
The Cryptoclub

Using Mathematics to Make and Break Secret Codes



Janet Beissinger
Vera Pless

Daria Tsoupikova, Artist



A K Peters
Wellesley, Massachusetts

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.