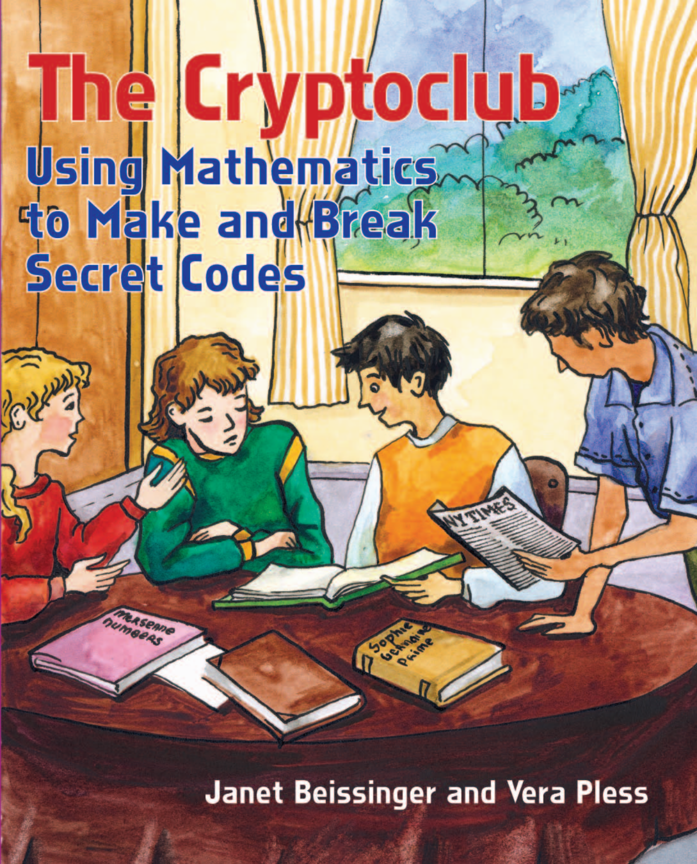
The Cryptoclub

Using Mathematics to Make and Break Secret Codes



Janet Beissinger and Vera Pless

Beissinger
Pless

The Cryptoclub

Using Mathematics to Make and Break Secret Codes

A K
PETERS

The Cryptoclub

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

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

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.

Unit I

Introduction to Cryptography

Chapter 1

I saw this cute boy today.
Everybody likes him.
I hope he likes me.

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)

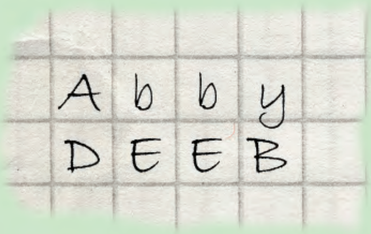
3. Decrypt the following note Evie wrote to Abby. She used a Caesar cipher with a shift of 4 like the one above.

WSVVC. PIX’W YWI GMTLIVW JVSQ RSA SR.

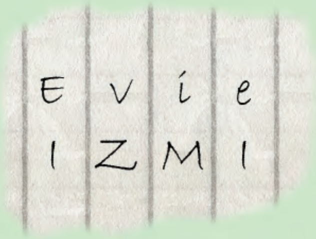
4. Use a shift of 3 or 4 to encrypt someone’s name. It could be someone in your class or school or someone your class has learned about. (You’ll use this to play Cipher Tag.)

★ 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:

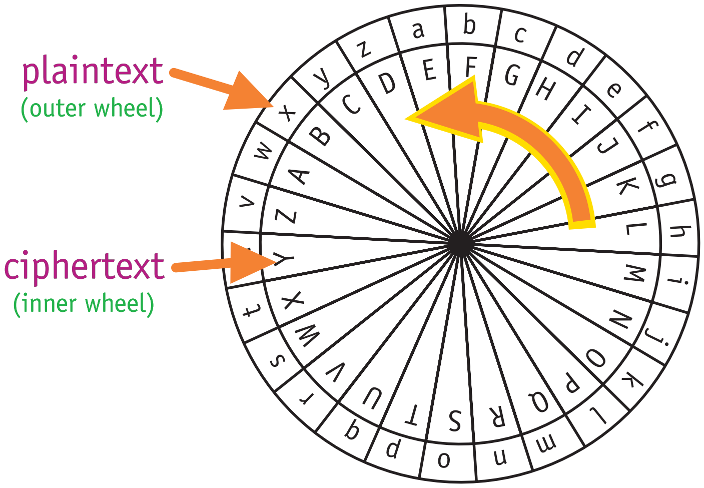
6. **Riddle:** What do you call a dog at the beach?

   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.


plaintext
(outer wheel)
ciphertext
(inner 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
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

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

e f g h i j k l m n o p q r s t u v w x y z
4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
J e n n y
9 4 13 13 24

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

a. Use the number method to encrypt your teacher's name. Compare your answer with the rest of the class.

b. Use the number method to encrypt your name. Put your encrypted name in a "hat" that your teacher provides.

c. 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.

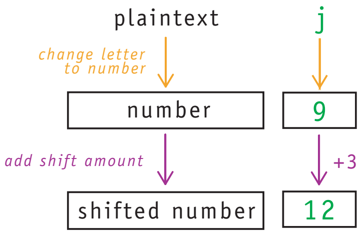
   c. Describe how you can use arithmetic to get your answer to **2b** from your answer to **2a**.

Do Problem 1 now.

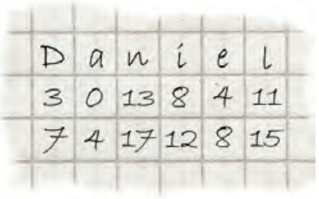
Jenny used her number method to encrypt messages for a while, but then she realized it would be very easy for someone else to figure out her method. When she heard about Caesar ciphers, she decided to combine them with her number method. She shifted the numbers on her strip three places and got the cipher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

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.

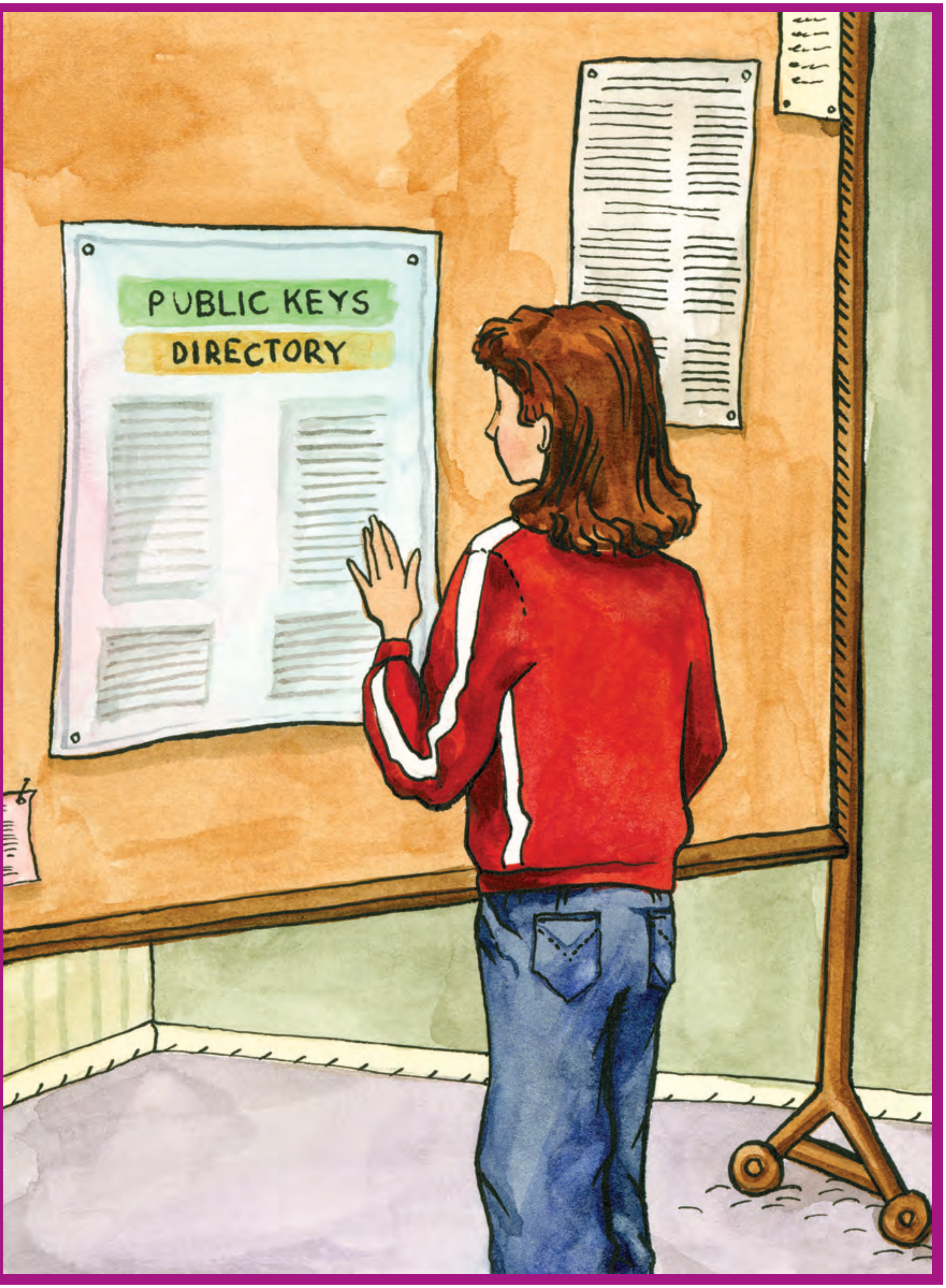
After the Revolutionary War, the Founding Fathers of the new nation needed a way to send secret messages to each other. In 1781, the Secretary of Foreign Affairs, Robert A. Livingston, printed up forms with the numbers 1 to 1700 on one side and a list of words and syllables that might be used in messages 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 $ed \equiv 1 \bmod (p - 1)(q - 1)$. (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 mod 55.

Here are Dan's calculations:

$$\begin{aligned} 2^7 \bmod 55 &= 128 \bmod 55 \\ &= 18 \end{aligned}$$

$$\begin{aligned} 17^7 \bmod 55 &= 410{,}338{,}673 \bmod 55 \\ &= 8 \end{aligned}$$

$$\begin{aligned} 24^7 \bmod 55 &= 4{,}586{,}471{,}424 \bmod 55 \\ &= 29 \end{aligned}$$

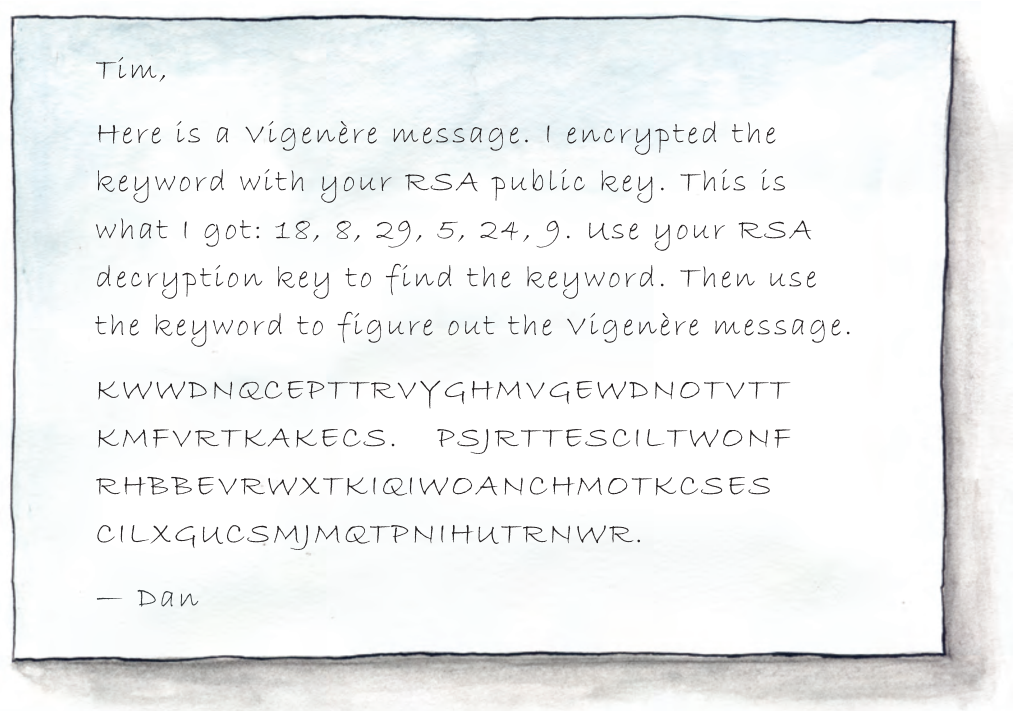
$$\begin{aligned} 15^7 \bmod 55 &= 170{,}859{,}375 \bmod 55 \\ &= 5 \end{aligned}$$

$$\begin{aligned} 19^7 \bmod 55 &= 893{,}871{,}739 \bmod 55 \\ &= 24 \end{aligned}$$

$$\begin{aligned} 14^7 \bmod 55 &= 105{,}413{,}504 \bmod 55 \\ &= 9 \end{aligned}$$

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
RHBBEVRWXTKIQIWOANCHMOTKCSES
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} mod 55.

Dan’s first number was $C = 18$, so Tim needed to compute 18^{23} mod 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} mod 55 = 2 (see Chapter 17). Using repeated squaring and reducing as he went along, he computed the rest of the numbers:

$$\begin{aligned} 8^{23} \bmod 55 &= 17 \\ 29^{23} \bmod 55 &= 24 \\ 5^{23} \bmod 55 &= 15 \\ 24^{23} \bmod 55 &= 19 \\ 9^{23} \bmod 55 &= 14. \end{aligned}$$

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.

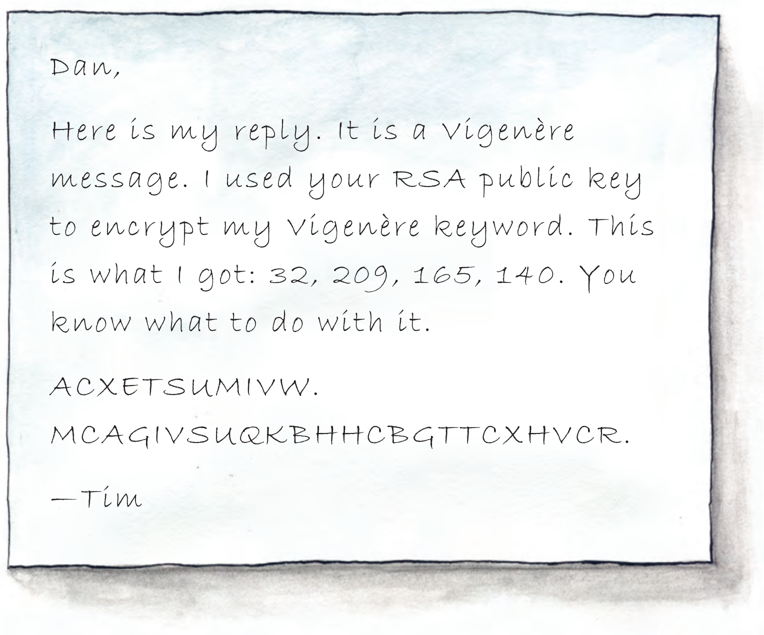
★ TIP

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.

MCAGIVSUQKBHHCBGTTCXHVCR.

—Tim

✎ **Do Problems 1–3 now.**

Index

The Cryptoclub

Using Mathematics to Make and Break Secret Codes

"[This book] certainly would have benefited me when I was in middle school."
—*from the foreword by Ronald L. Graham*

Join the kids of the Cryptoclub as they apply basic mathematics to make and break secret codes. The encryption systems covered in this book range from classic ciphers that have been around for hundreds of years, such as the Caesar and Vigenère ciphers, to the modern RSA system that provides security for information passed over the Internet. Connections are made to historical events and applications of recent mathematical research, giving students the opportunity to see mathematics as an exciting, changing subject.

The book includes problems, suggestions for games and classroom activities, and messages to encrypt and decrypt. The material can be used in conventional classrooms, by after-school clubs, in home-schooling environments, or for independent learning.

Mathematics topics covered include:

- ✓ Positive and Negative Numbers
- ✓ Decimals and Percents
- ✓ Data Analysis and Probability
- ✓ Prime Numbers and Factorization
- ✓ Modular Arithmetic
- ✓ Inverses
- ✓ Exponentiation

Janet Beissinger is a professor at the Institute for Mathematics and Science Education at the University of Illinois at Chicago. She is a coauthor of the widely-used *Math Trailblazers*, a mathematics curriculum for grades K–5.

Vera Pless is a professor in the Department of Mathematics, Statistics, and Computer Science, also at UIC. She is the author of *Introduction to the Theory of Error-Correcting Codes* and a coauthor of *Fundamentals of Error-Correcting Codes*. She has also published over 100 research papers.

ISBN 1-56881-223-X

9 781568 812236

A K Peters, Ltd.