiply by 11 and reduce modulo 26, but working with these numbers turned out to be very tedious. For example, to encrypt **Y**, he multiplied $24 \times 11 = 264$. To reduce this he could divide 264 by 26 and find the remainder, but this was more work than he wanted to do. He thought of a shorter way: He realized that $24 \equiv -2 \pmod{26}$. Multiplying by congruent numbers gives the same answer in modular arithmetic, so

$$\begin{aligned}11 \times 24 &\equiv 11 \times (-2) \pmod{26} \\&\equiv -22 \pmod{26} \\&\equiv 4 \pmod{26}.\end{aligned}$$

Do Problem 9 now.

Calendar Applications for Modular Arithmetic

The kids' teacher told them that modular arithmetic is useful for solving problems that involve cycles, such as calendar problems. She asked them, "If today is Sunday, what day of the week will it be in 50 days?"

Suppose you think of Sunday as Day 0, Monday as Day 1, etc. Then the numbers 0 to 6 represent the seven days of the week. Day 7 is Sunday again. Every day whose number is $0 \pmod{7}$ is Sunday. Every day whose number is $1 \pmod{7}$ is Monday, and so on. Since $50 \pmod{7} = 1$ (why?), the fiftieth day is Monday.

Do Problems 10–15 now.

TIP: Tim's Shortcut for Multiplying modulo 26

If the multiplication is messy, subtract 26 to get a number that (1) is congruent mod 26 to your number and (2) might be easier to work with.

PROBLEMS (**Workbook page W77**)

9. Encrypt "trick," using the times-11 cipher. Use Tim's shortcut when it makes your work easier.

Times-11 Cipher	t	r	i	c	k
change letters to numbers					
multiply by 11					
reduce mod 26					
change numbers to letters					

PROBLEMS

(Workbook page W78-W80)

10. Astronauts left on a Sunday for a mission into space. On what day of the week would they return if they were gone for

- a. 4 days? b. 15 days? c. 100 days? d. 1000 days?

11. If today is Wednesday, what day of the week will it be in

- a. 3 days? b. 75 days? c. 300 days?

Leap Years. There are 365 days in a year, except for leap years. In a leap year, an extra day (February 29) is added, making 366 days. Leap years occur in years divisible by 4, except at the beginning of some centuries. Years that begin new centuries are not leap years unless they are divisible by 400. So 1900 was not a leap year but 2000 was.

12. a. 2004 was a leap year. What are the next two leap years?

- b. Which of the following century years are leap years?

1800, 2100, 2400

- c. Which of the following years were leap years?

1996, 1776, 1890

13. If the Fourth of July is on Tuesday this year, on what day of the week will it be next year? (Assume that next year is not a leap year.) Explain how you got your answer.

14. a. What is today's day and date?

- b. What day of the week will it be on today's date next year? Your answer will depend on whether or not a leap year is involved. Explain how you got your answer.

15. a. On what day and date will your next birthday be? (You may use a calendar.)

- b. On what day of the week will your twenty-first birthday be? Answer without using a calendar. Don't forget about leap years. Explain how you got your answer.

DO YOU KNOW?

Non-Secret Codes

Not all codes are secret codes. For example, the International Standard Book Numbers (ISBNs) on books and Universal Product Codes (UPCs) on other products are designed to store information in a form easily understood by a computer. But this information is not meant to be secret.

Codes often store more information than just the name of the product. For books published before 2007, the ISBN is a 10-digit number divided into four parts. The first part tells the country or language area in which a book is published (0 or 1 represents English-speaking countries such as the United States, the United Kingdom, Australia, etc.). The second part identifies the publisher, and the third part is assigned by the publisher to identify the book itself. The last part, the tenth digit, is a special digit, called the check digit. It can help to check whether a mistake is made in typing or sending the number. It is not surprising that mistakes are sometimes made, but it might surprise you that the codes are designed to detect mistakes.

After the first nine digits of a book's ISBN are assigned, the check digit is chosen so that the sum of 10 times the first digit, plus 9 times the second digit, plus eight times the third, and so on, up to 1 times the tenth digit is equivalent to 0 mod 11. In other words, that sum is a multiple of 11. The number on the back of this book is ISBN 1-56881-223-X. The X stands for 10 (the check digit must be only one digit, so X is used in place of 10). You can check that

$$\begin{aligned}(10 \times 1) + (9 \times 5) + (8 \times 6) + (7 \times 8) + (6 \times 8) \\ + (5 \times 1) + (4 \times 2) + (3 \times 2) + (2 \times 3) + (1 \times 10) \\ = 242 \equiv 0 \text{ mod } 11.\end{aligned}$$

CONTINUED ON NEXT PAGE >

DO YOU KNOW? (CONTINUED)

Non-Secret Codes

Suppose someone tried to order this book but made a mistake and typed ISBN 1-56881-223-6 instead. The computer would calculate

$$(10 \times 1) + (9 \times 5) + (8 \times 6) + (7 \times 8) + (6 \times 8) + \\ (5 \times 1) + (4 \times 2) + (3 \times 2) + (2 \times 3) + (1 \times 6) = 238.$$

Since this is not a multiple of 11, the computer would warn that the number typed is incorrect – it couldn't possibly be the ISBN for a book.

Beginning in 2007, the ISBNs will be 13-digit numbers. This is because 10-digit numbers are running out. A three-digit prefix will be added to the front, the way area codes are added to phone numbers. Future printings of this book will have 978 added to the front, and the check digit will change. Instead of multiplying the first digit by 10, the second by 9, and so on, the new check digit will be determined by multiplying the first digit by 1, the second by 3, the third by 1, the fourth by 3, and so on, alternating 1 and 3. The check digit will be the number needed to make the sum a multiple of 10 (instead of 11, as in the old scheme). Thus the number of this book will become ISBN 978-1-56881-223-6 because

$$(1 \times 9) + (3 \times 7) + (1 \times 8) + (3 \times 1) + (1 \times 5) \\ + (3 \times 6) + (1 \times 8) + (3 \times 8) + (1 \times 1) + (3 \times 2) \\ + (1 \times 2) + (3 \times 3) + (1 \times 6) = 120,$$

which is a multiple of 10.

The ISBN code can detect errors, but some codes are so sophisticated that they can do more than that. Some codes can actually correct the errors. There is an entire field of mathematics devoted to the study of error-correcting codes.

Unit 5



Multiplicative and Affine Ciphers

Chapter 13



Multiplicative Ciphers

"I especially liked the ciphers we used that involved numbers," said Peter. "In the Caesar cipher we added numbers to encrypt. We've made a few ciphers by multiplying. Will that always work?"

"Let's make some tables," said Lilah, "and see what happens."

They built a times-3 cipher that multiplies the numbers by 3. As an example, they encrypted the letter **c**. The number for **c** on the cipher strip is 2, so they multiplied 2 times 3 and got 6. Since 6 is the number for **g**, they encrypted **c** as **g**. They encrypted the letter **i** as **Y** because the number for **i** is 8, $3 \times 8 = 24$, and 24 corresponds to **Y**.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$\times 3$

$\times 3$

They started to make a table for the times-3 cipher. The table on the next page shows that the letter **a** is encrypted as **A**, **b** is encrypted as **D**, **c** as **G**, and so on.

Do Problems 1–4 now.

plaintext:	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
numbers:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$\times 3 \pmod{26}$:	0	3	6	9	12	15	18	21	24	1	4	7														
ciphertext:	A	D	G	J	M	P	S	V	Y	B	E	H														

Times-3 cipher.

PROBLEMS

(Workbook pages W81-W83)

1. a. Complete the times-3 cipher table. (Tip: You can use patterns such as counting by 3s to multiply quickly.)
 b. Decrypt the following message Evie wrote with the times-3 cipher.
 JAN, Y ENQO OVAF UQI OZQFM.
 c. What has one foot on each end and one foot in the middle? (It was encrypted using the times-3 cipher.)
 A UAZJCFYGE
2. a. Make a times-2 cipher table.
 b. Use the times-2 cipher to encrypt the words **ant** and **nag**. Is there anything unusual about your answers?
 c. Make a list of pairs of letters that are encrypted the same way using a times-2 cipher. For example, **a** and **n** are both encrypted as **A**, **b** and **o** are both encrypted as **C**.
 d. Make a list of several pairs of words that are encrypted the same way using the times-2 cipher.
 e. Decrypt **KOI** in more than one way to get different English words.
 f. Does multiplying by 2 give a good cipher? Why or why not?
3. a. Make a times-5 cipher table.

Use the times-5 cipher table to decrypt the next two quotations.

- b. FU MWHU QSW XWR QSWH ZUUR ON RJJU HOEJR
 XDAKU, RJUN MRANP ZOHI.

—Abraham Lincoln

PROBLEMS

(Workbook pages W83-W84)

3. c. RJJU OIXSHRANR RJONE OM NSR RS MRSX CWUMROSNONE.

—Albert Einstein

4. a. Make a times-13 cipher table.

b. Encrypt **input** and **alter** using the times-13 cipher.

c. Does multiplying by 13 give a good cipher? Why or why not?

"When we multiply numbers by 3, every product is different," said Lilah. "But when we multiply by 2, some letters have the same encryption. So multiplying by 2 doesn't give a good cipher."

In a multiplicative cipher, the number by which you multiply determines the cipher. Therefore, this is the key. We'll call a number a **good key** if it encrypts every letter differently. The number 3 is a good key, but 2 is not.

"I wonder what makes some numbers good keys and some numbers bad keys," said Dan. "Let's see if we can figure out a pattern."

CLASS ACTIVITY

Workbook pages W85-W86

Work in groups to determine which numbers from 1 to 25 make good keys for multiplicative ciphers. Your group should:

- Choose one even number and one odd number between 4 and 25 to investigate. One number should be large, the other small. (Groups that finish early can work on the numbers not yet chosen.)
- Make cipher tables using your numbers as multiplicative keys. Decide which of your numbers make good multiplicative keys (that is, which numbers encrypt every letter differently).
- Pool your information with the rest of the class. Describe a pattern that tells which numbers give good keys.

The kids combined efforts and found which numbers made good keys and which made bad keys. Their pattern involved the factors each number had in common with 26.

"Since our pattern involves common factors, it reminds me of the term **relatively prime** that we learned in math class," Dan remembered. "This might be a place to use that term."

Numbers that do not have any common factors except 1 are said to be **relatively prime** to each other. For example 15 and 26 are relatively prime, but 15 and 20 are not, since 5 is a common factor. Note that numbers can be relatively prime to each other even if they aren't prime numbers.

"OK," said Lilah, "using that term, we would say that a number is a good key if it is relatively prime to 26."

You might wonder why multiplying by a key that has a factor in common with 26 causes the alphabet to repeat. Let's take a closer look. Let's try multiplying by 10:

$$10 \times 0 = 0$$

$$10 \times 1 = 10$$

$$10 \times 2 = 20$$

$$10 \times 3 = 30 \equiv 4 \pmod{26}$$

It seems OK so far, but when we reach 13 (a factor of 26), we start to repeat:

$$10 \times 13 = 5 \times 2 \times 13 = 5 \times 26 \equiv 0 \pmod{26}$$

So 0 and 13 are encrypted the same. That's because one of the factors of 26 (in this case 13) combined with one of the factors of 10 to get 26. But that is not all. The numbers continue to repeat, with 14 encrypted like 1, 15 encrypted like 2, and so on:

$$10 \times 14 = 10 \times (13 + 1) = (10 \times 13) + (10 \times 1) \equiv 0 + 10 \pmod{26} \equiv 10 \pmod{26}$$

$$10 \times 15 = 10 \times (13 + 2) = (10 \times 13) + (10 \times 2) \equiv 0 + 20 \pmod{26} \equiv 20 \pmod{26}$$

$$10 \times 16 = 10 \times (13 + 3) = (10 \times 13) + (10 \times 3) \equiv 0 + 30 \pmod{26} \equiv 4 \pmod{26}$$

This cannot be good, since a cipher must encrypt every letter (number) differently. The whole problem arose because 10 and 26 shared a factor.

"I've been thinking," said Jesse. "My grandfather is from Russia. He said there are 33 letters in the Russian alphabet. If we made a multiplicative cipher for a message in Russian, would the same numbers be good keys as in English?"

"I don't think so," said Dan. "For example, 13 would be a good key for Russian because 13 is relatively prime to 33. But 13 is a bad key for English."

Dan was right. Not all languages have 26 letters in their alphabets. For alphabets of different sizes, the numbers that make good keys are different. The general rule is

A number is a good key for a multiplicative cipher if it is relatively prime to the size of the alphabet.

"We don't even have to go to different languages to need different keys," said Lilah. "Sometimes I like to include symbols for punctuation in my messages. So if I include a period (.), comma (,), question mark (?), and blank space () in my encryption table, along with the 26 English letters, I would have an 'alphabet' of 30 letters to encrypt. My good keys would be different from those for the 26-letter alphabet.

 **Do Problems 5–9 now.**

PROBLEMS

(Workbook page W87)

5. Which of the following pairs of numbers are relatively prime?

- a. 3 and 12
- b. 13 and 26
- c. 10 and 21
- d. 15 and 22
- e. 8 and 20
- f. 2 and 14

6. a. List 3 numbers that are relatively prime to 26.

- b. List 3 numbers that are relatively prime to 24.

PROBLEMS

(Workbook pages W87-W91)

7. Which numbers make good multiplicative keys for each of the following alphabets?
- Russian; 33 letters
 - Lilah's "alphabet", which consists of the 26 English letters and the period, comma, question mark, and blank space
 - Korean; 24 letters
 - Arabic; 28 letters. This alphabet is used to write about 100 languages, including Arabic, Kurdish, Persian, and Urdu (the main language of Pakistan).
 - Portuguese; 23 letters

8. Compute the table for each cipher, then decrypt the quote.

- a. Times-7 cipher

UKP OXAPAODCP EW YXAD YC VU YXCN YC DXENS NU
UNC EW ZUUSENQ.

—H. Jackson Brown, Jr.

- b. Times-9 cipher

PLK EWGP KZLAYGPUNC PLUNC UN VUTK UG JKUNC
UNGUNSKXK.

—Anne Morrow Lindbergh

- c. Times-11 cipher

IS GNYI IZAB IS AFS, LMB NYB IZAB IS CAE LS.

—William Shakespeare

- d. Times-25 cipher (Hint: $25 \equiv -1 \pmod{26}$.)

HTW ZWUSNNSNU SI HTW OMIH SOLMJHANH LAJH
MV HTW EMJQ.

—Plato

PROBLEMS

(Workbook page W92)

9. Look at your cipher tables from Problem 8.

a. How was a encrypted? Will this be the same in all multiplicative ciphers? Give a reason for your answer.

b. How was n encrypted?

Challenge: Show that this will be the same in all multiplicative ciphers. Hint: Since all multiplicative keys are odd numbers, every key can be written as an even number plus 1.

DO YOU KNOW? Passwords

Many people use the Internet to pay their bills. If you do this, you must use a password to gain access to your bank account. You wouldn't want just anyone to be able to get into your account – they might take out your money without your permission.

Did you ever wonder what would happen if someone stole the file of passwords of all the banks' customers? Would that person be able to use those passwords to get access to all the accounts? Don't worry – the bank isn't careless enough to store the passwords in a way that anyone else can use them. It encrypts the passwords and stores only the encrypted form.

When you type your password to access your account, the computer encrypts what you type and compares it to the encrypted form of your password that it has stored. If it matches, you are allowed access. But if someone steals the file of passwords, he only has your encrypted password. When he types it, the computer encrypts what he types. But it won't match what is stored (since he didn't start with your plaintext), so the hacker won't gain access to your account.

You don't have to worry about someone stealing your stored password, but you do have to be careful to choose a good password. If you choose something obvious like your birthday, someone might guess it. If you use a regular word like "BIRD", then a hacker might find it by trying all words in the dictionary until he finds a match – computers can do this quickly. To avoid this, it is a good idea to mix numbers and letters in your password, for example, 1B2I3R4D. That won't be in the dictionary.

Chapter 14



Using Inverses to Decrypt

Each meeting of the Cryptoclub began with a short treasure hunt. Today it was Tim's turn to hide the treasure. He found two good places before the others arrived and put a surprise in each place. He wrote **DYS DAS** and **FQT CVMHP** on the board as clues about where to look.

"I used a multiplicative cipher with key 3," he explained as the others arrived. "I challenge you all to crack it without using your times-3 cipher tables."

Abby started thinking. "When we used addition to encrypt, we subtracted to decrypt," she reasoned. "So if Tim used multiplication to encrypt, maybe we can divide to decrypt."

"Let's decrypt **DYS DAS** first," Abby suggested. She changed the letters to numbers and got 3, 24, 18 3, 0, 18.

"Now we divide each number by 3 and see what we get." Abby did this and her answer was 1, 8, 6 1, 0, 6.

Abby changed the numbers back to letters and got **big bag**. And there in the corner of the room she saw the big bag. She looked inside and found the treasure Tim had hidden there.

"That wasn't hard. Now let's try Tim's second clue," said Evie. She started to work on **FQT CVMHP**. She began with **F**, the first letter.

"F corresponds to 5. Tim multiplied some number by 3 to get 5 mod 26, so I'll divide 5 by 3 to get back that number," Evie explained.

"But how can you do that?" asked Becky. "5 ÷ 3 isn't even a whole number."

"That's a problem," agreed Evie. "In mod 26, we only have the whole numbers from 0 to 25."

"Then how can we divide in mod 26?" asked Becky.

That wasn't so obvious.

"There is more to think about than I realized," said Evie. But she was determined to figure it out.

Inverses

In regular arithmetic, the way to undo multiplication by 3 is to divide by 3. We can show this with arrows,

$$5 \xrightarrow{\times 3} 15 \xrightarrow{\div 3} 5,$$

or as an equation,

$$(5 \times 3) \div 3 = 5.$$

Another way is to multiply by $\frac{1}{3}$, since multiplying by $\frac{1}{3}$ is the same as dividing by 3. The arrows show that we start and end with the same number:

$$5 \xrightarrow{\times 3} 15 \xrightarrow{\times \frac{1}{3}} 5$$

We can also show this as an equation:

$$(5 \times 3) \times \frac{1}{3} = 5$$

Multiplying first by 3 and then by $\frac{1}{3}$ gives us back what we started with! That's because, from the Associative Property, you can multiply in any order.

$$(5 \times 3) \times \frac{1}{3} = 5 \times (3 \times \frac{1}{3})$$

Multiplying $5 \times (3 \times \frac{1}{3})$ is the same as multiplying 5×1 , since $3 \times \frac{1}{3} = 1$.

The **multiplicative inverse** of 3 is the number n that solves

$$3 \times n = 1.$$

The multiplicative inverse of 3 is $\frac{1}{3}$, since $3 \times \frac{1}{3} = 1$. The multiplicative inverse of $\frac{1}{5}$ is 5 because $\frac{1}{5} \times 5 = 1$.

In regular arithmetic, the multiplicative inverse of a number is its **reciprocal**. To find the reciprocal (and therefore the inverse) of a fraction you turn the fraction upside down. For example, if you write 3 as the fraction $\frac{3}{1}$, you can turn it upside down to get its reciprocal, $\frac{1}{3}$.

Do Problems 1 and 2 now.

"Tim multiplied by 3 and reduced mod 26 to encrypt his clue," reviewed Becky. "Since dividing gave us problems, we could multiply by the inverse of 3 to get back what he started with."

"But we don't have $\frac{1}{3}$ in modular arithmetic," said Abby. "We only have whole numbers."

"Maybe there is another number that acts like an inverse," said Becky, "a number that gives 1 mod 26 when you multiply it by 3."

The **mod 26 inverse of 3** is the number from 0 to 25 that solves

$$3 \times n \equiv 1 \pmod{26}.$$

Abby started multiplying to see whether there is such a number:

$$3 \times 1 = 3$$

$$3 \times 2 = 6$$

$$3 \times 3 = 9$$

$$3 \times 4 = 12$$

PROBLEMS (Workbook page W93)

1. Compute the following in regular arithmetic.

a. $2 \times \frac{1}{2}$

b. $\frac{1}{4} \times 4$

c. $7 \times \frac{1}{7}$

2. Complete:

a. $3 \xrightarrow{\times 2} 6 \xrightarrow{\times \frac{1}{2}} ?$

b. $6 \xrightarrow{\times 3} 18 \xrightarrow{\times \frac{1}{3}} ?$

c. $2 \xrightarrow{\times 5} 10 \xrightarrow{\times ?} 2$

d. $4 \xrightarrow{\times 6} 24 \xrightarrow{\times ?} 4$

$$3 \times 5 = 15$$

$$3 \times 6 = 18$$

$$3 \times 7 = 21$$

$$3 \times 8 = 24$$

$$3 \times 9 = 27 \equiv 1 \pmod{26}$$

"That's it," exclaimed Abby. "3 times 9 is 1 mod 26. So 9 is the mod 26 inverse of 3."

"Let's test 9 to see if it works like an inverse," said Becky cautiously.

They multiplied 4 by 3, then multiplied the answer by 9 and reduced mod 26. They got back the number they started with!

$$4 \xrightarrow{\times 3} 12 \xrightarrow{\times 9} 108 \equiv 4 \pmod{26}$$

PROBLEMS (Workbook pages W93-W94)

3. Test Abby's theory that if you multiply by 3 and then by 9 (and reduce mod 26) you get back what you started with:

a. $6 \xrightarrow{\times 3} 18 \xrightarrow{\times 9} 162 \equiv ? \pmod{26}$

b. $2 \xrightarrow{\times 3} ? \xrightarrow{\times 9} ? \equiv ? \pmod{26}$

c. $10 \xrightarrow{\times 3} ? \xrightarrow{\times 9} ? \equiv ? \pmod{26}$

4. Where was Tim's second treasure hidden? Finish decrypting his clue to find out.

"We found the inverse—we can use it to decrypt Tim's clues."

Abby and Becky had realized this important fact:

If a message is encrypted by multiplying by a key, then it can be decrypted by multiplying by the mod 26 inverse of the key.

The girls took another look at Tim's second clue, **FQT CVMHP**. The first letter, **F**, matched the number 5. Tim had multiplied by 3 to encrypt, so the girls multiplied by 9 to decrypt, since 9 is the mod 26 inverse of 3. They computed

$$5 \times 9 = 45 \equiv 19 \pmod{26}.$$

Then they changed 19 to the letter **t**. They had decrypted the first letter of Tim's clue.

 Do Problems 3 and 4 now.

plaintext:	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
numbers:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$\times 3 \text{ (mod 26):}$	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23

Times-3 cipher.

Finding Modular Inverses

Finding inverses in modular arithmetic is not as easy as it is in regular arithmetic, but there are ways to do it—some easy and some not. Since you have already computed many tables for multiplicative ciphers, you can use your tables to help find mod 26 inverses.

For example, at the top of this page is the multiplication table for the times-3 cipher. The bottom row gives the products of 3 times the numbers in the second row. This table shows that $9 \times 3 \equiv 1 \pmod{26}$. This tells us that 3 and 9 are inverses mod 26.

Do Problem 5 now.

Abby noticed that she could have found the inverse of 3 without listing all the products of 3. She already knew that $27 \equiv 1 \pmod{26}$, so she could have factored $27 = 3 \times 9$ to discover that 3 and 9 are inverses. To find other inverse pairs, she listed other numbers that were congruent to 1 mod 26 and looked for their factors. Here is her list of some numbers that are congruent to 1 mod 26:

27, 53, 79, 105, 131

She couldn't factor 53 or 79, because they are prime numbers, but she could factor 105. She found inverse pairs from its factors.

Do Problems 6 and 7 now.

PROBLEMS (Workbook page W95)

5. Look at the tables of multiplicative ciphers you have already worked out. Find the column that has 1 in the product row and use this to find other pairs of numbers that are inverses mod 26. Save these for later.

PROBLEMS (Workbook page W95)

6. Since $5 \times 21 = 105 \equiv 1 \pmod{26}$, 5 and 21 are inverses of each other (mod 26). Find another way to factor 105. Use this to find another pair of mod 26 inverses.
7. The following was encrypted by multiplying by 21. Multiply to decrypt. (Hint: See Problem 6 for the inverse of 21.)
- A UMXX BMNLO A UAK.
—Orison Swett Marden

PROBLEMS (Workbook pages W96–W97)

8. Find another inverse pair by looking at the negatives of the inverses we have already found.
9. What is the inverse of 25 mod 26? (Hint: $25 \equiv -1 \pmod{26}$.)
10.
 - a. Make a list of all the pairs of inverses you and your classmates have found. (Keep this list to help you decrypt messages.)
 - b. What numbers are not on your list? (Not all numbers have inverses mod 26.)
 - c. Describe a pattern that tells which numbers between 1 and 25 have inverses mod 26.
11. **Challenge.** Explain why even numbers do not have inverses mod 26.

You can find more inverses by looking at the negatives of the inverse pairs you already know. For example, $-3 \equiv 23 \pmod{26}$ and $-9 \equiv 17 \pmod{26}$. So 23 and 17 are inverses because

$$\begin{aligned}23 \times 17 &\equiv (-3) \times (-9) \pmod{26} \\&\equiv + (3 \times 9) \pmod{26} \\&\equiv 1 \pmod{26} \text{ (since 3 and 9 are inverses).}\end{aligned}$$

☞ **Do Problems 8–11 now.**

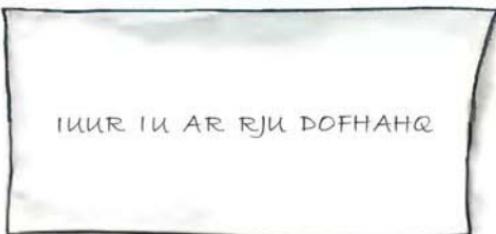
CLASS ACTIVITY: Play Cipher Tag Again

Play Cipher Tag. Encrypt a name or short message using a multiplicative cipher. Be sure to use a “good” key. Tell the class the key you used. They will have to decide how to decrypt. (Note: this time, encrypt and decrypt by multiplying, not by using the cipher tables.)

☞ **Do Problems 12–14 now.**

Cracking a Multiplicative Cipher

“I found this note that Evie sent to Abby,” said Dan. “She probably used a multiplicative cipher since that’s what we’ve been working on lately. The problem is I don’t know the key.”



"Let's see if we can crack it. A challenge is always fun," said Tim.

"A multiplicative cipher is a type of substitution cipher. If we do a frequency analysis, we might not need the key," said Dan.

"OK, let's look at the letter frequencies," agreed Tim. "The most common letter is **U**, so let's replace **U** with **e**. The next most common letter is **R**. A good guess is that **R** is **t**." He wrote his guesses above the message.

eet e t t e
IUUR IU AR RJU DOFHAHQ

"That is a good start, but the message isn't long enough to get enough information to guess all the letters," said Tim.

"Well, the word **t_e** is probably **the** and **_eet** could be **meet**. So let's try replacing **J** with **h** and **I** with **m**," said Dan.

This is what they got:

meet me t the
IUUR IU AR RJU DOFHAHQ

PROBLEMS

(Workbook pages W98-W99)

Solve problems 12 and 13 by multiplying by the inverse.

- 12.** What word is pronounced wrong by the best of scholars?

Answer (encrypted with a times-9 cipher):

16, 23, 22, 13, 2

- 13.** What's the best way to catch a squirrel?

Answer (encrypted with a times-15 cipher):

4, 9, 16, 24, 15 0
25, 21, 8, 8 0, 13, 19
0, 4, 25 9, 16, 20, 8
0 13, 14, 25.

- 14. Challenge:** Investigate inverses for one of the alphabets listed below. Find all pairs of numbers that are inverses of each other.

- Russian; 33 letters
- The English alphabet, and the period, comma, question mark, and blank space; 30 "letters"
- Korean; 24 letters
(Note: There is something unusual about the inverses for this alphabet.)

★ TIP

Beware of even numbers and 13—they can trick you. For example, suppose that you have a message in which you figure out that plaintext **e** encrypts as **Y**. Then, since **e** corresponds to 4 and **Y** corresponds to 24, you know that

$$\text{key} \times 4 \equiv 24 \pmod{26}.$$

You might think that 6 is the key since it is a solution to the equivalence, but 6 can't be a key for a multiplicative cipher since it is not relatively prime to 26. In this case, there is another solution, 19. (Check that $19 \times 4 \equiv 24 \pmod{26}$.) This is the only solution that could be a key.

To avoid this problem, choose a plaintext letter that corresponds to an odd number (except 13) when you write your equivalence.

"Maybe **A** is **a**, because then the message would begin **meet me at the**," said Tim.

"In fact, we know **A** *must* be **a** if it is a multiplicative cipher," agreed Dan. "But we just don't have enough information to figure out the last word."

"If it is a multiplicative cipher," said Tim. "We could use algebra to figure out the key Evie multiplied by. We guessed that when the plaintext is **m**, the ciphertext is **I**. Since **m** corresponds to 12 and **I** corresponds to 8, multiplying the key times 12 gives $8 \pmod{26}$:

$$\text{key} \times 12 \equiv 8 \pmod{26}.$$

"We could find the key by multiplying both sides by the inverse of 12."

"But 12 is an even number, so it doesn't have an inverse mod 26." Dan thought for a minute that Tim's method wouldn't work.

"OK, try another letter," said Tim. "We also guessed that plaintext **t** is encrypted as ciphertext **R**. Since **t** corresponds to 19 and **R** corresponds to 17,

$$\text{key} \times 19 \equiv 17 \pmod{26}.$$

"We can solve this because 19 *does* have an inverse—the inverse of 19 mod 26 is 11. We'll multiply both sides by 11 and use the fact that $19 \times 11 \pmod{26} = 1$.

$$\text{key} \times 19 \times 11 \equiv 17 \times 11 \pmod{26}$$

$$\text{key} \times 1 \equiv 187 \pmod{26}$$

$$\text{key} \equiv 5 \pmod{26}$$

"That means the encryption key is 5. To decrypt **DOFHAHQ**, we can multiply by the inverse of 5, which is 21. The first letter **D** corresponds to 3. Multiply by 21 to decrypt:

$$21 \times 3 = 63 \equiv 11 \pmod{26}.$$

"Since 11 corresponds to the letter **l**, we'll decrypt **D** as **l**."

☞ **Do Problems 15–17 now.**

PROBLEMS (Workbook pages W100–W102)

15. Where did Evie's note say to meet? Finish decrypting to find out.
16. The following messages were encrypted with multiplicative ciphers. A few letters in each message have been decrypted. For each message, write an equivalence that involves the key. Then solve the equivalence to find the key. Use the inverse of the key to help decrypt. Show your work.

a.

ite it e tt t ee
QXUPK UP WN IWYX LKAXP PLAP KHKXI

i t e e t i t e e
BAI UG PLK JKGP BAI UN PLK IKAX.

—Ralph Waldo Emerson

b.

the e t t hee e
ZBI PIKZ SAW ZC EBIIV WCOVKIJX OR QK

t t t hee e e e e
ZC ZVW ZC EBIIV KCYICNI IJKI OR.

—Mark Twain

PROBLEMS

(Workbook pages W103-W104)

17. For each of the following, find the most common letters in the message. Use this information or other reasoning to guess a few letters of the message. Then find the encryption key by solving an equivalence. Use the inverse of the key to help decrypt.

a. A HOYYCQCYV YOOY VFO RCLLCUSTVG CN
OPOBG KHHKBVSNCVG; AN KHVCQCYV YOOY VFO
KHHKBVSNCVG CN OPOBG RCLLCUSTVG.

—Winston Churchill

b. JTGAJ A SAN AO RG MO, ANL RG UMXX TGSAMN
AO RG MO. JTGAJ A SAN AO RG QIEXL VG, ANL RG
UMXX VGQISG URAJ RG ORIELX VG.

—Ralph Waldo Emerson

DO YOU KNOW?

The German Enigma Cipher

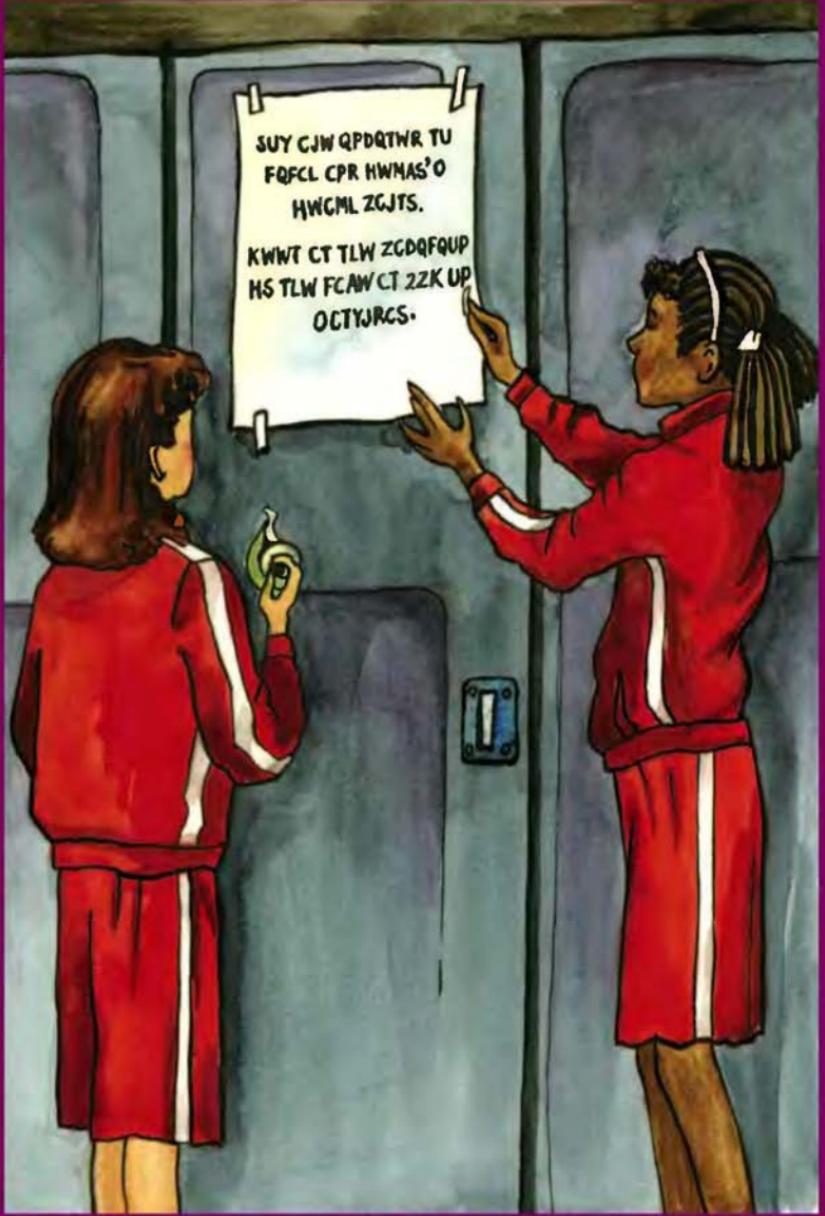
The skill of British cryptographers helped to win World War II. The British were able to figure out Germany's secret code – the Enigma cipher – without the Germans ever knowing. This enabled them to learn the location of German submarines. With this information, American ships carrying supplies to the British avoided the German submarines and reached Great Britain without being torpedoed.

CONTINUED ON NEXT PAGE >

To encode their messages, the Germans used an electro-mechanical machine called the Enigma. The Enigma looked somewhat like a typewriter, but had wheels and wires that worked together in a systematic and complicated way to encrypt the messages typed into it. In the 1930s Polish mathematicians, notably Marian Rejewski, analyzed German messages and learned to decrypt early versions of the Enigma cipher. Just before the Germans invaded Poland, the Poles sent the information they had about the Enigma to the British. British mathematician Alan Turing and others were able to build on the work of the Polish mathematicians and crack the new version of the cipher. The computations they used to decrypt the Enigma messages led to the building of the first electronic computer, the Colossus.

The capture of German submarines during the war greatly helped the effort to break the Enigma. One of the submarines captured by the Americans can be seen at the Museum of Science and Industry in Chicago, along with the Enigma machine and codebooks that were onboard at the time. On a tour of the submarine, you can see that the Enigma machine was kept in an important communications room, right across from the skipper's bed. Codebooks for encrypting and decrypting were locked in cabinets above his bed. The crew didn't have time to destroy the codebooks before capture, so the books and the machine were captured along with the sub. These books gave additional important information that helped the British break the cipher.

Chapter 15



Affine Ciphers

Dan and Tim decided they should change their cipher frequently to avoid having other people figure out their messages. They wondered how many different ciphers they could get by changing the keys in their additive (Caesar) and multiplicative ciphers.

Do Problems 1 and 2 now.

Dan and Tim decided that, even if they changed their keys every day, they wouldn't have many different ciphers—not even two months' worth. They wondered how many ciphers they could get if they combined multiplication and addition.

An **affine cipher** is a cipher that combines multiplication and addition. First you need to choose a good multiplicative key m (that is, an m that is relatively prime to 26) and an additive key b . Then the cipher is called an **(m, b) -affine cipher**, and the pair (m, b) is its **key**.

To encrypt with an (m, b) -affine cipher, multiply by m and add b . Then reduce mod 26.

PROBLEMS (Workbook page W105)

1. How many different additive ciphers are possible? That is, how many different numbers can be keys for additive ciphers? Explain how you got your answer.
2. How many different multiplicative ciphers are possible? That is, how many different numbers make good keys for multiplicative ciphers? Explain how you got your answer.

PROBLEMS

(Workbook pages W106–W107)

3. Encrypt the word “secret” using the (3, 7)-affine cipher.
4. Encrypt the word “secret” using the (5, 8)-affine cipher.
5. Some affine ciphers are the same as other ciphers we have already explored.
 - a. What other cipher is the same as the (3, 0)-affine cipher?
 - b. What other cipher is the same as the (1, 8)-affine cipher?
6. Suppose that Dan and Tim changed their key to get a different affine cipher each day. Would they have enough ciphers to have one for each day of the year? Explain.

To encrypt the letter **s** with a (3, 7)-affine cipher, first change **s** to 18. Then multiply by 3 and add 7. This gives $3 \times 18 + 7 = 61$. Reducing mod 26 gives 9, which corresponds to **J**.

We can use a mathematical formula to describe an affine cipher. After translating the letters to their corresponding numbers, we encrypt the plaintext number x with the ciphertext number Y using the formula

$$Y = (mx + b) \text{ mod } 26$$

Without the “mod 26,” you might recognize this as the equation for a line in regular arithmetic. “Affine” is a mathematical term used for equations of this form, so that is where this cipher got its name.

In the (3, 7)-affine cipher, $m = 3$ and $b = 7$. The encryption formula is $Y = (3x + 7) \text{ mod } 26$. We can use this formula to encrypt 18 (the number corresponding to **s**). Substituting $x = 18$, we have

$$\begin{aligned} Y &= (3 \times 18 + 7) \text{ mod } 26 \\ &= (54 + 7) \text{ mod } 26 \\ &= 61 \text{ mod } 26 \\ &= 9 \text{ mod } 26 \end{aligned}$$

Since 9 corresponds to the letter **J**, **s** is encrypted as **J**.

 **Do Problems 3–6 now.**

Decrypting Affine Ciphers

How would you decrypt a message that was encrypted with an affine cipher?

You could just “undo” the encryption steps, starting with the last step and going backwards. To undo addition, we subtract. To undo multiplication, we multiply by the inverse of the multiplicative key.

To decrypt an (m, b) -affine cipher, first subtract b , then multiply by the mod 26 inverse of m .

Let's look at the $(3, 7)$ -cipher we saw before and see if we can decrypt. We encrypted **s** by first multiplying by 3 and then adding 7. The answer was **J**. Let's start with **J** and go backward. First change **J** to 9. Then subtract 7 and multiply by 9, the mod 26 inverse of 3. This gives $(9 - 7) \times 9 = 18$. Reducing mod 26 still gives 18, which corresponds to **s**.

 **Do Problem 7 now.**

It was the end of the school year. The weather was nice. Lilah and Becky decided to have a party for the girls on their basketball team. After practice, they made an announcement. “We’re having a party. As soon as we know the final plans, we’ll post an encrypted invitation on Lilah’s locker. We’ll use an affine cipher with key $(5, 2)$. Remember the key but don’t tell anyone else.”

After finalizing their plans, they posted this sign on Lilah’s locker (*right*).

 **Do Problem 8 now.**

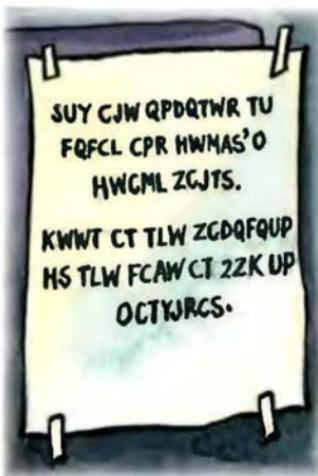
PROBLEMS

(Workbook page W107)

7. What insects are found in clocks?

Answer (encrypted with a $(3, 7)$ -affine cipher):

M F N L J



PROBLEMS

(Workbook page W108)

8. Decrypt the girls’ invitation.

Cracking the Cipher by Solving Equations

The boys had heard about the party. When they saw the encrypted invitation on Lilah's locker, they were determined to decrypt it. The Cryptoclub had been talking about affine ciphers lately so they figured that's what Lilah had used. But no one had talked about breaking affine ciphers yet. They decided to try.

"OK, we know that an affine cipher is of the form $Y = (mx + b) \text{ mod } 26$. If we can figure out m and b , we'll know the cipher they used and we'll be able to decrypt," said Tim.

"Can we figure out any part of the message?" Peter wondered.

"Maybe," said Tim. "Look at the number. It says '2 ZK.' Since 2 is the only number in the message, that might be the starting time. They couldn't start a party at 2 AM, so it must be 2 PM. So **p** must be encrypted as **Z** and **m** as **K**. Aha! That is useful information. Maybe we can use it to break the affine cipher."

"The number for **Z** is 25 and the number for **p** is 15," Tim continued. "Since we know that 25 is the encryption of 15, we know that

$$25 \equiv m \times 15 + b \pmod{26}.$$

"We also have the clue that the letter **m** is encrypted as **K**," said Peter. "This tells us that the number 12 is encrypted as 10, so we also have

$$10 \equiv m \times 12 + b \pmod{26}.$$

"We have two linear equivalences and two unknowns—we learned how to solve linear equations in math. Maybe equivalences work the same. Let's try."

The boys knew a couple of ways to solve a problem with two equations and two unknowns. They liked the method where they subtracted one equation from the other, so they tried that method with the equivalences.

$$\begin{aligned} 25 &\equiv 15m + b \pmod{26} \\ - (10 &\equiv 12m + b \pmod{26}) \\ 15 &\equiv 3m + 0 \pmod{26} \end{aligned}$$

Therefore,

$$15 \equiv 3m \pmod{26}.$$

They multiplied both sides by 9 (since 9 is the inverse of 3).

$$9 \times 15 \equiv (9 \times 3)m \pmod{26}$$

$$135 \equiv 1m \pmod{26} \text{ since } 9 \times 3 \equiv 1 \pmod{26}.$$

Since $135 \equiv 5 \pmod{26}$, they concluded that

$$5 = m.$$

They substituted $5 = m$ in the first equivalence. (They could have used the second equivalence and gotten the same answer.)

$$25 \equiv 5 \times 15 + b \pmod{26}$$

$$25 \equiv 75 + b \pmod{26}$$

$$-50 \equiv b \pmod{26}$$

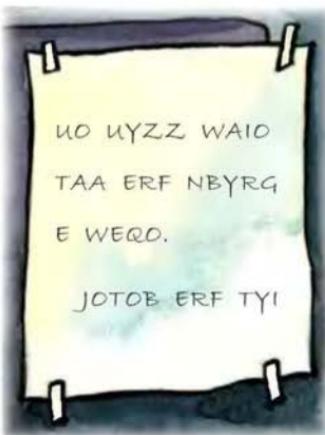
$$2 \equiv b \pmod{26}$$

"We did it," said Tim. "We figured out their encryption key—it is $m = 5$ and $b = 2$. So the girls' cipher must have been $Y = (5x + 2) \pmod{26}$. We'll decrypt by subtracting 2 and multiplying by the mod 26 inverse of 5, which is 21. Let's get busy and decrypt their message."

After cracking the girls' cipher, Peter and Tim encrypted their own message in a note to the girls. They posted their note (*right*) on Lilah's locker and waited to see whether the girls would figure it out.

You can use Peter and Tim's method to crack other affine ciphers. If you figure out two letters of the message, you can get two equivalences. Solve them like you solve equations in regular arithmetic, but don't divide. Instead, multiply by the modular inverses.

Sometimes you can figure out a few letters by looking at one-letter words or words with double letters. Sometimes you can guess words in the message such



as names. Other times you can do a frequency analysis to guess a few letters.

The method usually works pretty well, but a few problems could come up. You might guess letter substitutions that are incorrect and use them to write your equivalences. You could solve your equivalences correctly but get a value for m that isn't relatively prime to 26, so it couldn't be a key. This tells you to try a different letter substitution.

You might make a correct letter guess, but end up with an equivalence you can't solve because the coefficient doesn't have an inverse. (This situation also came up when cracking multiplicative ciphers.) You will avoid this problem if you choose one plaintext letter that corresponds to an odd number and one that corresponds to an even number when you write your equivalences (Peter and Tim used **p** and **m**, which correspond to 15 and 12). Then you will end up solving an equivalence that involves m times an odd number. You can solve this with inverses as long as the odd number is not 13.

 **Do Problems 9–11 now.**

PROBLEMS

(Workbook page W109)

9. Each of the following was encrypted with an affine cipher. A few letters have been decrypted. For each message, write equivalences involving the encryption key (m, b) . Solve the equivalences to find m and b . Then decrypt the message.

a.

e e en e e
MCZRN HZYJWDMI MPYAEN RY ICRWIVK MJMZK

n nee n e e n ee
GCP'I PMMD, LAR PYR MJMZK GCP'I EZMMD.

—Mahatma Gandhi

PROBLEMS

(Workbook pages W110-W113)

9. b.

i a a t a a i a a
S GY G UKWWMUU PORGQ BMWGKUM S XGR G

i i i a i
HZSMTR AXO BMDSMFMR ST YM GTR S

i t a t a t t t i
RSRT'P XGFM PXM XMGPZ PO DMP XSY ROAT.

—Abraham Lincoln

10. a. Guess a few letters of Peter and Tim's note on page 149, then solve two equivalences to find m and b .
b. Decrypt Peter and Tim's note.

11. Each of the following was encrypted with an affine cipher. Use letter frequencies or any other information to figure out a few of the letters. Write equivalences using the letter substitutions. Solve the equivalences to find the key (m, b) . Then decrypt.

a. BOIOINOB RAT ARZM TA KEM TPO BYGPT TPYRG YR TPO
BYGPT JZEWO, NCT XEB IABO FYXXWCZT KTYZZ, TA ZOELO
CRKEYF TPO UBARG TPYRG ET TPO TOIJTYRG IAIORT.

—Benjamin Franklin

b. RY XDP CBEJ BO BSSKJ BOU R CBEJ BO BSSKJ BOU TJ
JIFCBONJ ACJLJ BSSKJL ACJO XDP BOU R TRKK LARKK
JBFC CBEJ DOJ BSSKJ. QPA RY XDP CBEJ BO RUJB BOU R
CBEJ BO RUJB BOU TJ JIFCBONJ ACJLJ RUJBL, ACJO JBFC
DY PL TRKK CBEJ ATD RUJBL.

—George Bernard Shaw

DO YOU KNOW?

Atbash

A very early form of substitution occurs in the Hebrew Bible. It consists of interchanging the first letter, א (aleph), with the last letter, ת (tav), the second letter, ב (beth), with the next to the last letter ו (shin), and so on. In English, that would mean that **a** is interchanged with **z**, **b** is interchanged with **y**, and so on. You get the substitution table by writing the alphabet 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

The name Atbash itself describes the cipher. It tells how the letters are interchanged: aleph-tav-beth-shin. The sounds of these letters give us A-T-B-Sh, which is why we call it Atbash. If we gave the cipher a name in English by showing how the English letters are interchanged, it would be AZBY.

Biblical scholars think that Atbash was used in the bible to convey mystery, not to keep words secret. However, it inspired European monks in the Middle Ages to invent substitution ciphers, and that led to a renewed interest in cryptography in Europe.

Unit 6



Math for Modern Cryptography

Chapter 16



Finding Prime Numbers

The Cryptoclub had a planning meeting to talk about what to work on next.

"I think we should learn something more modern," said Jesse. "The ciphers we have worked with so far have been around for centuries."

"I agree," said Becky. "They were fun to learn about, but ciphers have to be more complicated today. Computers make the old ones too easy to crack."

Fortunately, Tim had been reading a bit about modern-day ciphers. "Well, the RSA cipher is probably the most widely known modern cipher," explained Tim. "It is named after Ronald Rivest, Adi Shamir, and Leonard Adleman, who invented it in 1977. It uses prime numbers—very large prime numbers—and it involves raising numbers to powers in modular arithmetic."

"Do we know enough math to learn about RSA?" wondered Jenny.

"I think we ought to review what we know about prime numbers," Tim said. "Especially larger prime numbers than we usually work with. Then we ought to practice raising numbers to powers in modular arithmetic. That is trickier than you might think, even with a calculator."

"OK, that sounds like plenty to do for the next few meetings," said Jenny. "When we're ready, we'll take a look at the details of RSA. Let's start with prime numbers."

The club members remembered some things about primes, and they knew some small prime numbers like 2 and 3, but Tim explained that to use RSA they would have to be able to find larger primes.

"I can't always tell whether a number is prime," said Peter. "I've been tricked by numbers that look prime but are not. My favorite example is 91. It looks prime to me and to most people I ask, but it turns out not to be prime: $91 = 7 \times 13$."

"You can tell whether a number is prime by testing whether it is divisible by any of the numbers that are smaller than it," said Becky.

"Sure, but that can be a lot of work if the number is large," said Peter. "Take 113, for example. It looks prime. But do I really have to test all the numbers up to 113 to find whether it has any factors besides itself and 1?"

"Why don't we check a few numbers and see what happens?" said Jenny. She got out her calculator.

"113 is not divisible by 2 since $113 \div 2$ is not a whole number. Besides, it isn't an even number so it can't be divisible by 2.

"113 is not divisible by 3 since $113 \div 3$ is not a whole number. Also, the sum of its digits is not divisible by 3.

"113 is not divisible by 4 since...."

"Wait—we don't have to test 4," Peter interrupted. "If 113 were divisible by 4, then it also would be divisible by 2. So we don't even have to check 4."

Jenny continued:

"113 is not divisible by 5 since $113 \div 5$ isn't a whole number. Besides, multiples of 5 always end with 0 or 5, so that's another reason I know 113 cannot be a multiple of 5.

"We don't have to check 6. If 113 were divisible by 6, it would have been divisible by 2 and 3. We already know it isn't."

"I see," Peter observed. "We only have to check the prime numbers to see if they divide 113. If 113 isn't divisible by a prime then it couldn't

be divisible by any multiple of that prime either. That is a pretty good shortcut.

"So to check whether 113 is prime," Peter continued, "Let's test every prime number less than 113. The next prime is 7."

"113 is not divisible by 7 since $113 \div 7$ is not a whole number."

"Wait," said Jenny. "Let's think before we do anymore calculations." Both Jenny and Peter had learned that thinking first often helps to cut the work. They liked math, but they liked to avoid extra work even more.

"The next prime is 11," Jenny thought out loud. "And $11 \times 11 = 121$, which is greater than 113."

"If the product of two numbers is 113," reasoned Peter, "at least one of them must be less than 11. If they both were 11 or more, then their product would be 121 or more."

"But we already showed that none of the primes less than 11 is a factor of 113," said Jenny. "So we don't have to check anything else. It must be that 113 is prime."

"To find that 113 is a prime number, we only had to check four primes. That was pretty quick." Peter was impressed. "But is there a pattern here?" he wondered.

"Well, 11 is the first prime number whose square is greater than 113." Jenny saw a pattern. "We didn't have to check anything greater than $\sqrt{113}$."

PRIME TESTING SHORTCUT

1. Check only prime numbers as possible divisors of your number.
2. Find the first prime number p whose square is greater than the number you are testing. You don't have to check anything greater than p .

(In other words, you only have to check primes up to the square root of your number.)

"If we want to find whether 343 is a prime number, what is the largest prime we have to test to see whether it divides 343?" Jenny wondered.

Peter started multiplying primes. He skipped the first few because he knew they were too small.

$$11 \times 11 = 121$$

$$13 \times 13 = 169$$

$$17 \times 17 = 289$$

$$19 \times 19 = 361$$

"OK," said Peter, "We see that 19 is the first prime number whose square is greater than 343. By our rule, we only have to test primes less than 19 to see whether they are divisors of 343." (This is Problem 1a.)

Jenny decided to try a larger number. "Is 1019 prime?" she wondered.

" $40 \times 40 = 1600$. That is more than 1019, so I don't have to check for prime divisors greater than 40.

" $30 \times 30 = 900$. That is less than 1019—I have to check primes greater than 30.

" $31 \times 31 = 961$. Still less than 1019. I have to go higher.

" $37 \times 37 = 1369$.

"To test whether 1019 is a prime number, I have to test only the primes less than 37," Jenny concluded. "Since 31 is the last prime before 37, I only have to check through 31."

PROBLEMS (Workbook page W115)

1. Find whether the following are prime numbers. Explain how you know.
 - a. 343
 - b. 1019
 - c. 1369
 - d. 2417
 - e. 2573
 - f. 1007

"I did it another way," said Jesse. "I used the square root key on my calculator. When we look for divisors of 1019, we only have to test prime numbers whose squares are less than $\sqrt{1019}$. These are the primes that are less than $\sqrt{1019}$. My calculator says $\sqrt{1019} \approx 31.92$. Since $\sqrt{1019}$ is between 31 and 32, we don't have to check any numbers higher than 31."

 **Do Problem 1 now.**

The Sieve of Eratosthenes

One method for finding prime numbers is called the **Sieve of Eratosthenes** (*air-uh-TAHS-thuh-neeZ*). It is named after a Greek mathematician who lived in North Africa around 230 BC.

"What is a sieve?" asked Evie.

"I know," said Abby. "It is a strainer, like the one my parents use to separate the spaghetti from the water."

The Sieve of Eratosthenes is a way of separating the prime numbers from the composite numbers. It involves crossing out all numbers that are divisible by 2, then all numbers divisible by 3, then numbers divisible by the next number not yet crossed out, and so on. The numbers that survive are the ones that are not divisible by other numbers (except 1), so the numbers that survive are prime.

THE SIEVE OF ERATOSTHENES

- A. Cross out 1 since it is not prime.
- B. Circle 2 since it is prime. Then cross out all remaining multiples of 2, since they can't be prime. (Why not?)
- C. Circle 3, the next prime. Cross out all remaining multiples of 3, since they can't be prime.
- D. Circle the next number that hasn't been crossed out. It is prime. (Why?) Cross out all remaining multiples of that number.
- E. Repeat Step D until all numbers are either circled or crossed out.

"I'll try the sieve method on the numbers from 1 to 50 to see how it works," said Lilah. "Then I'll try it again and watch more closely for a pattern."

 **Do Problems 2–5 now.**

PROBLEMS

(Workbook pages W116–W118)

2. Follow the steps in the Sieve of Eratosthenes to find all prime numbers from 1 to 50.
3. As you followed the steps in Problem 2, you probably found that multiples of the larger prime numbers had already been crossed out. What was the largest prime whose multiples were not already crossed out by smaller numbers?
4.
 - a. Use the Sieve of Eratosthenes to find all primes between 1 and 130. Each time you work with a new prime, make a note telling the first of its multiples not already crossed out by a smaller prime. (For example, when the prime is 3, the first multiple to consider is 6 but that has already been crossed out. Therefore, 9 is the first multiple of 3 not already crossed out by a smaller prime.)
 - b. Look at your notes from 4a. Describe a pattern that tells, for any prime number, its first multiple not already crossed out by smaller prime numbers.
 - c. When sieving for primes between 1 and 130, what was the largest prime that had multiples that were not already crossed out by smaller numbers?
 - d. After you had crossed out the multiples of enough primes, you could stop because only prime numbers were left. When did this happen?
5.
 - a. Suppose that you used the sieve method to find the primes between 1 and 200. List the primes whose multiples you would have to cross out before only primes were left. Explain why.
 - b. Suppose that you used the sieve method to find the primes between 1 and 1000. List the primes whose multiples you would have to cross out before only primes were left.

Counting Primes

Peter used the sieve to find all primes between 1 and 100. But he didn't stop there. He found all primes between 1 and 1000. He made the table at the right.

Peter noticed that the number of primes in an interval seemed to be going down as the numbers increased. He wondered whether this pattern continued. He decided to go to the library to see if he could find out more. He found a book there that gave a list of primes. He counted the primes in the list and added these lines to his table (*below right*).

"There seem to be fewer and fewer primes as the numbers get larger," he observed. "I wonder if you ever run out of primes. Wow. That would mean there is a largest prime number!"

"No," said Lilah. "It doesn't matter how large a prime number you find. There will always be one that is larger. This is how I know:

"Suppose you have a list of all the primes there are. Multiply them all together. You get a really big number, $N = 2 \times 3 \times 5 \times 7 \times \dots$. That number N is divisible by every prime on your list, right?"

"Of course it is, since it is a multiple of every prime on my list. I'm with you so far," said Peter.

"Good. Now add 1," Lilah continued. "You get $N + 1$, which cannot be divisible by 2."

"Let me think about that," said Peter. "I get multiples of two by counting by 2s, so the first number after N that is divisible by 2 is $N + 2$. So, I agree, $N + 1$ can't be divisible by 2."

Interval	Number of primes in interval
1 to 100	25
101 to 200	21
201 to 300	16
301 to 400	16
401 to 500	17
501 to 600	14
601 to 700	16
701 to 800	14
801 to 900	15
901 to 1000	14

Interval	Number of primes in interval
1 to 1000	168
1001 to 2000	135
9001 to 10,000	72

"OK," said Lilah, "and $N + 1$ also cannot be divisible by 3, since the first number after N that is divisible by 3 is $N + 3$."

"I see." Peter was following this reasoning. "And for a similar reason, $N + 1$ can't be divisible by any of the primes on my list."

"Right—and that means that either $N + 1$ is a prime number or it is divisible by a prime number not on your list. Either way, it must be that there is another prime."

"But how could that be, since you told me I had a list of *all* the prime numbers there are?" Peter was confused.

"It must be you didn't really have a list of *all* the primes. We can always find another prime—we'll never run out of primes."

Peter was disappointed—he had liked the idea that there might be a largest prime number. But Lilah was delighted to have convinced him otherwise.

What Lilah had explained was known to the Greeks more than 2000 years ago. It is called Euclid's Theorem. Here it is:

Euclid's Theorem: There are infinitely many prime numbers.

Formulas for Finding Primes

The Cryptokids wondered whether they could find a formula to generate all the prime numbers, but there is no such formula. They discovered, however, that there are formulas to describe some primes.

Twin primes are primes of the form p and $p + 2$. The numbers 3 and 5 are twin primes, as are 11 and 13. No one knows whether or not there are infinitely many pairs of twin primes.

Mersenne numbers are numbers of the form $2^n - 1$. A monk named Father Marin Mersenne worked with these numbers in the 1600s. The first Mersenne number is $2^1 - 1 = 1$. The second is $2^2 - 1 = 3$. If the exponent n is composite, then the corresponding Mersenne number is

composite. However, if the exponent n is prime, the corresponding Mersenne number can be either prime or composite.

For example, 4 is composite, and $2^4 - 1 = 64 - 1 = 63$, which is also composite ($63 = 3^2 \times 7$). The number 3 is prime, and $2^3 - 1 = 8 - 1 = 7$, which is prime.

Many of the largest known primes are Mersenne primes. In fact, one way people have found very large prime numbers is to test large Mersenne numbers to see whether they are prime.

A **Sophie Germaine prime** is a prime p such that $2p + 1$ is also prime. For example, 2, 3, and 5 are Sophie Germaine primes, but 7 is not, since $2 \times 7 + 1 = 15$, which is not prime. These primes were named after a French mathematician who lived about 200 years ago. No one knows whether or not there are infinitely many Sophie Germaine primes.

"How are these special numbers going to be useful to us?" Peter asked Tim.

"Well, we need large prime numbers for keys in the RSA cipher, or otherwise our ciphers will be too easy to break," Tim replied. "We can check numbers that might be Mersenne primes, Sophie Germaine primes, and twin primes—or other special primes. That's easier than checking all numbers."

"That's a good idea," said Evie. "Since most numbers are not prime, it would waste time to check every number."

 **Do Problems 6–10 now.**

PROBLEMS

(Workbook pages W119–W120)

6. a. One attempt at a formula to generate prime numbers is $n^2 - n + 41$. Evaluate the formula for $n = 0, 1, 2, 3, 4, 5$. Do you always get a prime?
b. **Challenge.** Find an n less than 50 for which the formula does not generate a prime.
7. Look back at your list of primes. Find all pairs of twin primes between 1 and 100.
8. Find the Mersenne numbers for $n = 5, 6, 7$, and 11. Which of these are prime?
9. Find at least three Sophie Germaine primes other than 2, 3, and 5.
10. **Challenge.** Find a large prime number. (You decide whether it is large enough to please you.) Explain how you chose the number and how you know it is prime.

Peter came to the next meeting of the Cryptoclub very excited.

"You know what I read? Regular people have found new prime numbers. In 1978, two high school kids found a new Mersenne prime. At the time, it was the largest known prime number. This news made the front page of the *New York Times*. Now people can join the Great Internet Mersenne Prime Search to hunt for Mersenne primes. In 2005, a volunteer found a Mersenne prime with 7,816,230 digits!"

"That is huge!" said Tim. "The largest number I knew about before was a googol. A **googol** is 10^{100} . You write it as 1 followed by 100 zeros. So a googol has only 101 digits. It's tiny compared to the largest known prime numbers."

"I am surprised people are still discovering new things about math," said Abby. "I thought all math was discovered a long time ago."

PROBLEMS (Workbook page W121)

- 11. a.** Test the Goldbach Conjecture: Pick several even numbers greater than 2 and write each as the sum of two primes. (Don't use 1 in your sums, since 1 is not prime.)
- b.** Find a number that can be written as the sum of two primes in more than one way.

Abby didn't realize that mathematics is a changing subject, not one that was completely figured out hundreds of years ago. Some mathematicians work on new problems such as how to find fast methods for computers to factor numbers. Others work on problems that were posed long ago but have not yet been solved. For example, a very famous statement about primes was made by Christian Goldbach (1690–1764). It is called the **Goldbach Conjecture**. It says that every even number greater than 2 is the sum of two primes. For example, $8 = 3 + 5$. Even though the Goldbach conjecture is simple to state, no one knows yet whether it is true or false.

 **Do Problem 11 now.**

DO YOU KNOW?

The Great Internet Mersenne Prime Search

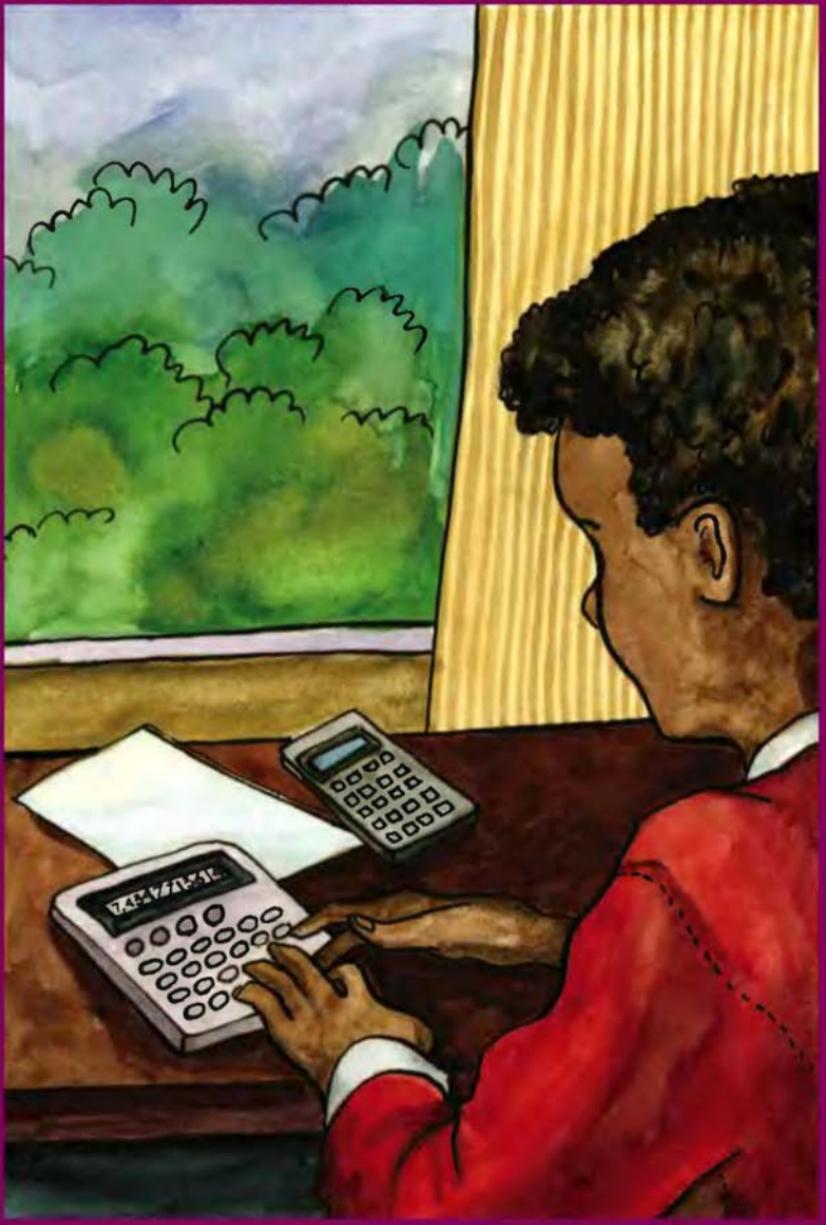
The Great Internet Mersenne Prime Search (GIMPS) is a project of volunteers who work together to find Mersenne primes using special software available for free on the Internet. The search is responsible for the discovery of eight Mersenne primes, each of which was the largest known prime when it was discovered. GIMPS was founded by George Woltman in 1997.

The exciting thing about the GIMPS project is that anyone can participate in the research. Sometimes entire school classrooms have participated. When you sign up, you receive a program that uses your computer to search for primes. Your computer runs the program while you are doing other things, like sleeping. It will let you and the GIMPS project know if it finds anything.

In February 2005, a new largest-known prime number was found by Dr. Martin Nowak, an eye surgeon in Michelfeld, Germany. It is $2^{25,964,951} - 1$ and has 7,816,230 digits. The previous largest prime was found by Josh Findley about a year before that.

To read more about the GIMPS project you can visit their website, <http://www.mersenne.org/>.

Chapter 17



Raising to Powers

The next topic the Cryptoclub members planned to explore was raising numbers to powers in modular arithmetic. Tim had warned them that this might be trickier than they expected. To get started, Tim asked them to compute

$$m = 18^{23} \bmod 55.$$

"This will be easy," Jesse said. "Both 18 and 23 are pretty small, so my calculator can handle that with no trouble."

But he was surprised when his calculator window showed him

7.4347713614 E28

That is his answer in scientific notation. It means $7.4347713614 \times 10^{28}$. To change his answer in scientific notation to standard notation, he moved the decimal point 28 places to the right—and added enough zeros to create all those places. So, according to his calculator,

$$18^{23} = 74,347,713,614,000,000,000,000,000.$$

"That is a huge number," Jesse said. The calculator didn't have enough places to show it all, so it had to round the answer and report only the first 11 significant digits.

Dan tried a different calculator. It reported that 18^{23} was

7.4348 28

Dan's calculator also reported the answer in scientific notation, although it didn't use the "E" in the notation that Jesse's calculator used, and it only reported five significant digits. The notation on Dan's calculator also meant that he had to move the decimal 28 places to the right and add enough zeros to do that. So according to Dan's calculator,

$$18^{23} = 74,348,000,000,000,000,000,000,000.$$

Both calculators rounded the number because it had too many digits to display in their windows. That works for many uses of numbers, but not for modular arithmetic.

"This doesn't help," said a frustrated Jesse. "To reduce a number mod 55, I need the exact number so I can figure out the remainder. The rounded answer gives me an idea of the size of the number, but that means nothing to me mod 55."

Peter had not heard the first part of this conversation. But when he heard that the others were stuck, he wanted to figure out a solution.

"What is the problem?" asked Peter.

"My numbers are way too big to work with," Jesse explained.

"But you're working in modular arithmetic—the numbers are small. In your example, you're working mod 55, so aren't the numbers less than 55?" Peter wondered.

"Yes, to start with, but when I raise them to a power, they get bigger before I can reduce them." Jesse was discouraged.

"Maybe you can raise the numbers to small powers first and then reduce the answers right away before they get too big," Peter suggested.

That was a great idea, so they worked out some examples.

$$18^1 = 18$$

$$18^2 = 18 \times 18 = 324 \equiv 49 \pmod{55}$$

$$18^3 = 18 \times 18^2 \quad \text{Now substitute } 49 \text{ for } 18^2.$$

$$\equiv 18 \times 49 \pmod{55}$$

$$\equiv 882 \pmod{55}$$

$$\equiv 2 \pmod{55}$$

$$18^4 = 18 \times 18^3 \quad \text{Next substitute } 2 \text{ for } 18^3, \text{ from the last line.}$$

$$\equiv 18 \times 2 \pmod{55}$$

$$\equiv 36 \pmod{55}$$

Do Problem 1 now.

"OK, so we have to multiply in small steps. But that means we can't use the exponent button on the calculator to calculate exponents. To compute 18^{23} , do we have to multiply 23 times? That's a lot of work." Dan was still discouraged.

"Well, it is actually only 22 multiplications, but it's still a lot of work," agreed Jenny. "And what if we have even larger exponents? That would be way too much work."

There is a quicker way to compute powers. It involves combining smaller powers to compute bigger powers. The simplest case is when the exponent is a power of 2, such as 2, 4, 8, 16, and so on. In that case, you compute bigger powers by repeatedly squaring smaller powers. For example, to compute 18^{16} you first compute 18^2 :

$$18^2 \equiv 49 \pmod{55}. \quad (\text{We computed this before.})$$

Next, you get 18^4 by squaring 18^2 and substituting $18^2 \equiv 49 \pmod{55}$.

$$\begin{aligned}18^4 &= (18^2)^2 \\&\equiv 49^2 \pmod{55} \\&\equiv 2401 \pmod{55} \\&\equiv 36 \pmod{55}\end{aligned}$$

PROBLEMS

(Workbook page W123)

1. Compute the following.

Reduce before your numbers get too large.

a. $482^4 \pmod{1000}$

b. $357^5 \pmod{1000}$

c. $993^5 \pmod{1000}$

d. $888^6 \pmod{1000}$

PROBLEMS

(Workbook pages W124–W126)

2. a. How many multiplications would it take to compute $18^{32} \text{ mod } 55$ using the method of repeated squaring?
- b. How many multiplications would it take to compute $18^{32} \text{ mod } 55$ by multiplying 18 by itself over and over?
- c. Compute $18^{32} \text{ mod } 55$ using the method from 2a or 2b that uses the fewest multiplications. (You can reuse calculations from this chapter.)
3. Use the method of repeated squaring to compute each number.
- $6^8 \text{ mod } 26$
 - $3^8 \text{ mod } 5$
 - $9^{16} \text{ mod } 11$
 - $4^{16} \text{ mod } 9$

You get 18^8 by squaring 18^4 . Substitute $18^4 \equiv 36 \pmod{55}$.

$$\begin{aligned}18^8 &= (18^4)^2 \\&\equiv 36^2 \pmod{55} \\&\equiv 1296 \pmod{55} \\&\equiv 31 \pmod{55}\end{aligned}$$

Square this to get 18^{16} .

$$\begin{aligned}18^{16} &= (18^8)^2 \\&\equiv 31^2 \pmod{55} \\&\equiv 961 \pmod{55} \\&\equiv 26 \pmod{55}\end{aligned}$$

We computed 18^{16} in only 4 multiplications. Notice that this method is a lot faster than multiplying 18 by itself over and over. It would have taken 15 multiplications to compute 18^{16} that way.

 **Do Problems 2–3 now.**

"I see that repeated squaring helps to compute powers when the exponent is a power of 2, like 2, 4, 8, 16, and so on, but what do I do when I have exponents that are not powers of 2?" Jesse asked.

"We can combine powers of 2 to get other exponents," said Tim. "Look at 18^{10} ."

$$18^{10} = \underbrace{18 \times 18 \times 18 \times 18 \times 18 \times 18 \times 18 \times 18}_{18^8} \times \underbrace{18 \times 18}_{18^2}$$

$$18^{10} = 18^8 \times 18^2$$

"By repeated squaring, we know $18^8 \equiv 31 \pmod{55}$ and $18^2 \equiv 49 \pmod{55}$. Substituting these values, we get

$$\begin{aligned}18^{10} &= 18^8 \times 18^2 \\&\equiv 31 \times 49 \pmod{55} \\&\equiv 1519 \pmod{55} \\&\equiv 34 \pmod{55}.\end{aligned}$$

"We still want to know 18^{23} ," said Tim. "It does not come up in the squaring method. But we can write 23 as $16 + 4 + 2 + 1$ —those numbers are all powers of 2. Then we can combine our earlier calculations to get what we are looking for."

$$\begin{aligned}18^{23} &= 18^{16} \times 18^4 \times 18^2 \times 18^1 \\&\equiv 26 \times 36 \times 49 \times 18 \pmod{55} \\&\equiv 936 \times 49 \times 18 \pmod{55}\end{aligned}$$

Now reduce the first part: $936 \pmod{55} = 1$.

$$\begin{aligned}18^{23} &\equiv 1 \times 49 \times 18 \pmod{55} \\&\equiv 882 \pmod{55} \\&\equiv 2 \pmod{55}\end{aligned}$$

"Wow. That huge number reduces to $2 \pmod{55}$." Jesse was impressed.

Tim summarized what they had learned. "A lot of calculations can be easier if we think about better ways to do them," he said.

 **Do Problems 4–6 now.**

PROBLEMS

(Workbook pages W127–W129)

4. Use some of the powers already computed in this chapter to find each value.
 - a. $18^6 \pmod{55}$
 - b. $18^{12} \pmod{55}$
 - c. $18^{20} \pmod{55}$
5. a. Make a list of the values $9^n \pmod{55}$ for $n = 1, 2, 4, 8$, and 16. Reduce each expression.
b. Combine your answers from 5a to compute $9^{11} \pmod{55}$.
c. Combine your answers from 5a to compute $9^{24} \pmod{55}$.
6. a. Make a list of the values $7^n \pmod{31}$, for $n = 1, 2, 4, 8$, and 16. Reduce each expression.
b. Combine your answers from 6a to compute $7^{18} \pmod{31}$.
c. Combine your answers from 6a to compute $7^{28} \pmod{31}$.

DO YOU KNOW?

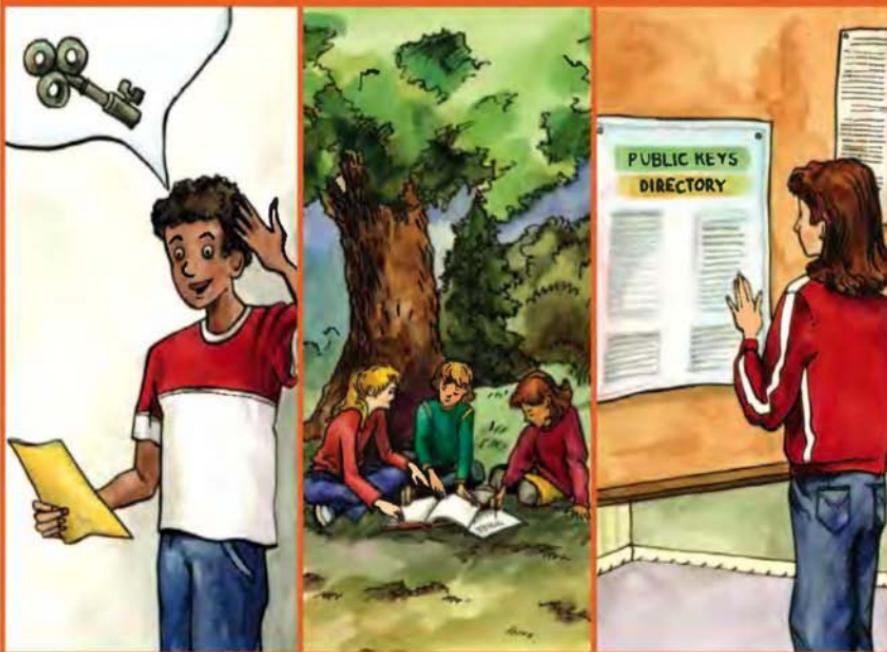
Dead Men Can't Tell Passwords

When the man in charge of archiving electronic copies of more than 11,000 of Norway's important historical documents died in 1993, so did access to the database that describes them, because he never told anyone else the password to the catalogue. Employees of the Ivar Aasen Center of Language and Culture that houses the documents tried to crack the password but were unable to do it. A team of computer technicians was hired to do it but could not.

In 2002, the director of the document center broadcast an appeal on national radio, asking computer hackers to crack the system and discover the password. About 25,000 people from all over the world responded and one of them suggested the password in less than an hour! It was the deceased man's last name, spelled backward.

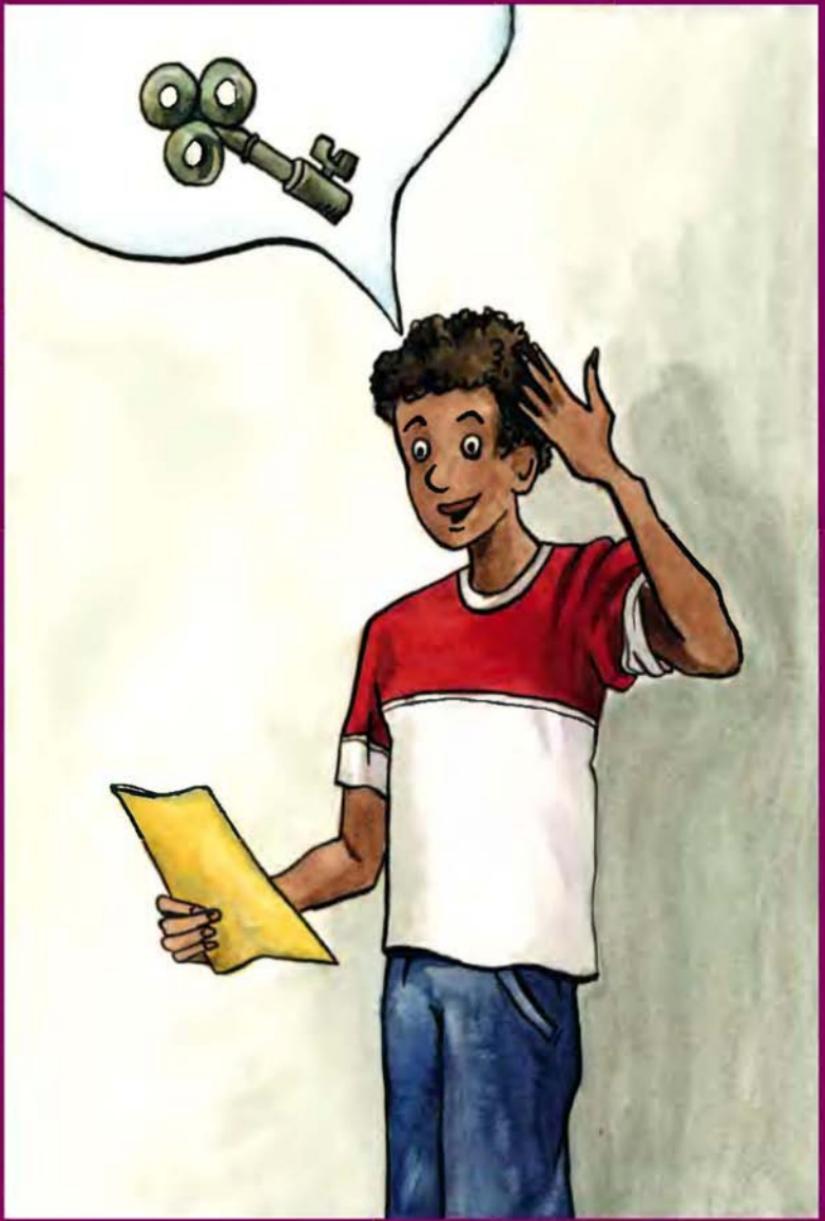
Employees of the center now keep their passwords on papers stored in the center's safe.

Unit 7



Public Key Cryptography

Chapter 18



The RSA Cryptosystem

Dan was going to visit his grandmother for a few weeks. He planned to send lots of e-mail messages to Jesse.

"You'd better encrypt your messages if they contain anything you don't want my sister to read," said Jesse.

"But how will you know what key I used? I can't send the key by e-mail because she might read that too," said Dan.

Jesse thought about this for a while. "Sending keys must be a problem for anyone who uses cryptography," he realized. "If spies are able to get messages, they could get the keys too. How can governments, businesses, and even regular people with important messages send their keys?"

This is a very important question. Until the 1970s, the problem of how to send keys secretly was a fundamental problem with all cipher systems. In 1975, however, Whitfield Diffie had an idea that changed the field of cryptography; it eliminated the need to keep keys secret.

In all the cipher systems known until that time and in all the ciphers we have learned about so far, the encryption key must be kept secret because if you know how to encrypt, you know how to decrypt. For example, if you learn that the sender added 3, then you know to subtract 3 to decrypt a message. Diffie realized that if there were a cipher system

in which the decryption key couldn't be figured out from the encryption key, then the encryption key wouldn't have to be secret.

A system in which it is very difficult to figure out the decryption key from the encryption key is called a **public key system**. In such a system, the encryption key could be known by anyone. The idea of public key cryptography was revolutionary when it was first announced, but at first no one had an example of a cipher system that worked that way. Then, in 1977, Ronald Rivest, Adi Shamir, and Leonard Adleman invented the **RSA cipher**, which was the first example of a workable public key system. It is still in use today.

In the RSA system, the *receiver* chooses both the encryption key and the matching decryption key. This is different from classical systems in which the *sender* usually chooses the encryption key and lets the receiver know what it is. After the receiver chooses his keys, he can list his encryption key in a directory—like a phone book—so anyone can use it to send him messages. But he is the only one who knows how to decrypt these messages.

Tim did some research into the RSA cipher system and came to the next meeting of the Cryptoclub prepared to teach it to his friends.

"To use RSA, we first need to choose an encryption key," said Tim, "We'll need two prime numbers p and q . I'll choose $p = 5$ and $q = 11$ for an example."

RSA works best with very large prime numbers, but Tim decided to start with small ones until everyone understood the system.

"We also need a special number, e ," Tim continued. "We have to choose e to be relatively prime to $(p - 1) \times (q - 1)$."

He calculated $(5 - 1) \times (11 - 1) = 4 \times 10 = 40$. Then he chose the number $e = 7$, since it is relatively prime to 40. He could have chosen a different number for e , as long as it was relatively prime to 40.

"The first part of the key is the product of p and q . This product is often called n , so in our example, $n = p \times q = 5 \times 11 = 55$.

"The encryption key is the pair (n, e) .

"Our encryption key is $(n, e) = (55, 7)$," announced Tim. "This is our public key. Anyone can use this to send us a message."

Tim went on to explain how to encrypt.

"To use RSA, you must first change your message to numbers. To encrypt a number message m with key (n, e) , compute

$$C = m^e \bmod n.$$

"So to send us a message using our encryption key $(55, 7)$, someone would compute

$$C = m^7 \bmod 55.$$

Tim showed his friends how to encrypt the letter **j**. "First you change the letter to a number," he said, "like we've been doing for a while." He converted **j** to 9.

"Next you compute $C = 9^7 \bmod 55$."

"We know how to do that!" exclaimed Dan.

$$\begin{aligned} C &= 9^7 \bmod 55 \\ &= 4,783,969 \bmod 55 \\ &= 4. \end{aligned}$$

"So," said Dan, "**j** becomes 4, right?"

"Right," said Tim. "Let's summarize."

CHOOSING AN RSA ENCRYPTION KEY

- Choose two prime numbers p and q . Compute the product $n = p \times q$.
- Choose a number e that is relatively prime to $(p - 1) \times (q - 1)$.

The **encryption key** is the pair (n, e) . It is also called the **public key**.

NOTE

There are different ways to change a letter-message to a number-message. Since Tim's friends were familiar with letting $a = 0$, $b = 1$, $c = 2$, and so on, he suggested they use that method. Serious RSA users who want to be sure no one can break their messages use more complicated methods—they change a block of letters to a many-digit number—but for our purposes, we will use Tim's method since that is what we are familiar with.

ENCRYPTING USING RSA

- First change your message to a number message.
- To encrypt a number message m with key (n, e) , compute

$$C = m^e \bmod n.$$

Do Problem 1 now.

"Now that we know how to encrypt using the RSA system," said Dan, "are you going to tell us how to decrypt?"

"Sure," said Tim. "It is very similar to encrypting. To decrypt 4, we have to calculate $4^d \bmod 55$, where d is my decryption key."

"Well," said Abby, "if you don't tell us the value of d , we can't decrypt."

"Exactly!" said Tim. "That's the beauty of RSA. I tell you my encryption key so you can send me a coded message, but I keep the decryption key a secret. That way no one can decrypt but me. But since I'm showing you how to use RSA, I'll show you how to find d .

"Remember that my encryption key is $(n, e) = (55, 7)$. Well," explained Tim, "to calculate d , you need to know the factors of $n = 55$, which we do—they are $p = 5$ and $q = 11$ —and we need the value of $e = 7$. Then, d is the inverse of $e \bmod (p - 1)(q - 1)$. Remember, the inverse d satisfies

$$ed \equiv 1 \pmod{(p - 1)(q - 1)}.$$

"That looks pretty complicated," said Abby.

"It's not too bad when you substitute numbers," assured Tim. "We substitute the values of e , p , and q . So we want d such that

$$\begin{aligned}7d &\equiv 1 \pmod{(5-1)(11-1)} \\&\equiv 1 \pmod{4 \times 10} \\&\equiv 1 \pmod{40}.\end{aligned}$$

"So we're looking for a number whose product with 7 reduces to 1 mod 40, right?" asked Abby.

"Right," said Tim.

They got to work looking for a number that fit this description. They decided to try all products until they found the one that worked (*right*).

They finally found it: $d = 23$ is the number they were looking for. (Tim wondered whether there was a shorter way to find his d than to multiply all those numbers, but he decided to worry about shortcuts later.)

Tim's public key is $(55, 7)$ and his private key is $d = 23$. To decrypt the message 4 that he had encrypted with his public key, Tim must compute $m = 4^{23} \pmod{55}$.

This is a bit messy and gives numbers too large for a calculator. He used repeated squaring to make the job easier, and he reduced as he went along to avoid calculator problems. He got the answer

$$4^{23} \pmod{55} = 9.$$

"See," said Tim. "Decrypting 4 gives the number 9, and 9 corresponds to **j**. That is the plaintext we started with."

$$7 \times 1 = 7$$

$$7 \times 2 = 14$$

$$7 \times 3 = 21$$

$$7 \times 4 = 28$$

$$7 \times 5 = 35$$

$$7 \times 6 = 42 \equiv 2 \pmod{40}$$

$$7 \times 7 = 49 \equiv 9 \pmod{40}$$

$$7 \times 8 = 56 \equiv 16 \pmod{40}$$

⋮

$$7 \times 22 = 154 \equiv 34 \pmod{40}$$

$$7 \times 23 = 161 \equiv 1 \pmod{40}$$

PROBLEMS

(Workbook pages W131-W132)

2. **Review:** Show that

$$4^{23} \bmod 55 = 9.$$

3. Dan encrypted a word with Tim's encryption key $(n, e) = (55, 7)$. He got the numbers 4, 0, 8. Use Tim's decryption key $d = 23$ to decrypt these numbers and get back Dan's word. (Hint: You can use your result from Problem 2.)

Let's summarize.

FINDING THE RSA DECRYPTION KEY

- If the encryption key is (n, e) , where $n = pq$, then the **decryption key** (also called the **private key**) is a number d such that

$$ed \equiv 1 \pmod{(p-1)(q-1)}.$$

In other words, d is the inverse of $e \bmod (p-1)(q-1)$.

DECRYPTING WITH RSA

- To decrypt C with RSA keys (n, e) and d , compute

$$m = C^d \bmod n$$

 Do Problems 2 and 3 now.

"The decryption formula looks a lot like the encryption formula," said Abby, a bit puzzled.

"It is similar," said Tim. "They both involve raising numbers to a power and reducing mod n . Decrypting isn't any harder than encrypting, if you know the decryption key."

"Then why can't everyone decrypt?" asked Evie.

"Because they don't know my d ," reminded Tim. "They don't even know my p and q since I only told them the product $n = p \times q$. When I said the public key was (n, e) , I never mentioned p and q . It is important to keep p and q secret. Otherwise, d can be figured out."

"But can't anyone figure out p and q by factoring n ?" asked Dan.

"Sometimes," agreed Tim. "Our example, $n = 55$, is easy to factor. But if p and q are large enough, it is *very hard* to factor their product, so the numbers p and q remain secret."

Tim was right. Factoring is not always easy. The numbers we have been working with have been tiny compared to the ones used in real-life applications of RSA. To keep messages secure, some people use prime numbers with more than 200 digits. These primes and their products are huge numbers.

It would take such a long time to factor these numbers—thousands of years—that the messages are safe now. But as computers get faster and as new methods of factoring are discovered, it might someday be possible to factor even these huge numbers in a reasonable amount of time. When that happens, RSA will no longer be a secure cipher. But by then, people might have thought of other public key systems.

DO YOU KNOW? Modern Uses of Cryptography

Up until about 30 years ago, the most important uses of cryptography were military and diplomatic. There are many examples of battles won during wartime because one side was able to decrypt the messages sent secretly by the other side, and there have been many situations in which leaders of some countries needed to communicate with each other without leaders of other countries knowing what they were saying. Today, however, cryptography has become important in many situations in the lives of ordinary people. For example, cryptography is used in automated-teller machines at banks, in cellular telephones, and on the Internet to ensure that important information, such as credit card numbers, travels securely. While users are not always aware of the encryption their computers are doing for them, cryptography is important to everyone.

Cryptography is used not only to keep messages secret, but also to make sure that the receiver knows who sent the message. If a person withdraws money from a bank, there has to be a way that the bank can prove that the person sending the message really is the owner of the account. In this situation, the ability of the bank to verify the identity of the person who sent the request is more important than secrecy.

Another application of cryptography is in e-mail. Some people want to send private e-mail messages. These messages are encrypted by their computers before being sent – without the sender having to do extra work each time.

Chapter 19



Revisiting Inverses in Modular Arithmetic

"We know just about everything we need to be able to use RSA, right?" said Evie.

"Not exactly," said Jenny. "To find the decryption key d , we have to find a modular inverse. That isn't so easy to do. Let's learn more about how to do that."

"Didn't we already find inverses in mod 26 when we worked with multiplicative ciphers?" Abby thought that all this sounded familiar.

"That's true," said Jenny, "but for RSA we have to find inverses in different mods, not just mod 26."

"I know a website on the Internet that helps us find inverses in modular arithmetic," said Tim. "We can always use that, but maybe we can learn to find them ourselves."

Finding Inverses in Modular Arithmetic

The Cryptokids reviewed what they knew about inverses.

The **inverse** of a number e is a number d such that $ed = 1$.

In regular arithmetic, you can find an inverse easily. For example, the inverse of 5 is $\frac{1}{5}$, since $5 \times \frac{1}{5} = 1$. But in modular arithmetic, fractions don't exist, so inverses are different.

"Let's practice by finding the inverse of 5 mod 7," suggested Jenny.

"If we work mod 7, we are only working with the numbers 0, 1, 2, 3, 4, 5, and 6. If one of these numbers satisfies $5 \times d \equiv 1 \pmod{7}$, then that number is the mod 7 inverse of 5.

"The inverse of 5 can't be 0, since $5 \times 0 = 0$. (In fact, 0 can't ever be an inverse, since 0 times any number is always 0.) Also, the inverse can't be 1 since $5 \times 1 = 5$. So let's look at other products involving 5.

$$5 \times 2 = 10 \equiv 3 \pmod{7}$$

$$5 \times 3 = 15 \equiv 1 \pmod{7}$$

"That's it! 5 times 3 is equivalent to 1 mod 7, so 3 is the inverse of 5 mod 7."

It turns out that not all numbers have inverses in modular arithmetic. In fact,

The only numbers that have inverses mod n are the numbers relatively prime to n .

"Let's try finding the inverse of 5 mod 18," said Jesse.

"The only numbers that have inverses mod 18 are the numbers that are relatively prime to 18, which are 1, 5, 7, 11, 13, and 17. We just have to check those to find the mod 18 inverse of 5. The inverse can't be 1 since $5 \times 1 = 5$. Let's check the other numbers on the list:

$$5 \times 5 = 25 \equiv 7 \pmod{18}$$

$$5 \times 7 = 35 \equiv 17 \pmod{18}$$

$$5 \times 11 = 55 \equiv 1 \pmod{18}$$

"So 11 is the inverse of 5 mod 18. We only had to test a few numbers to find that out."

"This is fun!" said Jenny. "Let's find the inverse of 7 mod 180."

Remember that the inverse of 7 mod 180 is the number d such that

$$7 \times d \equiv 1 \pmod{180}.$$

Jenny started to look for d , listing the products of 7 and all numbers relatively prime to 180.

Since $180 = 2^2 \times 3^2 \times 5$, numbers less than 180 that are relatively prime to 180 are numbers not divisible by 2, 3, or 5. These are 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 77, and so on.

Jenny planned to try all the numbers from the list until she got the right one.

$$7 \times 7 = 49$$

$$7 \times 11 = 77$$

$$7 \times 13 = 91$$

$$7 \times 17 = 119$$

$$7 \times 19 = 133$$

$$7 \times 23 = 161$$

$$7 \times 29 = 203 \equiv 23 \pmod{180}$$

$$7 \times 31 = 217 \equiv 37 \pmod{180}$$

⋮

Evie thought Jenny's method was taking too much time, so she tried to find a faster way.

Instead of multiplying 7 and all possible numbers to see if any products were congruent to 1 (mod 180), she started with a list of numbers congruent to 1 (mod 180). Then she checked whether anything on that list was a multiple of 7.

PROBLEMS

(Workbook pages W133–W135)

1. For each of the following, determine whether the inverse exists in the given modulus. If it exists, use either Jenny's method or Evie's method to find it.

- a. $10 \pmod{13}$
- b. $10 \pmod{15}$
- c. $7 \pmod{21}$
- d. $7 \pmod{18}$
- e. $11 \pmod{24}$
- f. $11 \pmod{22}$

2. Find the inverse of each of the following numbers in the given modulus.

- a. $11 \pmod{180}$
- b. $9 \pmod{100}$
- c. $7 \pmod{150}$

Numbers congruent to 1 (mod 180):

$180 + 1 = 181$ Not divisible by 7, since $181 \div 7$ is not a whole number, so 181 couldn't be $7 \times d$.

$2 \times 180 + 1 = 361$ Not divisible by 7, for the same reason, so 361 couldn't be $7 \times d$.

$3 \times 180 + 1 = 541$ Not divisible by 7, so not $7 \times d$.

$4 \times 180 + 1 = 721$ When we divide this by 7, we get 103, so $7 \times 103 = 721 \equiv 1 \pmod{180}$. That means the inverse of 7 mod 180 is 103.

Jenny's method and Evie's method show two ways to find the inverse of a number in modular arithmetic. There is a more direct way to find inverses, called the Extended Euclidean Algorithm, but trial and error works well enough for small numbers.

 **Do Problems 1 and 2 now.**

DO YOU KNOW?

Jefferson and Madison: But Where Is the Key?

Did you ever forget something important? Maybe you forgot to bring your homework to school. Or maybe you left something at school that you needed at home. You are not the only one. James Madison once forgot to bring his cipher key and that meant that he could not decrypt a secret message from Thomas Jefferson.

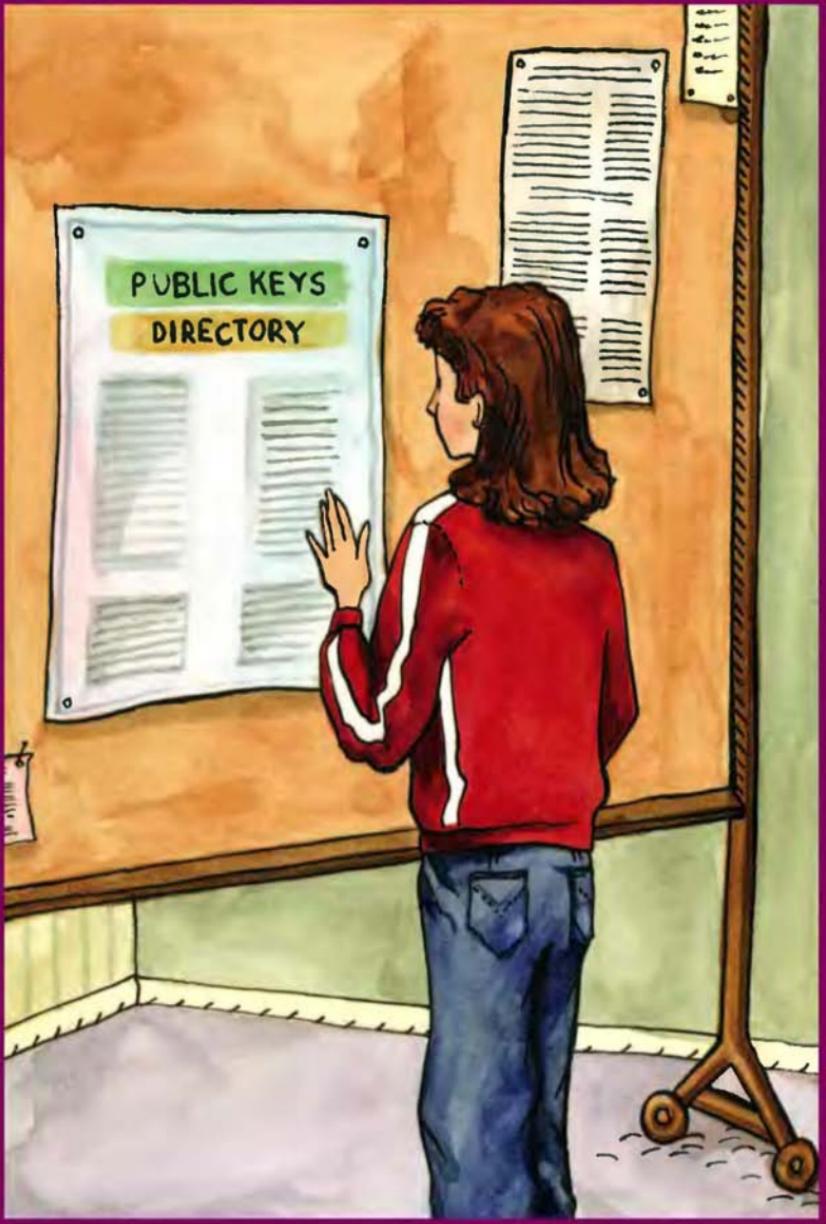
After the Revolutionary War, the Founding Fathers of the new nation needed a way to send secret messages to each other. In 1781, the Secretary of Foreign Affairs, Robert A. Livingston, printed up forms with the numbers 1 to 1700 on one side and a list of words and syllables that might be used in messages on the other side. Government officials could easily create codes that assigned numbers to words on the list. The key to the code was the list that told what number each word corresponded to.

James Madison and Thomas Jefferson agreed on a code in 1785 and used it to encipher messages to each other until at least 1793. In 1793, Madison, who was away on vacation, received a partially encoded message from Jefferson.

"We have decided unanimously to 130... interest if they do not 510... to the 636. Its consequences you will readily seize, but 145... though the 15..."

All Madison needed to do to understand this message was replace the numbers with the matching words according to his key. It was then that Madison discovered he had left his key in Philadelphia.

Chapter 20



Sending RSA Messages

"Enough practice," said Jenny. "Let's choose our RSA keys and start sending messages."

"Let's make a directory of everyone's public keys," Lilah said. "Then we can send messages to anyone. We'll post the directory on the message board."

CLASS ACTIVITY (Workbook page W137)

- A. With your group, choose an RSA key. You need two parts, the encryption key and the matching decryption key. Here is a summary of what you need. (If you want to check the details, go back to Chapter 18.)
 - Prime numbers p and q .
 - A number e relatively prime to the product $(p - 1)(q - 1)$.
 - A number d such that $ed \equiv 1 \pmod{(p - 1)(q - 1)}$. (In other words, d is the inverse of e mod $(p - 1)(q - 1)$.)
- B. Write your encryption key on the board, along with your group's name. Be sure to keep your decryption key secret.
- C. To test your encryption and decryption keys, ask another group to encrypt a short message to you using your encryption key. Use your decryption key to decrypt it.

★ TIP: Choosing your Key

- Depending on your p and q , you probably have several choices for e —it can be any number that doesn't have any factors in common with $(p - 1)(q - 1)$. But whatever you choose, you have to be able to find the matching decryption key d . If that is difficult, then pick another e .
- Keep your primes small (less than 20) for now. You can change them later when you want to make your messages more secure.

In practice, the RSA system takes a lot of time to implement—so much time that it is impractical to use for transmitting large amounts of data. So instead of encrypting entire messages with RSA, businesses sometimes use RSA to encrypt a keyword that is then used with a different, quicker cipher.

Dan prepared a message to send to Tim. He encrypted it with a Vigenère cipher using the keyword **CRYPTO**. He even took out the spaces in his message so as not to give extra clues. But Tim wasn't expecting the message, so he didn't know in advance what Vigenère keyword Dan had used.

Dan had to get the keyword to Tim, so he looked up Tim's public key in the club directory. He encrypted his keyword using RSA and Tim's public key.

First, he assigned letters to numbers using $a = 0$, $b = 1$, $c = 2$, and so on, since that is the system they were used to. This changed his keyword **CRYPTO** to the numbers, 2, 17, 24, 15, 19, 14.

Then, he used Tim's public key, (55, 7), and substituted each of those numbers for m in the expression $m^7 \bmod 55$.

Here are Dan's calculations:

$$\begin{aligned}2^7 \bmod 55 &= 128 \bmod 55 \\&= 18\end{aligned}$$

$$\begin{aligned}17^7 \bmod 55 &= 410,338,673 \bmod 55 \\&= 8\end{aligned}$$

$$\begin{aligned}24^7 \bmod 55 &= 4,586,471,424 \bmod 55 \\&= 29\end{aligned}$$

$$\begin{aligned}15^7 \bmod 55 &= 170,859,375 \bmod 55 \\&= 5\end{aligned}$$

$$\begin{aligned}19^7 \bmod 55 &= 893,871,739 \bmod 55 \\&= 24\end{aligned}$$

$$\begin{aligned}14^7 \bmod 55 &= 105,413,504 \bmod 55 \\&= 9\end{aligned}$$

So Dan's encryption of **CRYPTO** was: 18, 8, 29, 5, 24, 9.

He sent this note to Tim:

Tim,

Here is a Vigenère message. I encrypted the keyword with your RSA public key. This is what I got: 18, 8, 29, 5, 24, 9. Use your RSA decryption key to find the keyword. Then use the keyword to figure out the Vigenère message.

KWWDNQCEPTTRVYGHMVGEWDNOTVTT
KMFVRTKAKECS. PSJRTTESCILTWONF
RHBBEVRWXTKIQIWOANCHMOTKCES
CILXGUCSMJMQTPNIHUTRNWR.

- DAN

When Tim received Dan's message, he used his decryption key $d = 23$ to decrypt the keyword. He substituted each of Dan's numbers for C in the expression $C^{23} \bmod 55$.

Dan's first number was $C = 18$, so Tim needed to compute $18^{23} \bmod 55$. This was not as easy as the calculations Dan had done because 18^{23} is too big for his calculator and had to be rounded. Luckily, however, Tim had already computed that $18^{23} \bmod 55 = 2$ (see Chapter 17). Using repeated squaring and reducing as he went along, he computed the rest of the numbers:

$$8^{23} \bmod 55 = 17$$

$$29^{23} \bmod 55 = 24$$

$$5^{23} \bmod 55 = 15$$

$$24^{23} \bmod 55 = 19$$

$$9^{23} \bmod 55 = 14.$$

PROBLEMS

(Workbook pages W137–W140)

1. Use Dan's keyword **CRYPTO** to decrypt his Vigenère message to Tim.
2. a. Dan's RSA decryption key is $d = 5$. Use it to find the keyword that Tim encrypted.
b. Use the keyword you found in 2a to decrypt the Vigenère message Tim sent to Dan.
3. Combine RSA with the Vigenère cipher.
 - a. Encrypt a message using the Vigenère cipher with a Vigenère keyword you choose.
 - b. Encrypt your Vigenère keyword using RSA and the RSA encryption key of the person to whom you are sending the message.
 - c. Ask the person to decrypt your keyword using their RSA decryption key and to use it to decrypt your message.

★ TIP

If your messages are long or if you want to use a modular calculator, you can use the tools on the Cryptoclub website.

Tim learned that the numbers for Dan's keyword were 2, 17, 24, 15, 19, 14. He changed these back to letters and got **CRYPTO**. Then he got out his Vigenère Square and decrypted Dan's message.

Tim wrote a reply to Dan and encrypted it with a Vigenère cipher.

"I'll use RSA to encrypt my Vigenère keyword like Dan did," he said. He looked up Dan's public key in the club directory and found that it was $(n, e) = (221, 77)$. He used that to encrypt his keyword, and sent a note to Dan.

Dan,

Here is my reply. It is a Vigenère message. I used your RSA public key to encrypt my Vigenère keyword. This is what I got: 32, 209, 165, 140. You know what to do with it.

ACXETSUMIVW.

MCAQGIVSUQKBHHCBGTTCXHVCR.

—Tim

Do Problems 1–3 now.

DO YOU KNOW?

The British Public-Key Ciphers

It was a great achievement in 1976 when Whitfield Diffie, an independent cryptography enthusiast, teamed up with Stanford professor Martin Hellman and developed the ideas of public-key cryptography. In fact, it is considered the most important cryptographic discovery in the twentieth century. A year later, MIT professors Ronald Rivest, Adi Shamir, and Leonard Adleman developed RSA, the first workable system to implement the Diffie-Hellman ideas. They all published their work and were considered superstars. But there is more to the story.

When government agencies develop new secret codes, their work is usually kept secret. Nothing is published and the developers receive little public recognition. This was the case with public-key cryptography. According to the British government, public-key cryptography was invented by British cryptographers James Ellis, Malcolm Williamson, and Clifford Cocks at the British Government Communication Headquarters (GCHQ) in the early 1970s – several years before the Americans' work – but no one knew about it because all their work was secret. By 1975, Ellis, Williamson, and Cocks had discovered all the essentials of public-key cryptography, including the RSA cipher, but had to remain silent and watch as Diffie, Hellman, Rivest, Shamir, and Adelman rediscovered what they already knew. It was not until 1997 – one month after James Ellis died – that the British government finally broke its silence and revealed their work.

CONTINUED ON NEXT PAGE >

DO YOU KNOW? (CONTINUED)

The British Public-Key Ciphers

It is fortunate that the Americans discovered public-key cryptography, even if they were not the first. Since they didn't work for any government, they were free to publicize their discovery, and this made private communication on the Internet possible for businesses and ordinary people. But it is unfortunate that the British cryptographers had to wait so long to receive the public recognition they deserved for making such an important discovery.

Index

24-hour clock, 105

A

Adleman, Leonard, 176, 193
affine ciphers, 145–151
 cracking, 148–150
 decrypting, 147
 definition, 145
 key, 145
algorithm, 21
Atbash, 152

B

Beale Ciphers, 18–19

C

Caesar ciphers
 cracking, 21–25
 definition, 4
 with numbers, 10
Captain Kidd, 39
Captain Midnight, 7
cicadas, 83
ciphers. *See names of individual ciphers*
 definition, 4
ciphertext, 4

cipher strip, 9
Cipher Tag, 5, 15, 60, 138
cipher wheel, 6
 tips for using, 6
Civil War, American, 61
clock arithmetic. *See modular arithmetic*
Cocks, Clifford, 193
Code-O-Graph, 7
Colossus, 143
common factor. *See factor*
composite number, 76
congruent, 11
congruent mod n , 108. *See also modular arithmetic*
cryptography, 3

D

Dancing Men, 33
decrypting, 4
Diffie, Whitfield, 175, 193
divisibility, rules for, 78–79
Doyle, Sir Arthur Conan, 33

E

Ellis, James, 193

encrypting, 4
Enigma cipher, 142–143
equivalent, 11
equivalent mod n , 108. *See also modular arithmetic*
exponents, 80, 167–171

F

factor, 75
 common, 82
 greatest common, 82
factoring, 75–83
factor tree, 76
Findley, Josh, 165
frequencies, 35–39
 definition, 36
 of letters in English
 alphabetical, 41
 by frequency, 39
 relative frequency, 36
frequency analysis, tips, 48

G

Germaine, Sophie, 163
GIMPS. *See Great Internet Mersenne Prime Search*

- Goldbach Conjecture, 164
“The Gold Bug”, 39
greatest common factor.
 See factor
Great Internet Mersenne Prime Search, 164, 165
- H**
Hellman, Martin, 193
Holmes, Sherlock, 33
- I**
International Standard Book Number. *See* ISBN
inverses, 133–142
 modular, 135, 137–138, 183–187
 multiplicative, 135, 183
ISBN, 121–122
- J**
Jefferson, Thomas, 73, 187
- K**
key, 21
 good and bad.
 See multiplicative ciphers
public and private. *See* RSA cipher
keyword ciphers, 29–32
 definition, 30
 keyword, 30
 key letter, 30
- L**
leap years, 120
letter frequencies.
 See frequencies
Lewis and Clark, 73, 88–89
- linear equivalences, solving, 148–150
Little Orphan Annie, 7
Livingston, Robert A., 187
- M**
Madison, James, 187
Mary Queen of Scots, 50
Mersenne numbers, 162
 primes, 163
military time. *See* 24-hour clock
modular arithmetic, 103–111
 applications of, 115–122
 calendar applications of, 119
 definition, 107
 reduce mod n , 109
modulus, 107
The Mod Game, 111
multiple, 75
multiplicative ciphers, 125–131
 bad key, 127
 cracking, 138–142
 decrypting, 133–142
 good key, 127, 129
- N**
Navajo Code Talkers, 26
negative numbers, 12–15
Nowak, Martin, 165
- O**
one-time pad, 98–99
- P**
passwords, 131, 172
Pass the Hat, 9
plaintext, 4
Poe, Edgar Allan, 39
powers. *See* exponents
prime factorization, 76
- prime numbers, 76, 155–165
 counting, 161
 definition, 76
Mersenne primes, 163
Sophie Germaine primes, 163
testing shortcut, 157
twin primes, 162
public-key cryptography, 176.
 See also RSA cipher
British role, 193
- R**
reciprocal, 135
Rejewski, Marian, 143
relatively prime, 128
relative frequency.
 See frequencies
remainders, using a calculator to find, 117–118
Rivest, Ronald, 176, 193
RSA cipher, 155, 175–181, 189–193
 decrypting, 180–181
 decryption key, 180
 definition, 176
 encrypting, 178–179
 encryption key, 177
 sending messages, 189–193
- S**
secret code, 3
Shamir, Adi, 176, 193
shift cipher. *See* Caesar ciphers
Sieve of Eratosthenes, 159
substitution ciphers, 29–50
 cracking, 41–50
 definition, 29
- T**
Turing, Alan, 143
24-hour clock, 105

V

VENONA, 99
Vigenère cipher, 53–99
 cracking with known
 keylength, 63–73
 cracking with unknown
 keylength, 85–96

decrypting, 57–60
definition, 55
keyword, 55
with numbers, 60

Vigenère square, 58–59

W

Waltmann, George, 165

Williamson, Malcolm, 193

World War I, 112
World War II, 26, 142–143

Z

Zimmermann telegram, 112–113

Make Your Own Cipher Wheel

Cut out the circles and fasten with a brad (paper fastener). Make sure the brad goes through the exact centers, or the wheel might not work very well.

TIP: To make a sturdy wheel, paste the circles onto posterboard or cardstock before cutting.

