Teacher`s Guide

to accompany

The Cryptoclub

Using Mathematics to Make and Break Secret Codes

Janet Beissinger
Vera Pless

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.

The Library of Congress has cataloged the book associated with these teacher materials as follows:

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

Contents

Introduction

Cryptography has long been important to diplomats and military personnel. Today, it has become important to ordinary citizens when they use the Internet, ATM machines, and credit cards. But even before electronic communication made encryption necessary in everyday applications, children have always been intrigued by secret codes. Their natural curiosity and enjoyment in sending messages, combined with the mathematical nature of the subject, make cryptography a motivating setting for learning and applying mathematics skills.

The Cryptoclub follows a group of characters who form a club to help each other learn about cryptography. Mathematics is explored through conversations of the characters as they try to crack each other's messages. The book covers ciphers that apply mathematics topics that are part of the middle-grade curriculum, such as negative numbers, decimals and percents, prime numbers and relatively prime numbers, factorization and common factors, multiplicative inverses, and exponents, along with modular arithmetic that applies division with remainder. The ciphers range from classic ones that have been around for centuries to the modern-day public-key RSA cipher. Problems involve encrypting and decrypting riddles, quotations, and other longer messages. Particular focus is on how to crack messages when the key is unknown, since that takes more thinking and builds more problem-solving skills than simply using a known formula to decrypt.

Field-Test Settings

We developed and tested the material in a variety of settings in Grades 5–8. Teachers reported that it appealed to students of all ability levels. Students who usually are low achievers found it nonthreatening and enjoyable and therefore stayed on task. They were actively involved and able to experience success. High achieving students also enjoyed the material and were challenged by the non-routine mathematics involved. In several classes, the advanced students worked independently on the more difficult sections that the rest of the class did not cover.

Although the middle-school curriculum is already quite full, teachers found a variety of ways to fit in cryptography. During our testing, some teachers taught the material as part of their regular math classes and others used it in alternative settings, both inside and outside of school.

Regular Math Classes

About half of our field-test teachers taught cryptography interspersed throughout the year in their regular math classes. They used it to reinforce a variety of concepts and skills in their mathematics curriculum. They reported that it provided valuable experiences with problem solving and fostered a positive attitude about mathematics. Some chapters, such as Chapter 9 ("Factoring") and Chapter 16 ("Finding Prime Numbers"), can be used to replace similar chapters in the regular curriculum.

Alternative School Settings

Some teachers used the material in school settings other than regular math classes. A fifth-grade honors math class covered it one period per week throughout the year, as did a middle-grade remedial class. A seventh-grade gifted-class teacher covered the first half of the book during a concentrated three-week session. A sixth-grade teacher in a departmentalized school covered the first few chapters in a ten-week cross-curricular course that met twice a week with students of all ability levels.

Out-of-School Settings

In addition to the formal school settings, the book was also used in home-schooling settings, after-school math clubs, and a museum summer camp. Some students read it on their own, outside of any formal educational setting.

Suggestions for Teaching

The mathematics in the book is developed through the characters' conversations as they think about making and breaking each other's messages. One enjoyable way to get students involved in the book is to have the class read portions of it aloud, with students playing the roles of the characters. You can pause at times during the reading to highlight the key mathematics.

Students often do not read their math books, and this becomes a problem as they progress to high-school and college math courses. The style of the book is intended to help students make the transition from learning math by listening and watching a teacher, to learning by reading and thinking about what is in a math book.

Several chapters begin with the characters discussing how they would solve certain problems. It works well if you pose the problems to the class before reading how the characters solved them. This way, the book can reinforce the concepts after students have thought about them. The lesson guides for several of the chapters provide suggestions of opening questions for the class to think about before they read the chapter.

As students work on the problems in the book, encourage them to think on their own. They will have insights about how to solve the problems, and they will find different ways to crack the messages. Encourage them to discuss their methods with the class.

The many problems in the book help you to assess students' understanding. Students themselves will know whether they have correctly decrypted the messages, since their messages won't look like English if they have not.

One way to assess whether students understand certain broader topics is to ask them to teach someone at home. Ask them to describe in writing how to solve a problem, for example, how to crack a substitution cipher or how to reduce, add, and subtract numbers in clock arithmetic. Then have them show a family member what they have written. The family member can simply reply on the paper "we understand" or "we don't understand" and send it back to you. This helps you check your students' understanding and keeps parents connected as well.

Workbook

The workbook pages provide the same problems as the book, but in a format students can write on. You can either purchase printed workbooks from the publisher, or download an electronic version (PDF) from the publisher's website at no charge:

http://www.akpeters.com/product.asp?ProdCode=2981

If you print your own pages, ask students to keep them together in a binder, so they have access to the work they have done in previous chapters. If possible, print the pages double-sided so that they form a workbook when placed into a binder.

Using the ``Do You Know?´´ Items

Cryptography provides an opportunity to make many cross-curricular connections. Each chapter contains a "Do You Know?" item, which is a brief story of how cryptography has been used—or misused—throughout history. Some items connect to historical events, others to literature, and others to modern-day topics. They can be a springboard for further investigation of these topics.

If you don't plan to cover the entire book, you can still ask students to read all the "Do You Know?" items. Most are general enough that they don't require the specific content of the chapter in which they occur, so they can be read whether the chapter is covered or not. One way to do this is to have students read the "Do You Know?" from a chapter that is not covered and report to the class, perhaps adding information that they researched on their own.

Class Message Center

It is a good idea to have a box or a bulletin board where students can put encrypted messages for others to solve. Students who finish their work before others can create messages for the bin or they can decrypt messages that are already there.

You can suggest students write their message on the front of a slip of paper. They should write the name of the cipher they used, along with their names in case there are questions. They can choose whether they want to write the key or not—it is more challenging to crack a message if the key is not revealed.

Students who decrypt the messages can sign their names on the back for recognition, then return the messages to the bin for others to solve. Ask them not to write on the messages, so that others can work on them too. The messages can accumulate and be available when anyone has spare time. Then from time to time, you can read the names of the solvers and encourage others to join in the activity.

Classroom Treasure Hunts

In the Treasure Hunts section at the end of this guide, we describe two variations of classroom treasure hunts. In each variation, students follow a trail of encrypted clues hidden in the classroom or on the playground to find a treasure at the end. The hunts differ in the amount of preparation needed to implement them. In one type of hunt, you make and hide clues. In the other, students make and hide the clues. In the Treasure Hunts section, we provide sample clues, and we describe how to coordinate the hiding of the clues so that the hunts run smoothly.

The Cryptoclub Website

We have also developed an interactive website to support the learning and teaching of cryptography:

http://cryptoclub.math.uic.edu

It has tools for encrypting and decrypting messages, a classroom message board, interactive activities such as a treasure hunt, as well as math tools to help with topics such as modular arithmetic and prime numbers. It can help collect data about messages such as letter frequency that would be tedious to collect by hand. This allows students to work with more complex problems and more interesting messages. New activities are planned for future development. Most activities on the site require access to the Internet, however you can download the Treasure Hunt to a CD and install it on computers that do not have an Internet connection.

Electronic Classroom Message Board

The Cryptoclub website has an electronic message board that enables students to work with longer messages than they would normally want to encrypt or decrypt by hand. Users enter plaintext messages, and the machine helps encrypt them before posting. Classmates can then use the electronic tools on the site to help decrypt the messages.

You can sign up online for your own Classroom Message Board. Only users who have access to your class's account can read messages posted by your class. You will have a special password to your class's Message Board that gives you more powers than your students' password: for example, you can see decryptions of the messages that are on your class's message board. This way you can easily monitor the appropriateness of your students' messages without having to decrypt each one yourself. With your teacher password, you are also able to delete messages from your class's message board.

Electronic Treasure Hunt

After students have completed Unit 1, they will be ready to try the website's "Stormy Night Treasure Hunt." This is an animated adventure that students progress through by decrypting clues at the computer. The clues for this treasure hunt and their decryptions are provided in the Treasure Hunts section.

Recommended Reading

Books

In Code: A Mathematical Journey, by Sarah Flannery and David Flannery (Workman Publishing, 2001).

This book describes the first author's growth from a young girl who solved math puzzles with her family at dinnertime to a teenager who won both the Ireland Young Scientist of the Year Award and the European Young Scientist of the Year Award for her discoveries in cryptography.

Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age, by Steven Levy (Viking, 2001).

This tells how a group of mathematicians and programmers went outside the normal government security channels to make strong encryption available to ordinary people. It gives a very interesting account of the struggle between the government's need for security and individual citizens' rights to privacy in the age of technology. The level of the book is for older readers.

The Codebreakers: The Comprehensive History of Secret Communication form Ancient Times to the Internet, second edition, by David Kahn (Scribner, 1996).

This classic book, with nearly 1200 pages, gives a very thorough history of the subject.

The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography, by Simon Singh (Doubleday, 1999).

This gives a very interesting discussion of historical events that involved cryptography. It has a lot of information, without being too technical.

The Prince of Mathematics: Carl Friedrich Gauss, by M. B. W. Tent (A K Peters, Ltd., 2005).

This biography of Gauss is enjoyable reading for all ages, particularly intended to inspire young readers. It describes some of the mathematics problems Gauss solved as a child, as well as his achievements as an adult.

Journal Articles

Lisa J. Evered and Serigne Gningue. "Developing Mathematical Thinking Using Codes and Ciphers." *Teaching Children Mathematics* 8 (September 2001), 8–15.

This article uses messages from the 1930s and 1940s cartoon and radio characters Little Orphan Annie, Dick Tracy, and Captain Midnight to introduce principles of encrypting and decrypting.

Paul D. Marshall and Laszlo Varro. "Cracking the Code." *Mathematics Teaching in the Middle School* 10 (August 2004), 54–63.

This article describes a sixth-grade class's use of frequency analysis to crack a substitution cipher.

Jeffrey Wanko and Christine Venable. "Investigating Prime Numbers and the Great Internet Mersenne Prime Search." *Mathematics Teaching in the Middle School* 8 (October 2002), 70–76.

This article describes classroom activities for exploring large prime numbers. It also describes one class's participation in current mathematical research by signing up for the Great Internet Mersenne Prime Search.

Overview

The book contains seven units. Everyone should do Units 1 and 2, since they introduce basic terminology and cryptographic techniques. The other units can be selected as time permits. Unit 3 is a favorite of ours because it combines and reinforces skills learned in the first two units as students crack Grandfather's message about lost silver, but it is not a prerequisite for the units that follow. Unit 4 introduces modular arithmetic, which is used throughout the rest of the book, so it should not be skipped if you plan to cover later units. The last four chapters (Chapter 17 of Unit 6 and all three chapters of Unit 7) are beyond the level of most fifth and sixth graders. However, in our fifth- and sixth-grade field-test classes, some advanced students enjoyed working on those topics as a challenge, either independently or with other interested students.

Unit 1 Introduction to Cryptography

Chapter 1 Caesar Ciphers
Chapter 2 Sending Messages with Numbers
Chapter 3 Breaking Caesar Ciphers

Basic terminology used in cryptography is introduced. Students encrypt and decrypt with Caesar ciphers, which shift letters of the alphabet. They use both tables and cipher wheels to represent the shifts. Then, they change letters to numbers and shift by adding and subtracting. Finally, they crack messages when they don't know the shift amount, using patterns in the message such as frequency of letters.

- *Math Content:* Addition and subtraction, negative numbers, addition in a circle (in preparation for modular arithmetic), using tallies to collect data
- *Connections:* Julius Caesar, Paul Revere, radio shows in the 1930s and 1940s, American Gold Rush (Beale Cipher and Buried Treasure), Declaration of Independence, price of gold, Navajo Code Talkers, Pacific battles of World War II, quotations of famous people

Unit 2 Substitution Ciphers

Chapter 4 Keyword Ciphers
Chapter 5 Letter Frequencies
Chapter 6 Breaking Substitution Ciphers

Students explore letter frequencies and other patterns of English text and use them to crack substitution ciphers—ciphers in which letters or symbols are substituted for the plaintext letters. Chapter 4 introduces a specific kind of substitution cipher, the *keyword cipher*. The remaining two chapters develop techniques for cracking simple substitution ciphers. In Chapter 5, students determine the frequencies of letters in samples of English text. Then, in Chapter 6, they compare the letter frequencies in messages to the letter frequencies in regular English to crack the messages.

- *Math Content:* data collection, combining data from several groups, finding the frequency of letters in English text, computing relative frequencies, changing fractions to decimals, changing decimals to percents, ordering decimals, using data from a sample to predict
- *Connections:* Sir Arthur Conan Doyle, Sherlock Holmes mysteries, Edgar Allen Poe, Mary Queen of Scots

Unit 3 Vigenère Ciphers

Chapter 7 Combining Caesar Ciphers
Chapter 8 Cracking Vigenère Ciphers When You Know the Key
Chapter 9 Factoring
Chapter 10 Using Common Factors to Crack Vigenère Ciphers

Students encrypt, decrypt, and crack Vigenère messages, combining skills from previous units with other math skills such as finding common factors. The Vigenère cipher is interesting because it was once thought to be unbreakable, but today middle-grade students can break it. Encrypting with the Vigenère cipher involves dividing the message into parts and encrypting each part with different Caesar ciphers. This conceals letter frequencies, making it harder to crack than a simple substitution cipher. Cracking involves finding repeated patterns and then finding common factors of the distances between those patterns. Working with the Vigenère cipher, students combine many mathematics skills, solidify their understanding of concepts used in the previous units, and build confidence in solving complex problems.

- *Math Content:* Exploring different methods (wheels, tables, numbers) to represent information, finding data in a matrix (the Vigenère square), tallying letters to find the most common letters, combining data from several problems to solve a larger problem, finding prime factorizations, divisibility, exponents, finding common factors and greatest common factors, finding repeated patterns
- *Connections:* Lewis and Clark, Thomas Jefferson, American Civil War, life cycles of cicadas, one-time pad, VENONA program, spies during the Cold War

Unit 4 Modular (Clock) Arithmetic

Chapter 11 Introduction to Modular Arithmetic
Chapter 12 Applications of Modular Arithmetic

Students solve problems that involve adding and subtracting hours on clocks. The 24-hour clock is introduced, and arithmetic problems on this type of clock are solved. Then the notion of arithmetic on a clock is generalized to clocks of any size, and the terminology of modular arithmetic is introduced. Students explore ways to change decimal remainders displayed on their calculators into whole number remainders, and they solve calendar problems using modular arithmetic, including problems with leap years.

- *Math Content:* elapsed time, clock arithmetic, 24-hour time, modular arithmetic, multiplication and division, several ways to find remainders, changing decimal remainders to whole number remainders, problem solving with remainders
- *Connections:* World War I, Zimmermann telegram, ISBN numbers

Unit 5 Multiplicative and Affine Ciphers

Chapter 13 Multiplicative Ciphers
Chapter 14 Using Inverses to Decrypt
Chapter 15 Affine Ciphers

Students explore multiplicative ciphers in Chapter 13. It turns out that multiplying by some numbers makes a reasonable cipher, but multiplying by others does not. In a class activity, students determine that the numbers that make good multipliers (keys) are the ones that are relatively prime to 26, the size of the alphabet.

In Chapter 14, they review multiplicative inverses in regular arithmetic. They extend this concept to inverses in modular arithmetic and use modular inverses to decrypt multiplicative ciphers. In Chapter 15, they combine addition and multiplication to make affine ciphers. This unit spans a wide spectrum of mathematics levels from Grades 5–8. Chapter 13 is suitable for all levels, while the skills used to crack the ciphers at the end of Chapters 14 and 15 are more advanced. They involve looking for clues in the message and representing them in algebraic equations that they then solve.

- *Math Content:* multiplication (up to 2-digit by 2-digit numbers), reducing mod *n*, division with remainder, factoring, relatively prime numbers, multiplicative inverses in regular arithmetic and in modular arithmetic, using inverses to solve equations, factoring, reciprocals, relatively prime numbers, linear equations, solving two equations in two unknowns (optional)
- *Connections:* alphabets of different languages, passwords, World War II, German Enigma Cipher, the biblical cipher Atbash

Unit 6 Math For Modern Cryptography

Chapter 16 Finding Prime Numbers
Chapter 17 Raising to Powers

This chapter explores prime numbers and exponentiation. In Chapter 16, we investigate shortcuts for testing whether a number is prime. The Sieve of Eratosthenes is explored as a method for finding all prime numbers within a chosen range. The question of whether there is a largest prime number is discussed, with the conclusion that there are infinitely many prime numbers. Finally, special numbers are investigated: twin primes, Mersenne numbers, and Sophie Germaine primes, which have lead to the discovery of very large prime numbers. In Chapter 17, students raise numbers to powers and reduce in modular arithmetic. They discover that the exponent key on their calculators won't help because the answer is usually larger than the calculator can handle without rounding, which loses information needed to correctly reduce the answer. Students explore ways to avoid this round-off problem. As they work to solve the problems, they reinforce their understanding of exponents and develop flexibility in calculations.

- *Math Content:* factors, multiples, primes, and composites; efficient ways to test primality; Sieve of Eratosthenes; counting prime numbers; variables and formulas; special primes: twin, Mersenne, Sophie Germaine primes; Goldbach Conjecture; square root; googol, scientific notation on calculators, exponents, computing powers by repeated squaring, modular arithmetic
- *Connections:* Great Internet Prime Search (GIMPS), mathematics research, passwords

Unit 7 Public-Key Cryptography

Chapter 18 The RSA Cipher
Chapter 19 Revisiting Inverses in Modular Arithmetic
Chapter 20 Sending RSA Messages

This unit introduces the basic ideas of public-key cryptography and focuses on the RSA cipher, a powerful public-key cipher used for Internet security today. RSA involves raising numbers to powers and reducing in modular arithmetic. It uses large prime numbers, and cracking it involves factoring large numbers. Working with RSA is an opportunity for students to practice and expand what they know about prime numbers and factoring, work with exponents in a flexible way, and learn about some of the issues involved in modern-day cryptography. Public-key cryptography is introduced and the RSA cipher is described in Chapter 18. RSA uses modular inverses to compute its decryption key, so Chapter 19 revisits modular inverses. In the final chapter, students choose RSA keys and set up a classroom

Alignment with the NCTM's Principals and Standards for School Mathematics for Grades 6–8	Unit 1 Intro to Cryptography	Unit 2 Substitution Ciphers	Unit 3 Vigenère Ciphers	Unit 4 Modular (Clock) Arithmetic	Unit 5 Multiplicative and Affine Ciphers	Unit 6 Math for Modern Cryptography	Unit 7 Public-Key Cryptography
Number and Operation							
• Work with fractions, decimals, and percents to solve problems		×					
• Compare and order decimals		×					
• Develop an understanding of large numbers and recognize and appropriately use exponential, scientific, and calculator notation			×			×	×
• Use factors, multiples, prime factorization, and relatively prime numbers to solve problems			×		×	×	×
• Use negative integers	×			×			
• Understand and use the inverse relationships of addition and subtraction, and multiplication and division, to simplify computations and solve problems	×				×		×
• Develop and analyze algorithms for computing with integers						×	×
Algebra							
• Analyze and generalize a variety of patterns	×	×	×		×	×	
• Relate and compare different forms of representation of a relationship	×		×	×	×		×
• Develop initial understanding of different uses of variables					×		×
• Use symbolic algebra to represent situations and solve problems, especially those that involve linear relationships					×		×
• Solve linear equations					×		
• Model and solve contextualized problems using tables and equations			×	×	×		
Data Analysis and Probability							
• Collect data about a characteristic shared by two populations		×					
• Use observations about differences between two or more samples to make conjectures about the populations involved		×					
Reasoning and Proof							
• Examine patterns and structures to detect regularities	×	×	×		×	×	
• Formulate conjectures about observed regularities	×	×	×		×	×	
• Evaluate conjectures	×	×	×		×	×	

public-key directory. Then they combine the RSA and Vigenère ciphers to send messages. They use RSA to encrypt and decrypt keywords, which they use with the Vigenère cipher to encrypt and decrypt messages.

- *Math Content:* prime numbers, modular inverses, raising numbers to powers and reducing in modular arithmetic, relatively prime numbers, factoring, efficient trial-and-error methods to find inverses mod *n*
- *Connections:* mathematics research into large prime numbers and factoring, Thomas Jefferson and James Madison, British discovery of public-key cryptography

Alignment with NCTM Standards

The table outlines the alignment of the mathematics that students experience using these ciphers with the content standards in the NCTM *Principals and Standards for School Mathematics* for Grades 6–8.

In addition to the specific content standards listed in the table, teachers reported that engaging in the cryptography activities in the book strengthens students' problem solving skills. They reported that some of their students who don't normally experience success in other problem solving situations were willing to persist at solving problems in the cryptography setting.

Other Teacher Materials

There are three parts to the "Teacher Materials." The first is this *Teacher's Guide*. The second is the *Answer Key*, which provides the solutions to the problems in the book; it is formatted exactly like the workbook, but with the answers filled in. The third part is the *Blackline Masters*, pages designed to be copied and handed out as needed; some are handouts described in this guide, and other pages are blank tables to facilitate more code making and breaking.

Unit 1

Introduction to Cryptography

This unit introduces students to the basic terminology of cryptography. In Chapter 1, the Caesar cipher is introduced, which shifts letters of the alphabet to encrypt. In Chapter 2, the messages are converted to numbers and then encrypted by adding. In both cases, it is easy to decrypt a message if you know how much the letters were shifted or what was added to each number. In Chapter 3, students crack messages when they don't know the shift amount. This is more challenging, but by collecting data about the frequencies of letters in the message and using what they know about patterns in English, they are able to figure out the shift amount.

You can extend the activities in this chapter by having students make their own messages. They can leave these in a class Message Center to be solved by others, or they can use them to play Cipher Tag, a game in which students take turns presenting encrypted messages for the class to decrypt.

After students are familiar with the ciphers in this unit, they are ready to visit the Cryptoclub website.

Chapter 1

Caesar Ciphers

Summary

Basic terminology used in cryptography is introduced. Students encrypt and decrypt using a Caesar cipher, which is represented with a cipher table and also with a cipher wheel. Students make and use their own cipher wheels.

Key Vocabulary

cryptography
cipher
cipher wheel
Caesar cipher
encrypt
decrypt
plaintext
ciphertext

Materials

cipher wheel circles, one set per student, from student text or copied onto cardstock from "Cipher Wheels" in *Blackline Masters*
scissors, one pair per student (for cutting wheels)
brads (paper fasteners), one per student
optional: paper clips, one per student, to clip wheels inside workbook cover for storage

Connections

Julius Caesar
Paul Revere
radio shows in the 1930s and 1940s

Opener

It works well to begin most chapters with a short problem for students to think about, before they read about the methods described in the chapter. Encourage them to use their own observations and understanding of patterns in English and mathematics to help solve the problems. After they have worked on the problem themselves, they are ready to read about how the characters in the book solved similar problems.

As an opener for this chapter, put an encrypted riddle or message on the board for students to try to crack. Here is a sample riddle, whose answer was encrypted with a shift of one letter:

Riddle: What is the clumsiest bee?
Answer: B CVNCMJOH CFF (a bumbling bee)

You don't need to explain in advance how the answer was encrypted—just let students try to figure it out for themselves. After some have successfully decrypted the message, ask them to explain the clues that helped them figure it out. Some might mention the one-letter word (**B**) or the double letters (**FF**). Some will explain that they used trial and error until they got a message that made sense.

Teaching

One way to teach the lessons is for students to take turns reading the text aloud, pausing to work on the problems as they come up. You can begin Problem 1 with the whole class, but then let students finish by themselves. They can discuss their answers with their partners or groups as they go along. Decrypting is often easier and more interesting than encrypting because students can tell when they get the correct answers—if they have made mistakes, their answers won't make sense.

A common mistake when encrypting and decrypting is to mix up the plaintext and the ciphertext. To avoid confusion, we usually use lowercase for plaintext (except for proper nouns and at the beginning of sentences) and uppercase for ciphertext. It is not essential that students follow this convention in their own writing, but they might find it helpful. We also always put the plaintext on top and the cipher text underneath. Doing this consistently will help avoid confusion.

In the second part of this chapter, students make cipher wheels. The wheels will be used often, so it is a good idea to laminate them or copy them onto cardstock to make them sturdy. To save paper, use the "Cipher Wheels" page in *Blackline Masters*, which has several circles on one page. Alternatively, students can cut the wheels from their books.

It is very important that students match up the centers of the two circles when they make their cipher wheels. If the brad is placed off-center, then the letters will not line up properly when the wheel is turned.

Since the wheels will be used often, students should keep them in a safe place. It works well to clip the wheel into the workbook or text with a paper clip so that it is always available.

Students are sometimes confused about how to turn the cipher wheel to get the desired shift. Ask them to line up the plaintext **a** with the ciphertext **A**. Then have them turn their inner wheels *counterclockwise* one letter so **a** matches **B.** Explain that this is a shift of one. Continue turning to show other shifts.

In the game Cipher Tag, students take turns presenting encrypted messages for the class to crack. Common mistakes are often detected when you play Cipher Tag. One common mistake is turning the wheel the opposite direction—it helps if you get everyone to set their wheels together before they do a lot of work on a problem. Students usually enjoy playing Cipher Tag. It is suggested several places in the book, as other ciphers are introduced.

Students who finish early can make up their own riddles and encrypt their answers. Post sheets of paper on which students can record their riddles for others to work on at another time. You can clip a Caesar wheel to the sheet for students to use when decrypting. Another idea is to make a class Message Center. Students write encrypted messages on the front of a piece of paper, sign their names in case there are questions, and place the paper in a bin or envelope. Students who decrypt a message write their names on the back and return it to the bin for others to solve.

Related Topics

Topics such as Paul Revere and Julius Caesar appear briefly in this section. You can use this as an opportunity to discuss geography or history or other related topics. Also of interest are the cartoons and radio shows of the 1930s and 1940s that incorporated ciphered messages. See the article "Developing Mathematical Thinking Using Codes and Ciphers" by Lisa J. Evered and Serigne Gningue for more details (*Teaching Children Mathematics* 8, September 2001, pp. 8–15).

Chapter 2

Sending Messages with Numbers

Summary

In this chapter, letters are encrypted with numbers. Students continue to use Caesar ciphers, but this time the shift is described by adding. Decrypting involves subtracting, which often leads to negative numbers. Methods to make calculations easier are explored, and in the process, the concepts of modular arithmetic are informally introduced.

Math Content

addition and subtraction
negative numbers
addition in a circle—preparation for modular arithmetic

Key Vocabulary

equivalent on a circle
congruent on a circle

Materials

"hat" or basket for collecting encrypted names (Exercise 1)

Connections

American Gold Rush (Beale Cipher and Buried Treasure)
Declaration of Independence
price of gold

Opener

Before students read the chapter, ask them to crack a few messages encrypted with numbers. Riddle 1 is a sample message that simply substitutes 0 for **A**, 1 for **B**, and so on. After they have solved Riddle 1, they are ready for Riddle 2, which makes the same number-for-letter substitutions, but then adds 3 to everything.

Riddle 1: What has teeth but can't bite?
Answer: 0 2 14 12 1 (a comb)

Riddle 2: What do you call a dog in a car?
Answer: 3 5 3 20 18 7 22 (a carpet)

Don't explain in advance how the messages were encrypted, but ask students who were able to solve them to explain how they did it. Some students will notice that the first number must be **a** or **I** because those are the only one-letter words. That helps them figure out the other letters.

Teaching

Some students find encrypting with numbers easier than shifting letters. There is less confusion about what is plaintext and what is ciphertext. To encrypt, they add; to decrypt, they subtract.

Since the numbers involved with these ciphers are only the numbers 0 through 25, the addition and subtraction involved is a special arithmetic, called clock or modular arithmetic (mod 26). Terminology used with modular arithmetic will be introduced more formally in Unit 4, but in this chapter students work informally with the following key ideas:

- If adding (shifting) results in a number larger than 25, start counting again with 0 = 26, 1 = 27, and so on. (Example: 24 + 4 = 28 = 2.)
- If subtracting gives a negative number, count backwards from 26 = 0. (Example: 5 – 8 = –3, which is 3 less than 0. Since 0 is equivalent to 26, –3 is equivalent to 23.)
- If we encrypt by adding a number, we can decrypt by subtracting that number. But, there is another number that could be used to give the same answer by adding. The circle with the 26 numbers from 0 to 25 is a good tool for showing this: going around 20 places in one direction (adding) is the same as going 6 places in the opposite direction (subtracting). The same is true for decrypting (see answer to Problem 16).

As students work with encrypting and decrypting in this chapter, encourage them to look for ways to make their calculations easier. Since a message can be encrypted either by adding *n* or by subtracting 26 – *n*, encourage them to choose the method that makes their calculations simplest (see answers to Problems 17–19)—the simplest method might be different for different letters in the same message.

This activity can help you to diagnose weaknesses that your students might have in subtraction. Some students make systematic errors that can be pinpointed as you watch them solve these problems.

To keep faster students engaged, you can keep an ongoing collection of encrypted riddles or other messages. Students who finish early can add to this collection or choose something from it to decrypt.

Students play Cipher Tag again in this chapter. Sometimes it is hard to figure out other students' messages. They might make errors in the original spelling of the words or in the encrypting. It often helps to work with a partner and double check before taking a turn at being "It."

Related Topics

The "Do You Know?" about the Beale Ciphers that appears at the end of the chapter can be discussed at any time—it is not directly related to the cipher used in this chapter. Some students may want to investigate it further. An excellent reference is *The Codebook*, by Simon Singh (Doubleday, 1999). The Internet also has many links to the Beale Cipher.

Students who investigate will discover that the cipher used to decrypt the second page of Beale's messages is not too difficult for them to understand. It involves the Declaration of Independence. Each word of the Declaration is numbered in order, and the first letter of the word is assigned that word's number. Here are the first ten words: "^{1}When ^{2}in ^{3}the ^{4}course ^{5}of ^{6}human ^{7}events, ^{8}it ^{9}becomes ^{10}necessary…." Since the first word starts with **w**, 1 represents **w**. Similarly 2 represents **i**, 3 represents **t,** 4 represents **c**, and so on. (In this method, the same letter could be represented by different numbers, for example, **i** = 2 and also **i** = 8.)

An interesting problem is to calculate the value of the Beale treasure using today's prices. Students will have to investigate the current prices of gold and silver per pound and then combine that with the number of pounds given in the story to calculate the value.

Chapter 3

Breaking Caesar Ciphers

Summary

Students crack Caesar ciphers when they don't know the key. One method that they use is to guess the decryptions of the one-letter words and use this to set the wheel. Another method is to find the most common letter in the message and match it with the most common letter in English.

Math Content

collecting data with tallies

Key Vocabulary

algorithm
key

Materials

cipher wheels, one per student
optional: "Can You Crack These Messages?" (page in *Blackline Masters*), one copy per student or one transparency

Connections

Navajo Code Talkers
Pacific battles of World War II
quotations of famous people

Opener

In this chapter, the Cryptokids in the story crack three messages of increasing difficulty. Before students read how they do it, ask them to crack the three short messages on "Can You Crack These Messages?" Make copies or a transparency, or write the messages on the board. Here are the messages, along with their decryptions:

1. Ciphertext: AOL AYLHZBYL PZ OPK BUKLY AOL VSK VHR AYLL (hint: 7)

   Plaintext: The treasure is hidden under the old oak tree.

   The number 7 is a hint that the alphabet was encrypted with a shift of 7.

2. Ciphertext: N XFB YMJ UNWFYJ GZWD YMJ LTQI.

   Plaintext: I saw the pirate bury the gold.

   *A clue is in the one-letter word. Since one-letter words are usually a or I, you can try each of those possibilities. Here, matching the ciphertext **N** with the plaintext **i** gives a message that makes sense.*

3. Ciphertext: EWWLHWLWJSFVEWLGFAYZLSLGMJKWUJWLHDSUW. AZSNWKGEWLZAFYWDKWLGLWDDQGM.

   Answer: Meetpeterandmeatmidnightatoursecretplace. ihavesomethingelsetotellyou.

   *This can be broken by noticing that the most common letter in the message is **W**. This most likely corresponds to the most common letter in English, which* *is **e**. We don't expect that students will decrypt this third message, but thinking about it as an opener will help prepare them for reading the chapter since it is the message that is cracked by Evie at the end of the chapter. Working with this message should lead to the observation that removing spaces between words makes messages harder to break.*

Teaching

This chapter introduces two new words, *key* and *algorithm*. An important issue in cryptography is how a person who wishes to send a secret message can let the receiver know what encryption key has been used. Ask your students to think of ways to solve this problem. One method is to agree in advance to shift according to something everyone knows or can easily find out, such as the date. For example, on the fifth day of the month, they will shift 5 places. Students might have other suggestions.

The word *algorithm* might be familiar to your students from other contexts. In general, an algorithm is a systematic method for doing something. In arithmetic, an algorithm is a procedure for doing a calculation, for example, long division. In computer science, an algorithm is a step-by-step method for solving a problem on a computer. In cryptography, it is the method of encrypting, such as shifting letters a chosen number of places.

In this chapter, students decrypt messages without knowing the key in advance. This is more challenging than when they know the key, but it is also more rewarding. Messages are decrypted by matching one of the most common letters in the message with **e**, the most commonly occurring letter in English. To crack a Caesar cipher message, only one letter needs to be guessed—from that you can determine what the shift is. In the next chapter, we will look at substitution ciphers where there isn't a simple shift pattern. In that case, the frequency of all letters is used, not just one letter.

After students have solved the cryptograms, ask them what clues helped them besides letter frequency. Some might use patterns in English, such as common two- and three-letter words, letters that follow apostrophes, and letters that occur as double letters.

The messages in this section are quotations from famous people. You can have students find and encrypt other quotations for the class to decrypt.

Related Topics

The story of the Navajo Code Talkers has been in the news in the last few years. An Internet search brings up several websites that give more information about this topic.

Website

This would be a good time for students to visit the Cryptoclub website,

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

It has an animated treasure hunt, through which students proceed by decrypting clues. All the clues involve Caesar ciphers with either letters or numbers.

If you have access to a computer that can be connected to a projector, we recommend that you use it to introduce the components of the website. It is helpful for students to have suggested activities to do when they visit the site, rather than general instructions to explore it.

Unit 2

Substitution Ciphers

In this unit, students explore letter frequencies and other patterns of English text and use that information to crack substitution ciphers.

A substitution cipher is a cipher in which letters or symbols are substituted for the plaintext letters. The Caesar cipher of the last unit is an example of a substitution cipher, but there are many others. In this unit, we'll work with *simple* or *monoalphabetic* substitution ciphers. The Vigenère cipher of the next unit is a polyalphabetic substitution cipher, because it makes different substitutions for the same letter in different parts of the message.

Substitution ciphers have long been favorites of puzzle lovers. "Cryptograms," which are messages encrypted with substitution ciphers, regularly appear in newspapers and magazines. Entire books of cryptograms are often found where crossword puzzle books are sold.

Simple substitution ciphers can usually be cracked by matching the most common letters in the message with the most common letters in English and by recognizing patterns in words. Although many people enjoy solving cryptograms for recreation, cracking substitution ciphers also provides an excellent opportunity to develop mathematical skills such as collecting and analyzing data and using decimals and percents.

In the first chapter of this unit, Chapter 4, we introduce a specific kind of substitution cipher, the keyword cipher. This has the advantage that it can easily be described with a keyword and a key letter. The remaining two chapters develop techniques for cracking simple substitution ciphers. In Chapter 5, students explore the frequency of letters in English. Then, in Chapter 6, they use these frequencies to crack messages.

After students have had the opportunity to collect data and compute letter frequencies themselves, we encourage you to have them use the Cryptoclub website. There the frequencies can be quickly computed by machine, freeing students to use the data and their own reasoning skills to crack longer and more interesting messages.

Chapter 4
Keyword Ciphers

Summary

The chapter begins with a discussion of substitution ciphers. It then focuses on the keyword cipher, which is a particular type of substitution cipher.

Key Vocabulary

substitution cipher
keyword cipher
keyword
key letter

Materials

Optional: "Can You Crack This?" (page in *Blackline Masters*), one copy per student or one transparency

Connections

Sir Arthur Conan Doyle
Sherlock Holmes mysteries

Opener

Caesar ciphers are fairly easy to break, as students discovered in the last chapter. However, in general, substitution ciphers are not as easy. You can open this lesson by asking students to try to crack the following message, which appears on the "Can You Crack This?" blackline master.

Ciphertext:

CUVB ZPBBLSP HLB PGNTJECPO HVCU L XPJHRTO NVEUPT. NULECPT 4 HVYY CPYY URH L BPGOPT NLG OPBNTVMP CUP BDMBCVCDCVRG CLMYP MJ CPYYVGS JRD RGYJ L XPJHRTO LGO L XPJ YPCCPT.

Students will probably first try to decrypt the one-letter word as **a** or **I** and use Caesar wheels to figure out the rest of the letters, as they did in Chapter 3. But, this will give a message that doesn't make sense. They will realize quickly that this message is different from other messages with which they have worked. It couldn't have been encrypted by simply shifting the alphabet.

After awhile, write the following substitution table on the board, and let them use it to decrypt the message.

After making the table substitutions, they will have the following message.

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

Plaintext:

This message was encrypted with a keyword cipher. Chapter 4 will tell how a sender can describe the substitution table by telling you only a keyword and a key letter.

Ask, "How would you tell a friend the table you used?" They will probably agree that the entire table would have to be written out. They are now ready to read about the keyword cipher, which can be described with only one word and one letter. From the keyword and key letter, the receiver can recreate the substitution table used to encrypt.

Teaching

Ask students to read the story in the text. In it, Dan realizes that the shift pattern in Caesar ciphers makes them too easy to break, so he makes a substitution cipher that has no pattern at all. But, he realizes that it is awkward to send the entire table along with the message, and this motivates the discussion of the keyword cipher.

The keyword cipher is a substitution cipher that is not as easy to crack as Caesar ciphers because it does not have obvious patterns, and it is easy to use because the sender can describe it with just one keyword and one key letter.

Create the substitution tables for a few keyword ciphers together, so everyone sees how to do it. First the keyword is written, beginning under the key letter. Then the alphabet follows, omitting any letters that have already been written. There is a special case students need to be aware of: letters that repeat in the keyword are only written once (e.g., **DANNY** is written as **DANY**, and **MISP** is written instead of **MISSISSIPPI**).

Students sometimes make mistakes when writing out keyword cipher tables. They either omit letters or put some letters in more than once. It is easy for them to realize when they have made a mistake, because the alphabet won't fit in the boxes. When this happens, they need to go back and make changes. You should advise them to use pencil so they can erase.

Dan's message in Problem 8 is fairly long. You can assign each group a few lines and have groups take turns reading their decryptions aloud to reveal the entire message. (Some students enjoy long messages and might choose to work on more than what they are assigned.)

The workbook has extra cipher tables on page W22 to use for additional messages. Encourage students to put messages in the class Message Center for others to decrypt.

Related Topics

The Sherlock Homes mystery, "The Adventure of the Dancing Men" by Arthur Conan Doyle, is an example of a fiction story that uses cryptography. Ask students to decrypt Slaney's message that appears in the "Do You Know?" of this chapter. Using the substitutions given, the message becomes, "Come here at once."

Classroom Treasure Hunt

This would be a good time to prepare a classroom treasure hunt. Descriptions of two different types of hunts are in the "Treasure Hunts" section at the end of this guide. You can use Caesar ciphers with letters, Caesar ciphers with numbers, and/or keyword ciphers to encrypt your clues. You can save time by using the website to encrypt. If students have easy access to computers, they can use the website to decrypt longer clues.

Website

You can use the Substitution Cipher on the Cryptoclub website to encrypt and decrypt messages with keyword ciphers. Enter the keyword and key letter, and fill out the rest of the alphabet to make the substitution table; the computer uses your table to encrypt and decrypt. Alternatively, the website's Classroom Message Board is a place where you can quickly encrypt using a keyword cipher without entering the table.

Chapter 5

Letter Frequencies

Summary

Students collect data about the frequency of letters in typical English text. Each group selects a sample from a newspaper or magazine and counts the occurrences of each letter of the alphabet. The class combines their data to make a larger sample. From this data, the relative frequencies of letters in English are estimated. Students compare the class data with data collected by mathematicians. They discuss the effects of sample size and other factors on their data.

Math Content

data collection—combining data from several groups
finding the frequency of letters in English text
computing relative frequencies
changing fractions to decimals
changing decimals to percents
ordering decimals
using data from a sample to predict

Key Vocabulary

frequency
relative frequency

Materials

a few lines of text (about 100 letters) from a newspaper, magazine, or other text, per group (Note: Each group should have a different sample, and they should be able to write on it.)
one transparency of "Class Letter Frequencies" (page in *Blackline Masters*), or a similar table drawn on the board or chart paper
calculators

Connections

Edgar Allen Poe, the originator of the detective story

Opener

Ask students to select a sample of about 100 letters from a newspaper, magazine or other text. Be sure groups choose different samples—using the same text for each group will defeat the purpose of collecting multiple samples. Some students like to cross off letters as they count. For this reason, it is a good idea to give them text they can mark on, such as old newspapers instead of books.

Teaching

In the Class Activity of this section, groups collect data from a relatively small sample of letters. Then, they combine their data to get one large class sample. They compare the effects of sample size on the data collected and discuss variations in individual groups' data.

So that the activity runs smoothly, it is important for each group to understand its role in contributing to the class's results. Here is a summary:

- In Part 1, student groups choose a sample of about 100 letters. They count the number of occurrences of each letter in their sample and record it in their workbooks in the Letter Frequencies for Your Sample table on workbook page W23.
- In Part 2, the class pools their data to make a larger class sample. They record their groups' data on a table that you provide. This can be a transparency of the "Class Letter Frequencies" blackline master page or a class table that you make on the board or on chart paper. After all groups have entered their data, assign each group the task of adding a few rows of the class table and writing the row sums on the table so that the Total for All Groups column is completed. (See the figure on text page 37.)
- In Part 3, students compute the relative frequencies of the letters in the class sample. They record their findings in their workbooks in the Relative Frequency table on workbook page W24. (They first transfer the class's information from the Total for All Groups column of the Class Letter Frequencies table of Part 2 to the Frequency column of their Relative Frequency table of Part 3.)

There are various ways students might choose to collect their data. Some might work in pairs with one partner reading off the letters and the other making tallies as the letters are read. Others might count all the **A**s, then all the **B**s, and so on. In this case, they can divide up the letters so that each person in the group counts some of the letters and no one has to count all 26 letters. Ask them to suggest different methods before they begin, and then let each group choose the method that they prefer.

It is not important that they count exactly 100 letters, since they will later divide by the total number counted to arrive at the relative frequency. If one group counts substantially more than 100 letters, their raw data will look different when posted on the group table, but the most common letters will probably be the same as for the other groups. This is an opportunity to discuss the effects of sample size.

After they have answered the workbook questions, discuss their results. Ask students to look at the Class Letter Frequencies table on the board, chart, or overhead. Here are a few questions you might ask about the data:

- *What are the most common letters?*

  The most common letters in the class data will probably be **E**, **T**, **A**, **O**, and **I**, although not necessarily in that order.
- *Is **E** the most common letter in every group?*

  In many groups, **E** will be the most common letter, but probably not in all groups. Be sure to call attention to data from groups that have a different most common letter, since students often mistakenly assume **E** is always the most common letter when they crack substitution ciphers.
- *Can you compare raw data between groups?*

  Looking at the raw numbers does not tell you how common a letter is. For example, one group might count 16 occurrences of the letter **N**, while another group counts 12 occurrences of the letter **E**. But this does not necessarily mean **N** was more common than **E**. If further examination reveals that the first group counted a total of 252 letters, while the second only counted 105 letters, then in the first group **N** occurred 16/252 = 6.3% of the time and in the second group **E** occurred 12/105 = 11.4% of the time.
- *Why do some groups have very different data?*

  A few groups might have unexpectedly high occurrences of some letters. Ask them to look at the text they analyzed to find an explanation. Sometimes the text repeats a word such as a name, and this makes certain letters occur more often than expected.

- *Does the class data match the table in the book?*

  Although groups will vary in how closely their data matches the table on text page 39, the frequencies in the combined class data will probably be quite similar to that table. That is because larger samples tend to average out special cases that occur in small samples.

Related Topics

The “Do You Know?” in this chapter discusses the author Edgar Allen Poe, who was very interested in cryptography. In fact, some people believe the story of the Beale Ciphers (Chapter 1) was really a hoax created by Poe. Students might enjoy researching Poe’s other writings about cryptography.

Edgar Allen Poe and Sir Arthur Conan Doyle are two authors who have used codes in their stories. Ask students to suggest other literature they have read that involves cryptography.

Chapter 6
Breaking Substitution Ciphers

Summary

The characters in the story compare the letter frequencies in a message to the letter frequencies in regular English to crack a substitution cipher. Students do the same for two other messages. For the first message, students collect letter frequency data and use it to crack the message. For the second message, they use data that has already been collected for them.

Math Content

data collection
computing relative frequencies
changing fractions to decimals
changing decimals to percents
ordering decimals
using data to solve a problem

Materials

calculators

Connections

Mary Queen of Scots

Opener

This chapter uses the data collected in the previous chapter, so a separate opener is not necessary.

Teaching

Explain that, by comparing the most common letters in English with the most common letters in a message, simple substitution ciphers can often be broken. In the Caesar cipher, only one letter needs to be matched to determine the shift. However, in a substitution cipher that doesn't have such a nice pattern, each letter needs to be matched. Letter frequencies, along with other information about word patterns, can suggest the underlying substitutions.

There is a detailed discussion in the text about the clues Jenny used to crack Dan's message. The specific way that Jenny cracked the message in the text is not important, since there are many ways to do it. What should come through in reading is more the spirit in which she cracked it. Here are some of the phrases she uses that indicate a style of attacking a problem, not necessarily a specific method:

> "I decided to decrypt the most common letters first…"
> "I went with my first guess…in pencil because I knew I might change my mind later.…"
> "The whole time I was working on this, I was keeping track of the substitutions…"
> "Next I looked for other short words…"
> "That didn't look like a familiar word…So I skipped **I** for a while."
> "…the word **here** appeared. That encouraged me."

"I noticed an apostrophe…"
"I must have been wrong….so I erased the match of **M** with **n**. It's a good thing I used pencil…"
"At this point I didn't need frequencies. I could see what the message probably said…"

Ask students to work with partners to collect data on the frequency of letters in Jenny's message (Problem 1) and use the data to crack her cipher. They should decide whether they want to record tallies as one partner calls out the letters or simply count occurrences of each letter.

When students decrypt the message, it will help if they write the original words in lower case above the encrypted words. This is consistent with their previous work. Remind them that since their first guesses for letter substitutions might not be correct, they should use pencil so they can erase.

You should let them make mistakes in their substitutions because they will often be able to recognize and correct their own mistakes. However, if you find a group has made several incorrect substitutions, you can give them a few clues about which of their substitutions are correct, so they can change the others and get back on the right track.

One common mistake students make when using letter frequencies to break substitution ciphers is to assume that the most common letter in English must match the most common letter in the message, the second most common letters must match each other, and so on. It is important to stress that the letter frequencies give suggestions—not guarantees—as to which letters might be substituted for others. Students should also use other clues, such as those listed in the tip on text page 48.

Students will probably notice that, when cracking messages, they usually don't need all the letter frequencies. They use the frequencies to get started, but after the words begin to emerge, their knowledge of English is probably more useful than the frequencies. (In messages that do not have spaces between words, it is more difficult to recognize words, and the frequencies become more helpful.) In this chapter, we've asked them to work with all the frequencies to reinforce their understanding of decimals and percents. In later chapters, they won't have to compute all 26 letter frequencies each time they want to crack a message.

Problem 2 can be used for homework or extra practice in class. The letter frequencies have already been computed, so the work will go more quickly.

When students have finished cracking the message(s), make a class list of the methods that they found most useful. It will look something like the list in the tip on text page 48, but it should reflect their opinions of what worked best for them.

Related Topics

The "Do You Know?" of this chapter tells the story of Mary Queen of Scots, who was executed when secret messages were cracked, implicating her in a plot to overthrow Queen Elizabeth. An interesting account of this story is in Simon Singh's *The Codebook* (Doubleday, 1999).

Website

There is a Frequency Analysis tool on the Cryptoclub website that can be used to crack substitution ciphers. It computes the frequencies, and it also substitutes your guesses. This makes it easy to change your guesses—the machine erases for you.

To encrypt your own messages for students to decrypt, you can use the Substitution Cipher in the Cipher section of the website. Students can then use the Frequency Analysis tool to help crack the messages.

The Classroom Message Board on the website is a good place to leave encrypted messages for each other. That way, errors in typing are avoided. Choose the keyword cipher on the Message Board to encrypt. Since a keyword cipher is a type of substitution cipher, it can be decrypted using the Frequency Analysis tool.

Unit 3

Vigenère Ciphers

After students have learned to crack the ciphers from Units 1 and 2, they might like to learn about a cipher that is harder to break. The Vigenère cipher is certainly harder—for centuries people believed it was unbreakable—yet today students can break it with nothing more than middle-grade mathematics, as long as the keyword is not too long.

The Vigenère cipher is a good choice to teach for several reasons.

- Encrypting, decrypting, and cracking a Vigenère message reinforce what students learned about the Caesar cipher in Unit 1.
- Cracking a Vigenère message involves many steps and combines many mathematics skills. It gives students the opportunity to build confidence in solving complex problems.
- The Vigenère cipher has historical connections: For example, the Confederate Army used it during the American Civil War. Before that, President Jefferson suggested to Lewis and Clark that they use it to send him messages during their expedition.

The Vigenère cipher is an example of a polyalphabetic cipher. It involves breaking a message into parts and using different Caesar ciphers to encrypt the different parts of the message. By doing this, the same letter is encrypted different ways in different places. This conceals letter frequencies, and therefore cracking a Vigenère cipher is more complicated than cracking a simple substitution cipher.

To crack a Vigenère message, students find repeated patterns in the ciphertext. Then, they find common factors of numbers that are related to these patterns. This tells them how to break up the message into parts that can be decrypted separately using the frequency analysis methods that they previously used for Caesar and substitution ciphers. Thus, working with the Vigenère cipher solidifies their understanding of concepts used in the previous chapters, while requiring a new understanding of how components of a problem fit together.

In the first chapter of the unit, Chapter 7, students learn to encrypt and decrypt Vigenère ciphers. In Chapter 8, they learn how to crack a Vigenère cipher when the key length is known. The case of how to crack a Vigenère message when they know nothing about the key, not even the length, involves finding common factors. To prepare for this, factorization is covered in Chapter 9. Students who are familiar with factoring and finding common factors can skip Chapter 9 and go right to Chapter 10, where they apply common factors to crack Vigenère messages.

The background story of this unit involves a note Jenny and Abby find among their Grandfather's old papers. In the process of cracking the message, they learn about Vigenère ciphers. The message is finally decrypted in the last chapter of the unit and reveals information about a silver treasure.

We recommend that, after students have worked with Vigenère messages by hand, they use the Cryptoclub website to encrypt, decrypt, and crack Vigenère messages. If you want to create Vigenère messages for students to crack, they will need to be longer than substitution messages in order for there to be enough data (see Chapter 10 for more details). But, working with long messages by hand can be very tedious. Students will be able to focus more on using their reasoning skills if the machine does some of the data collection and computation for them.

Chapter 7

Combining Caesar Wheels

Summary

Students explore three different ways to represent a Vigenère cipher: with Caesar wheels, with a Vigenère square, and with numbers. A Vigenère cipher encrypts letters differently in different places in the message and is therefore more difficult to break than a simple substitution cipher. The characters in the story are motivated to learn about the Vigenère cipher after they discover an encrypted message that does not appear to be a substitution cipher among their grandfather's papers in the attic.

Math Content

exploring different methods (wheels, tables, numbers) to represent information

finding data in a matrix (the Vigenère square)

Key Vocabulary

Vigenère cipher

Materials

cipher wheels, one per student

Vigenère Square (inside front cover of text), one per student

Connections

Lewis and Clark

Thomas Jefferson

American Civil War

Teaching

The chapter opens with Jenny and Abby finding an encrypted note that they assume was written by their grandfather. Ask students to examine Grandfather's note on text page 54 to see whether there are unusual patterns in it. Ask whether it could have been encrypted with a simple substitution cipher. (These are the questions in the discussion box on text page 54). They can examine the note as an opener before reading the chapter or after the class reads the first few pages.

Here are some of the unusual things about Grandfather's message students might observe:

- **OOF** is a word that begins with a double letter.
- **CGGG** has 3 repeated letters in a row.
- There are many different letters that are one letter words—in a substitution cipher we would expect at most two different one-letter words.

These unusual patterns suggest that the note couldn't be a simple substitution cipher. This begins the study of the Vigenère cipher.

We present several ways to encrypt with a simple Vigenère cipher. The first way uses wheels and the second uses the Vigenère square. Students should try both of these methods and then use whichever method works best for them. A third method uses numbers and is outlined as a challenge in Problem 11.

When using the Vigenère cipher, it is important to correctly write the keyword above the message. Leaving a letter out or adding an extra space will change the way all the letters that follow are encrypted. This caused problems for soldiers in the Civil War, and it will cause problems for students as well, if they are not careful.

Students will most likely work at different paces as they decrypt the messages in the problems of this chapter. It is not essential that all students complete all the messages before moving on. You might assign each group one message to report on and ask them to work on as many other messages as time permits. After they have used both the wheel and the square methods, they can move to Problem 10 and create their own messages to share.

Messages from Problem 10 can be used to play Cipher Tag, or can be copied and placed in the Message Center for others to decrypt. Creating messages makes a good homework assignment because students' families can help them select interesting quotations to encrypt.

Related Topics

The "Do You Know?" items in this unit discuss several historical connections to the Vigenère cipher. This chapter discusses the use by the Confederate Army in the American Civil War. The next chapter discusses the use by Lewis and Clark, and the final chapter discusses a generalization, the one-time pad, which is unbreakable. Students might want to explore these uses in greater depth.

Website

It can be very tedious to encrypt and decrypt long Vigenère messages by hand. We encourage you to visit the Cryptoclub website and use the encrypting/decrypting tools to create messages for your students. You can post messages on your Classroom Message Board (which encrypts for you), where your students can retrieve them electronically and use the website to help decrypt. This makes it possible to work with longer, more interesting messages. As in most of the ciphers on the site, students are asked to encrypt or decrypt the first few letters of a message themselves. When they have proved to the computer that they understand how to encrypt or decrypt, the computer will do the rest of the work for them.

Chapter 8

Cracking Vigenère Ciphers When You Know the Key Length

Summary

The Cryptokids examine their Vigenère messages to find patterns that will help them crack other Vigenère messages. They observe that, when they know the key length, they can crack a message by dividing it into parts and cracking each part separately as Caesar ciphers. As a class activity, students work together to finish decrypting parts of a long message that the Cryptokids began.

Math Content

tallying letters to find the most common letters
combining data from several problems to solve a larger problem

Materials

cipher wheels, one per student
one transparency of "Class Letter Frequencies" (page in *Blackline Masters*), or a similar table drawn on the board or chart paper

Teaching

In the Class Activity of this chapter, the class will work together to decrypt "the girls' message." We suggest that you divide up the work of cracking the message so that each group decrypts a few lines and then shares their results with the class. Students who work faster than others can do more than their assigned lines if they want to, but 3–4 lines per group is plenty and will give the slower workers the satisfaction of contributing to the class solution. When everyone is finished with at least their assigned lines, ask groups to take turns reading their lines aloud until the entire message is revealed.

The girls' message uses four wheels. Cracking it alone would take a long time, but the activity is designed so that there is not a lot of data collection. The decrypting for the first wheel is done already in the text. The data for the second wheel is collected and displayed in a table (text page 72) so students can use it to decrypt. The class will need to collect data for the third wheel, as described below. After that, the fourth wheel can be guessed without collecting more data.

To collect data for the third wheel, each group only counts letters in their assigned lines. They combine their data with the rest of the class to get the frequencies for the whole message. This is similar to the way the class combined data to make a class frequency table for English text in Chapter 5. Students count **A**s, **B**s, **C**s, and so on, in their assigned lines and record their results in their Frequency in Your Assigned Lines table on workbook page W38. They then enter their results in a Class Letter Frequencies table that you provide on the overhead, board, or chart paper. After all groups enter their data, each group adds a few rows of the table and records the row sums in the class table. Students then record these totals in their Class Total table on workbook page W38.

Take a moment to be sure that you understand how the work is divided up before the class begins work on the message. This will help the activity run smoothly. You will want to decide in advance which lines each group will work on and be familiar with the tables used in the group data collection for the third wheel (workbook page W38).

You will notice that the Vigenère messages that we present in this chapter are longer than most of the other messages with which students have worked. If the messages are too short, there won't be enough data for each wheel for frequency analysis to be useful.

Website

There is a Vigenère Cracking Tool on the website that helps students crack Vigenère ciphers. It includes both the case in which the user knows the key length and the case in which the key length is unknown (discussed in Chapter 10). After students have cracked the problems in the text by hand, we encourage you to have them use this feature of the site. The computer does a lot of the tedious work, and the students are freed to think.

Chapter 9

Factoring

Summary

This chapter provides the opportunity for students to learn or review methods for finding prime factorizations of numbers and finding common factors. These skills will be needed to crack the Vigenère cipher in the next chapter.

Math Content

finding prime factorizations
divisibility
exponents
finding common factors and greatest common factors

Key Vocabulary

factor
multiple
prime number
composite number
prime factorization
factor tree
divisible
exponent
common factor
greatest common factor

Materials

calculators, one per student

Connections

life cycles of cicadas

Teaching

This chapter is not about cryptography. It serves as a review of or an introduction to definitions and methods for factoring and finding common factors. Common factors will be used in the next chapter to crack the Vigenère cipher.

In this chapter, students factor larger numbers than are typically handled in middle school. This is because factoring large numbers is useful in cryptography, particularly in modern-day ciphers. By using divisibility rules, students can factor the numbers in this chapter without much difficulty.

Prime numbers are investigated in more depth in Chapter 16. In that chapter, students explore shortcuts for testing whether a number is prime. They use the Sieve of Eratosthenes as a method for finding all prime numbers within a given interval, and they explore the question of how many primes there are, concluding that there are infinitely many prime numbers. Prime numbers are used in the modern-day RSA cipher of Chapters 18 and 20.

Related Topics

Probably the most common application of common factors in the middle-school curriculum is to reduce fractions. This unit provides two other applications. The “Do You Know?” of this chapter presents a biological application involving the life cycles of cicadas. The next chapter uses common factors to help crack Vigenère messages.

Website

The Cryptoclub website has tools for finding the prime factorization of a number. It also has a program that will help build factor trees.

Chapter 10

Using Common Factors to Crack Vigenère Ciphers

Summary

Students look for patterns in Vigenère messages that will help figure out key lengths. They observe that, when strings of letters repeat in a message, the key length is usually a common factor of the distances between repetitions. They look for strings of letters that repeat in Grandfather's message, find common factors of the distances between them, and guess the key length. They use this to crack Grandfather's message and discover that he had found silver.

Math Content

common factors
finding repeated patterns
factoring numbers into prime factors
tallying
combining data from several problems to solve a larger problem

Materials

cipher wheels, one per student
Optional: "Patterns in the Girls' Message" (page in *Blackline Masters*), one copy per student or one transparency

Connections

one-time pad
VENONA program
spies during the Cold War

Opener

In this chapter, characters in the story examine messages and find a pattern that helps figure out key lengths. Before reading about the pattern in the book, your students should try to find it themselves. Ask them to examine the girls' message and answer the questions on a copy or transparency of "Patterns in the Girls' Message." (Alternatively, they can examine their decrypted girls' message on workbook page W36.) This can be assigned as homework or an opening activity for students to think about before the lesson.

In Problem 1 of "Patterns in the Girls' Message," students find occurrences of **the** in the message. They are in lines 1, 2 (twice), 4, 6, 8, and 10 (twice). (Line 10 appears on workbook page W36 but not on the "Patterns in the Girls' Message" page.)

Problem 2 asks why **the** is not always encrypted the same way. This is because the keyword **DIME** lines up differently above different occurrences of **the**. For example, when the letters **DIM** of the keyword are above **the**, then **the** is encrypted as **WPQ** (lines 1 and 2)**.** When **EDI** is above **the**, then **the** is encrypted as **XKM** (lines 4 and 10). When **IME** is above **the**, we get **BTI** (lines 6, 8, and 10). (Note that the workbook page W36 shows wheel numbers rather than keyword letters, but the answer is similar: when the numbers 1, 2, 3, and 4 line up differently below different occurrences, the letters are encrypted differently.)

Problem 3 asks for a pattern to tell when different occurrences of **the** are encrypted the same. This happens when the keyword lines up the same above the letters. This only happens when the keyword fits a whole number of times between occurrences of **the**, which happens when the distance between occurrences is a multiple of the key length. We don't expect that all students will reach this conclusion the first time they think about it. But, after thinking through this opening example, they will be ready to read how the characters in the book reasoned about a similar problem.

Teaching

Ask students to look for repeated strings in the boys' message in the picture on text page 84. A few strings are already underlined. Then, ask them to read the first few pages of the chapter. They can take turns reading, playing the roles of the characters in the story. The main conclusion of this part is that the key length is usually a factor of the distance between repeated occurrences of letter strings.

In Problems 1 and 2, students examine messages from the journal of Lewis and Clark. They practice finding distances between repeated strings of letters and investigate the relationship between the distance between repeated strings, the length of the keyword, and the way the keyword lines up above repeated strings. Problem 3 confirms that the key length is usually a factor of the distances.

In Problem 4 they examine repeated strings in Grandfather's message, and in Problem 5 they decrypt his message. You can assign each group a few lines to decrypt, encouraging them to do more if time permits. Then, have them take turns reading the lines aloud to reveal the decrypted message. This way, everyone contributes. The faster workers often choose to do more than their assigned lines instead of waiting to hear the full message, and the slower workers feel that they have accomplished their assigned work without falling behind.

In Problems 6–8, students look for common factors to guess key lengths. There is no need to decrypt these messages, since it is Grandfather's message each time.

In Problem 9 they put together everything they have learned and crack a message without hints. There are many steps involved, so students should feel proud when they finish. To save time, you can have students divide up the work of collecting data. They can share information about distances between repeated strings (Problem 9a in the workbook). In Problem 9b, they conclude the key length is probably four. This tells them they need four wheels. You can divide the class into four groups and ask each group to collect frequency data for one of the wheels and share it with the class. Students use this information to decrypt the message. You can ask each group to do a few lines of the message and report to the class, or they can divide up the work within their group if they prefer.

Website

One difficulty in working with Vigenère ciphers is that the messages need to be fairly long in order for useful patterns to emerge. Thus, we encourage you and your students to use the Cryptoclub website to encrypt and decrypt messages. Working with messages on the website will help students get the big picture of how to crack a Vigenère cipher, without getting too bogged down in data collection.

If you make messages for your students to crack, you should try to have at least 30 letters per wheel in your messages—longer is better—if you want the data to be helpful for cracking. (Of course, if you really intended to send messages that would be difficult to crack, you would want to make short messages or use several wheels to make frequency analysis of little use.)

Unit 4

Modular (Clock) Arithmetic

In this chapter, students learn to use the notation and terminology of modular arithmetic, which make it easier to discuss cryptography. Students used modular arithmetic informally in Unit 1, when they added to encrypt number messages. They worked with the numbers from 0 to 25 and used the term *equivalent* to describe numbers that wrapped around to the same place on a circle. In this unit they extend this concept to larger numbers and circles of different sizes.

Although the notation of modular arithmetic is not a standard part of the middle-grade curriculum, the concepts and calculations involve division with remainder, which is a middle-grade topic. As students explore modular arithmetic and its applications, they strengthen their understanding of and their ability to compute and solve problems involving remainders.

In Chapter 11, we begin with a setting that is familiar to students—time—and include several problems about elapsed time. We use both 12-hour and 24-hour clocks. Then, clocks of different sizes are considered, and the basic terminology of modular arithmetic is introduced.

In Chapter 12, students explore ways to use a calculator to find remainders. They apply modular arithmetic to cryptography and use it to solve calendar problems.

Chapter 11

Introduction to Modular Arithmetic

Summary

Students solve problems that involve adding and subtracting hours on clocks. The 24-hour clock is introduced and arithmetic problems on this type of clock are solved. Then, the notion of arithmetic on a clock is generalized to clocks of any size, and the terminology of modular arithmetic is introduced.

Math Content

elapsed time
clock arithmetic
24-hour time (military time)
modular arithmetic
division with remainder

Key Vocabulary

24-hour clock
modular arithmetic
equivalent mod *n*
congruent mod *n*
reduce mod *n*

Materials

calculators, one per student

Connections

World War I
Zimmermann telegram

Teaching

Modular arithmetic is useful in situations that involve cycles. Although some of the terminology of modular arithmetic is new to most students, the concepts are familiar, since they come up naturally when working with clocks and calendars.

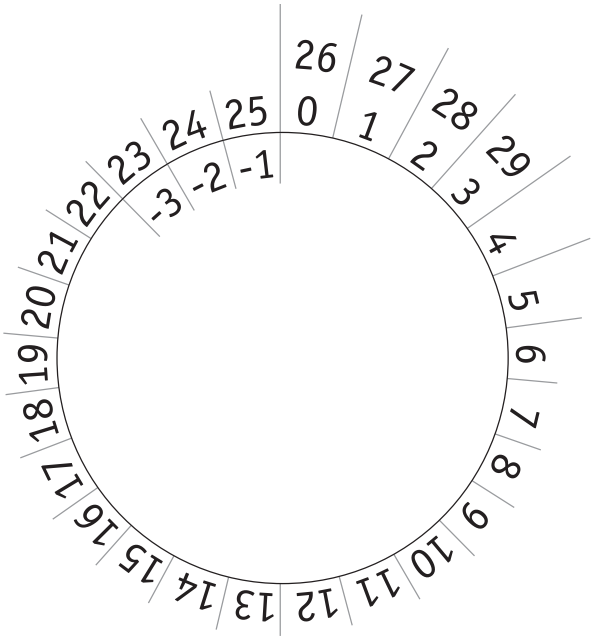
The chapter begins with problems that involve adding and subtracting hours on a clock. These are everyday problems, but students will probably have different ways to solve them. As you discuss answers to the problems, ask students to describe the methods that they used.

Some students will solve a problem like 8 + 11 (on a 12-hour clock) by starting at 8 and counting 11 more hours, pointing to each hour on a picture of a clock until they reach 7. Others might compute 8 + 11 = 19 and then subtract 12 to get 7. Others might begin at 8, and add 4 to get 12. This leaves 11 – 4 = 7 hours after 12, so again the answer is 7. Still others might reason that adding 11 hours is one less than adding 12 hours and from this conclude that the answer is one less than 8, which is 7. Some students who solve clock problems by pointing to each hour on a clock or counting on their fingers are surprised to discover that they can often solve them more easily with arithmetic than with direct counting.

After working with the 12-hour and 24-hour clock, we introduce the terminology of modular arithmetic, which is useful on any size clock. In modular arithmetic, we think of numbers wrapping around a circle and identify numbers as "equivalent" if they wrap to the same position.

For example, on a 12-hour clock, 1 o'clock and 13 o'clock are equivalent.

Remind students that they worked with the notion of equivalent numbers in Chapter 2, where they wrapped 0, 1, ..., 25 around a circle. In that chapter, 26 was equivalent to 0, 27 was equivalent to 1, and so on, as in the figure below. Explain that, in this chapter, we will use the same idea but with circles of different sizes.



The symbol "≡" for equivalence is introduced in this chapter. We want students to see the proper use of this symbol, but it is acceptable for them to use the equal sign if they prefer.

When we work mod n, we often use only the numbers from 0 to $n - 1$. If another number arises in our calculations, we replace it with the number between 0 and $n - 1$ that is equivalent to it mod n. This is called "reducing mod n," and it is the same as replacing with the remainder after division by n. Ask students how they would find the remainder. Then, have them read the methods used by the characters in the book. Problems 18–24 provide practice with reducing small numbers. Students practice reducing larger numbers in the next chapter.

The notation for equivalence and for reducing both use the term "mod," but in slightly different ways. For example, to indicate that 79 and 27 are equivalent mod 26, we write

$$79 \equiv 27 \pmod{26}.$$

To indicate that we want to reduce 79 or find the remainder of 79 ÷ 26, we write the expression

$$79 \bmod 26.$$

Such an expression can be evaluated, and we use the equal sign (not the equivalence sign) to show the answer:

$$27 \bmod 26 = 1.$$

To indicate equivalence, we use the equivalent sign "≡" and parentheses. To indicate remainder, we use the equal sign and no parentheses. Although there is a difference between these uses of the mod notation, it need not be emphasized. The equivalent sign isn't used much in this chapter, but it will appear more in later chapters.

Related Topics

The "Do You Know?" of this chapter is about the Zimmermann telegram, which precipitated the entrance of the United States into World War I. This topic can be discussed at any time, since it is not directly related to modular arithmetic.

Chapter 12

Applications of Modular Arithmetic

Summary

Students continue to work with modular arithmetic. The multiplicative cipher is introduced, which involves reducing larger numbers than in the previous chapter. Students explore ways to change decimal remainders displayed on their calculators into whole number remainders, and they solve calendar problems using modular arithmetic, including problems with leap year. International Standard Book Numbers (ISBNs) are introduced in this chapter's "Do You Know?"

Math Content

multiplication and division
several ways to find remainders
changing decimal remainders to whole number remainders
problem solving with remainders

Key Vocabulary

leap year
ISBN
check digit

Materials

calculators, one per student

Connections

ISBN numbers

Teaching

The chapter begins by reminding students that they have used modular arithmetic in ciphers (Chapter 2) without using that terminology. Problem 2 introduces multiplicative ciphers, which involve reducing larger numbers than the additive (shift) ciphers of Chapter 2 did.

The characters in the story use several different methods to reduce 154 mod 26. Before reading about the methods in the book, ask students to solve the problem. Then, have them describe their methods to the class. After they have discussed their own methods, they can look over the methods in the book and see whether theirs are among them.

Ask students how they would use a calculator to find a remainder. Some calculators are sophisticated enough to calculate whole-number remainders, but others are not. If a calculator divides and expresses the quotient with a decimal remainder, it is an interesting problem to convert the decimal remainder to a whole-number remainder. Ask students to solve a problem like 154 mod 26 with a calculator, and discuss their solutions before they read the methods in the book.

Encourage students to look for and use shortcuts when working with modular arithmetic, such as Tim's shortcut for multiplying mod 26 on text page 119. Large numbers can often be reduced to smaller numbers, making mental arithmetic a quicker way to solve some problems than using a calculator. For example, since $25 \equiv -1$ (mod

26), multiplying by 25 then reducing is the same as multiplying by –1 then reducing. Most would agree the latter is easier. Similarly, multiplying by 24 then reducing is the same as multiplying by –2 then reducing. This shortcut is suggested, but students can use the method with which they are most comfortable.

Students may have a variety of ways to solve the calendar problems. Ask them to describe their solutions to the class.

Related Topics

The "Do You Know?" in this chapter describes the system of International Standard Book Numbers (ISBNs). Ask students to check the ISBNs on a few other books and verify that the sum of the check equation is a multiple of 11. Then, show them a few numbers, and ask them to decide whether they are valid ISBNs or not.

Students might like to investigate and report on other non-secret codes and their check digit schemes. For example, the Universal Product Code (UPC) is a bar code that appears on most consumer products. It also has a check digit scheme.

Website

The Cryptoclub website has a calculator that can reduce numbers in modular arithmetic. This is useful if you are doing several calculations. Students can also use it to check calculations that they have done by hand or with a handheld calculator.

Unit 5

Multiplicative and Affine Ciphers

After using addition to encrypt in Chapter 2, it is natural to ask whether we can make a cipher using multiplication. It turns out that multiplying by some numbers does make a reasonable cipher, but multiplying by others does not. For example, 2 is not a good multiplier, since multiplying by 2 gives only even numbers and encrypts some numbers the same.

This unit spans a wide spectrum of mathematics levels from Grades 5–8. Chapter 13 is suitable for all levels, while the skills used to crack the ciphers at the end of Chapter 15 are more advanced and include solving algebraic equations.

In Chapter 13, students complete multiplication cipher tables and look for patterns to predict which numbers make good keys (multipliers) for multiplicative ciphers. They decrypt using their tables.

Chapter 14 introduces modular inverses and uses them to decrypt multiplicative ciphers. It is natural to assume at first that you can use division to decrypt multiplicative ciphers. But, you can't always divide in modular arithmetic since you might not get a whole number. In regular arithmetic, multiplying by the inverse of a number is the same as dividing by that number. In Chapter 14, we extend the idea of an inverse to modular arithmetic. We then multiply by modular inverses to decrypt.

At the end of Chapter 14, students apply their skills to crack multiplicative ciphers when they don't know the key. This involves looking for clues in the message and representing them in algebraic equations. The equations are solved in modular arithmetic similar to the way they would be solved in regular arithmetic. The context of cryptography helps students know that they are on the right track mathematically as a message that makes sense is revealed.

In Chapter 15 the affine cipher is introduced, which combines addition and multiplication. The encryption formula for an affine cipher is like the formula for a straight line: $Y = (mx + b) \bmod 26$. Decrypting is straightforward when the key is known. When the key is not known, it is an interesting challenge to crack an affine cipher. Algebra students who have learned to solve systems of two equations in two unknowns are able to apply similar methods to crack affine ciphers.

The "Do You Know?" sections of this unit are about passwords, the German Enigma cipher of World War II, and the biblical Atbash cipher, which is a substitution cipher. They are not directly related to the ciphers of the chapter, so students can read them at any time.

Chapter 13

Multiplicative Ciphers

Summary

Students explore multiplicative ciphers. They compute cipher tables using different keys (multipliers) and discover that not all numbers work well as keys—some keys encrypt some letters the same. In a class activity, students share the work of testing each number from 2 to 25 to see which make good keys. They conclude that the good keys are the numbers that have no factors in common with 26, that is, those that are relatively prime to 26. The even numbers and 13 have factors in common with 26, and they do not make good keys. Students compute cipher tables for several keys and use these tables to decrypt quotations.

Math Content

multiplication (up to 2-digit by 2-digit numbers)
reducing mod *n*
division with remainder
factoring
relatively prime numbers

Key Vocabulary

good key
relatively prime

Materials

calculators

Connections

alphabets of different languages
passwords

Teaching

In the first part of the chapter, students compute tables for various multiplicative ciphers. They can do this by multiplying each plaintext number by the key and then reducing mod 26, or they can use patterns such as *skip counting* to fill out the tables, subtracting 26 when necessary to keep the answer in the 0 to 25 range. For example, to multiply by 5 they would count: 5, 10 15, 20, 25, 30. Since 30 is out of range, they subtract 26 to get 4 and then continue on counting by 5s: 4, 9, 14, and so on.

After students have completed Problems 1–4, they are ready to do the class activity, which explores which numbers are good keys. They will work in small groups or pairs, with each group checking a few numbers. Groups should work on different numbers so that they can pool their results and find a pattern at the end. You can assign each group their numbers or let them choose their own from a list of those not yet chosen. As faster groups finish, ask them to work on numbers not yet chosen until the class has tested all numbers up to 25.

Groups should make multiplicative cipher tables using their assigned numbers as keys to decide whether their numbers make good keys. If every number from 0 to 25 appears once in the product row, the key is good. If there are repeated numbers, the key is bad because it would encrypt some letters the same way. The numbers 0, 1, 2, 3, 5, and 13 don't need to be assigned since 0 and 1 are obvious and the tables for 2, 3, 5, and 13 have already been computed in Problems 1–4.

To keep products low as they multiply by large keys, remind students that they can multiply by equivalent smaller numbers. For example, 25 is equivalent to –1. It is much easier to multiply by –1 than by 25. Using this, they can compute that $25 \times 8 \equiv -1 \times 8 \equiv -8 \equiv 18 \pmod{26}$. This idea was introduced as a shortcut in the previous chapter (text page 119) and is also used in Problem 8d of this chapter.

Put the numbers 2–25 on the board, and ask groups to write "yes" or "no" beside their assigned numbers as they decide whether the numbers are good keys, as in the table below. As the results are posted, ask students to look for a pattern. Students will often guess that "even numbers are bad, and odd numbers are good." Point out that 13 is an odd number that is bad, so that guess isn't quite correct.

Number	Good Key?
2	no
3	yes
4	no
5	yes
6	no
etc.	etc.

The correct pattern is that the good keys are the numbers that are relatively prime to 26, the size of the alphabet. For languages that have a different size alphabet, the good keys will be different.

Problem 7 asks students to investigate alphabets of different languages to determine which numbers are good keys for those languages. Russian, Korean, and Arabic are explored in this problem. Ask students whether their families speak other languages, and then ask how many letters are in the alphabets of those languages. Ask students to find good keys for any languages that have a different number of letters than those investigated so far.

The chapter ends with several encrypted quotations. Students can decrypt these using their multiplicative cipher tables, reading from bottom to top. Although the quotations were encrypted by multiplying, it might surprise students that not all letters can be decrypted by dividing. That is because division doesn't always give a whole number. The next chapter will introduce modular inverses, which will be used to decrypt messages instead of using the tables.

Related Topics

The "Do You Know?" of this chapter is about computer passwords. You might ask the class to make a class list of places where they have needed to use passwords.

Website

There is a multiplicative cipher program on the website that can encrypt using a key you choose. The cipher program decrypts using modular inverses, which will be discussed in the next chapter.

Chapter 14

Using Inverses to Decrypt

Summary

In this chapter students first review multiplicative inverses in regular arithmetic. Then, they explore inverses in modular arithmetic. Although modular inverses are not as easy to find, they share the important property of all inverses: Multiplying by a number and then multiplying by its inverse gives you back what you started with. This makes inverses useful for decrypting multiplicative ciphers. After decrypting messages using inverses, students crack messages when the key is unknown. This involves using algebra to solve equations obtained from clues in the messages.

Math Content

multiplicative inverses in regular arithmetic and in modular arithmetic
using inverses to solve equations
factoring
reciprocals
relatively prime numbers

Key Vocabulary

multiplicative inverse
reciprocal
modular inverse

Materials

calculators, one per student

Connections

World War II
German Enigma Cipher

Teaching

Begin by asking students to think about how they would decrypt multiplicative ciphers. Remind them that when they added to encrypt (in Chapter 2), they could subtract to decrypt. Students will probably suggest that when they multiply to encrypt, they can divide to decrypt. But this is not always possible in modular arithmetic, since we only use whole numbers.

Ask students to try out the hypothesis that division can be used to decrypt. They can look at some of the cipher tables that they computed in the previous chapter or at the times-3 cipher table on text page 137. In the times-3 cipher, for example, letters at the beginning of the alphabet can be encrypted and decrypted with multiplication and division. But, letters after **j** in the alphabet are encrypted with numbers that are not divisible by 3, so you can't divide to get back what you started with.

The characters in the story try a few examples and conclude that "there is more to think about." This introduces a review about inverses in regular arithmetic.

The reciprocal of a number—the fraction obtained by writing 1 divided by the number—is probably the first inverse that students encounter in their mathematical studies. However the concept of inverse—something that, when multiplied by the original, yields the identity (which in this case is 1)—comes up in many other places in mathematics. The next inverse about which they will probably learn in their mathematical studies is the inverse of a matrix. Seeing the concept of inverse used in different situations helps students solidify their understanding of the meaning of inverse and the way it is used to solve problems.

You may want to create and post a class list of modular inverses as students discover inverse pairs. This way, they can refer to it as they decrypt, for example, during Cipher Tag. This list will also be useful when they decrypt affine ciphers in the next chapter.

Here is a list of pairs of numbers that are inverses mod 26:

1 and 1
3 and 9
5 and 21
7 and 15
11 and 19
17 and 23
25 and 25

Not all numbers have inverses. Those that do are the odd numbers except 13—these are the numbers that are relatively prime to 26. These are the same numbers found to be good keys in the previous chapter. That makes sense—it means that any message encrypted by multiplying by a good key can be decrypted (by multiplying by the inverse of the key).

At the end of the chapter, students crack messages when they do not know the keys. Since a multiplicative cipher is a type of substitution cipher, some letters can be guessed using frequency analysis. But, if the message is short, this probably won't give enough information to guess all the letters. However, knowing a few letters helps to write equations that can be solved using algebra and inverses. This activity combines many skills, and students will feel a sense of accomplishment when they complete it.

In Chapter 19, we discuss methods for finding inverses in more detail and consider inverses in different mods, not just mod 26.

Related Topics

Students should be able to find a lot of information written about the German Enigma Cipher discussed in the "Do You Know?" of this chapter. A website that can get them started is the National Security Agency's site, http://www.nsa.gov.

Website

The calculator on the Cryptoclub website has a button for computing modular inverses.

Chapter 15

Affine Ciphers

Summary

Students combine addition and multiplication to make ciphers. First, they encrypt and decrypt when the affine key is known. Then, they crack ciphers with unknown keys by using algebra to solve systems of linear equations.

Math Content

multiplication
reducing mod 26
using inverses
linear equations
solving two equations in two unknowns (optional)

Key Vocabulary

affine cipher
(m, b)-affine cipher
key

Materials

calculators, one per student

Connections

the biblical cipher Atbash

Teaching

There are several places where the text tells how to solve certain problems, but we suggest that, before reading together the book's solutions, you first ask your students to think about how to solve the problems themselves. For example,

- After discussing together the encryption steps for encrypting with an (m, b)-affine cipher—multiply by m and add b, then reduce mod 26—ask students to suggest a mathematical formula that matches these steps, before the book tells that this formula is $Y = (mx + b) \bmod 26$.
- When introducing the idea of decrypting, ask students how they would decrypt a message that had been encrypted with an affine cipher, before the book tells them to subtract b and then multiply by the mod 26 inverse of m.
- When reading how Peter and Tim break the girls' cipher by using the clue about **2 PM**, ask the students if they can find any clues in the girls' message that would help them break the cipher. Do this before reading what Peter and Tim did.

In the last section of the chapter, the characters in the story crack a message when they don't know the key. If your students have solved linear equations in math class, then they have the background needed for this section. If not, you can make the section optional and encourage them to crack the messages in Problems 9–11 as a challenge. Here are a few tips for cracking affine ciphers:

- If your students have studied the topic of solving two linear equations in two unknowns, they may already know at least three methods for solving such systems of equations: graphing, substitution, and subtracting a multiple of one equation from another. The subtraction method works well for finding m and b to crack affine ciphers. Simply subtracting one equation from the other will always eliminate b because the constant term in each equation is always b.
- In the example presented in the book (text pages 148–149), the problem reduces to solving the equivalence $15 \equiv 3m \pmod{26}$. The solution to this is $m = 5$, which is the same in both modular arithmetic as it is in regular arithmetic. This problem is solved in the book by multiplying both sides by 9, which is the inverse of 3. It could also have been solved by dividing both sides by 3, but division will not always work to solve equivalences. For example, an equivalence such as $4 \equiv 3m \pmod{26}$ cannot be solved by dividing both sides by 3, since 4/3 is not a whole number. Multiplying by the modular inverse will always work.
- In cracking the messages in the story, enough was known about the messages that certain letters could be correctly guessed. In one message, the boys figured out that **2 ZK** was probably the starting time of the party and that, therefore, **ZK** was probably the encryption of **PM**. In another message, the words at the end were assumed to be names, and that helped the girls to know a few letters. Another way to get a few letters of a message is to use frequency analysis. After you know a few letters, you can use them to find equivalences and then solve the equivalences to get a formula for the rest of the letters.
- If you or other students prepare affine messages to challenge each other, the messages should contain a few words that cannot be guessed by frequency analysis. For example, if a message includes words that can be decrypted more than one way, such as Tim and Tom, students have to figure out the key to be sure which is the correct decryption.

Cracking affine ciphers when the key is not known is a challenge that uses many mathematics skills. You can suggest that student groups prepare messages and place them in the Message Center for other groups to crack. Students who succeed at cracking the extra messages should feel proud of their achievement.

Related Topics

The “Do You Know?” of this chapter is about the Atbash cipher, which is a form of substitution cipher that occurs in the Hebrew bible.

Website

The Cryptoclub website has a program to help encrypt and decrypt affine ciphers when the key is known. After students correctly encrypt or decrypt the first few letters of a message, the machine will do the rest.

Unit 6

Math for Modern Cryptography

In the next unit, we examine RSA, which is a powerful modern-day cipher. RSA involves raising a number to a large power and reducing in modular arithmetic. Encrypting with RSA involves large prime numbers. This unit explores primes and powers in preparation for studying RSA. However, you can teach this unit as part of a number theory unit whether or not you continue on to Unit 7.

Chapter 16 focuses on finding large prime numbers. It is hard to recognize whether a number is prime—if it is big and odd, students often assume it is prime. They can test other numbers to see whether they are factors of the number, but how do they know when they have tested enough? If they don't find factors among those they test, how can they be sure there aren't any among those they haven't tested? This chapter investigates these questions and develops systematic ways to find prime numbers. It also examines some of the research questions mathematicians have explored about prime numbers.

Chapter 17 involves exponents in modular arithmetic. It explores the problem of working with large numbers on a calculator. When we raise a number to a power, the answer can be too large for the calculator to display in standard notation. The calculator changes to scientific notation, but this involves rounding the number, making modular arithmetic impossible. To get around this problem, we can raise the number to smaller powers first and reduce before the answer gets too large for the calculator. Exploring the questions in this unit helps students to develop flexibility in working with exponents.

Chapter 16

Finding Prime Numbers

Summary

In this chapter, we investigate shortcuts for testing whether a number is prime. The Sieve of Eratosthenes is explored as a method for finding all prime numbers within a chosen range. The question of whether there is a largest prime number is discussed, with the conclusion that there are infinitely many prime numbers. Finally, special numbers are investigated: twin primes, Mersenne numbers, and Sophie Germaine primes, which have lead to the discovery of very large prime numbers.

Math Content

factors, multiples, primes, and composites
efficient ways to test for primes
Sieve of Eratosthenes
counting prime numbers
variables and formulas
special primes: twin, Mersenne, and Sophie Germaine primes
Goldbach Conjecture
square root
googol

Key Vocabulary

Sieve of Eratosthenes
twin primes
Mersenne numbers
Sophie Germaine prime
googol
Goldbach Conjecture

Materials

calculators, one per student

Connections

Great Internet Mersenne Prime Search (GIMPS)
mathematics research

Opener

Begin by putting a large number on the board and asking whether it is prime. A number such as 1517 is a good choice. Since 1517 = 37 × 41, its factors won't be easily guessed and it will "look prime" to many students. Ask students to give reasons for their answers. If anyone was able to factor this number, ask them how they did it and what other numbers they checked before finding the factors. Many students will probably give up before reaching a conclusion. At this point, they will be interested in learning efficient ways to test whether a number is prime. Tell them you will return to 1517 later.

Teaching

Students often think that if a number is big and unfamiliar looking, it must be prime. The task of checking whether it has any factors besides itself and one seems at first to be overwhelming. But, to check whether a number has any other factors, they only have to test the prime numbers less than the number. And, in fact, they only have to check the primes less than the square root of the number. This means that you can test whether a number like 1517 is prime by testing only the prime numbers less than 39 to see whether they divide 1517 evenly—there are only 12. By efficiently checking for divisors, students will be able to find that many numbers that "look prime" are not.

You can introduce these ideas by having students take turns reading the dialogue in the text as the characters in the story discover the shortcuts for testing for primes. Or, you can lead a classroom discussion in which the class figures out those shortcuts themselves, using the conversation of the Cryptokids as a model.

To lead a conversation similar to that in the book, ask students whether 149 is prime. It is, but ask students how they can be sure. Ask how they can check in a systematic way. They will probably suggest trying 2, 3, 4, … and so on to look for divisors of 149. Let the class do this together:

- First check 2. It does not divide 149.
- Check 3. It does not divide 149.
- Begin to check 4, but encourage students to conclude that they don't need to check 4 since a number divisible by 4 would already have been found to be divisible by 2.
- Encourage students to conclude that they only need to check prime numbers.
- Encourage them to conclude that they only need to check up to the square root of 149 (see Jenny's reasoning on text page 157).

To reinforce these ideas, ask students to take turns reading the roles of the characters in the book to see how the Cryptokids discuss shortcuts for testing for primes.

After exploring the shortcuts for prime testing, you can return to the number from the opener, 1517, and systematically test whether it is prime. Students will be able to factor it after 12 divisions, since its smallest factor, 37, is the 12th largest prime number.

The next topic covered in the text is the Sieve of Eratosthenes. This is a method for efficiently generating a list of all primes in a chosen interval. This method again uses the idea that, when testing for primes, they only need to check up to the square root.

The chapter continues with a discussion of the number of primes. Before reading the conversation in the book, ask students how many primes they think there are. Is there a largest prime or are there infinitely many primes? If there is a largest prime, what is it? How do they know there are not more? If there are infinitely many primes, how do they know that? After hearing their ideas, ask them to take turns reading the roles of Peter and Lilah as they talk about these questions.

The final section is about a few special types of prime numbers that are expressed using formulas. Making lists of some of these numbers gives students the opportunity to work with formulas in which the variable *n* has different values, instead of just being a place holder for a single number.

Problem 10 challenges students to find a large prime number. It is up to them to decide how large they want it to be. Ask students to explain how they know the number is prime. Remind them that just because they can't find divisors, that doesn't mean there aren't any. They should test primes up to the square root of their number to be sure. You can use the prime tester on the Cryptoclub website to quickly confirm that the proposed answers are prime.

Related Topics

This chapter is an opportunity for students to see that there are still unanswered questions in mathematics. No one knows whether there are infinitely many twin primes or infinitely many Mersenne primes. No one knows whether the Goldbach Conjecture is true or false. Students often view mathematics as a subject in which all the answers are already known, and they are surprised that there are mathematicians doing research today to further develop the field.

Some mathematics research problems are too hard to explain in simple terms. But some, such as the Goldbach Conjecture, are easy to state so that students can understand them. Learning about such unsolved problems can be very motivating to some students. A very well-known example is Fermat's Last Theorem, which was solved in 1993 by a mathematician, Andrew Wiles, who had first heard about it when he was ten years old. He made the decision at that time to learn enough mathematics to solve the problem, and 30 years later he succeeded.

You can ask students to report on other unsolved problems in mathematics.

The "Do You Know?" of this chapter is about the Great Internet Mersenne Prime Search (GIMPS). This project is responsible for discovering several prime numbers that were the largest-known primes at the time they were discovered. The current largest-known prime keeps changing. You can ask students to research and report on the largest-known prime(s) that have been discovered since the Cryptoclub book went to press.

If you think your class might like to participate in the GIMPS project to search for the next largest prime, we recommend the article listed below, which describes a fifth-grade class's participation.

Website

After students have used the Sieve of Eratosthenes by hand to find prime numbers, they can go to the Cryptoclub website to use the Sieve of Eratosthenes program to work with larger numbers. The Math Tools section of the site will also tell whether a given number is prime or not.

Recommended Reading

Jeffrey Wanko and Christine Venable. "Investigating Prime Numbers and the Great Internet Mersenne Prime Search." *Mathematics Teaching in the Middle School* 8 (October 2002): 70–76.

This very interesting article describes classroom activities for exploring large prime numbers. One activity for helping students understand large numbers is to write out a many-digit number on index cards, with three zeros per card and then place the cards together end-to-end to represent the number. Students in the article placed cards in the hallway and were only able to fit 1440 digits before running out of room—the largest prime number known at the time had 2,000,000 digits! This article also describes one class's participation in current mathematical research by signing up for the Great Internet Mersenne Prime Search.

The Prince of Mathematics: Carl Friedrich Gauss, by M. B. W. Tent (A K Peters, Ltd., 2005).

This biography of Gauss is enjoyable reading for all ages, particularly intended to inspire young readers. It describes some of the mathematics problems Gauss solved as a child, as well as his achievements as an adult.

Chapter 17

Raising to Powers

Summary

Students raise numbers to powers and reduce in modular arithmetic. They discover that the exponent key on their calculators won't help because the answer is usually larger than the calculator can handle without rounding, which loses information needed to correctly reduce the answer. Students explore ways to avoid this round-off problem. They compute powers by repeatedly multiplying smaller numbers and reducing before the answers get too big. They use a method of repeated squaring to solve the problems with fewer multiplications. As they work to solve the problems, they reinforce their understanding of exponents and develop flexibility in calculations.

Math Content

scientific notation on calculators
exponents
computing powers by repeated squaring
modular arithmetic

Materials

calculators, one per student

Connections

passwords

Teaching

When a number is raised to a power and reduced in modular arithmetic, the answer is usually much larger than the final answer will be after it is reduced. Although the calculator can handle the final answer without problems, it doesn't have enough space to display the larger intermediate answers. It switches to scientific notation to display large numbers but, in the process, it rounds the numbers and loses information needed to reduce.

To introduce the issues of the chapter, ask students to compute 18^{23} mod 55 , the number Dan and Tim work with in the book. Discuss their calculations and the problems that occur before reading the book's account of Dan and Tim's calculations.

The students' first step probably will be to compute 18^{23} using calculators. Their calculators will use scientific notation to display the answer because it is too big to display in standard notation. Be sure that they understand how to convert the answer in their calculator window to a number in standard notation.

Next, ask them to reduce their answer mod 55. Do they notice that there is a problem doing this? When the calculator switched to scientific notation to display the large number, it had to round the number. But, the rounded number is an estimate of the original number, so reducing the rounded number won't give the same answer as reducing the original number.

Ask students to suggest a different way to solve this problem that avoids large numbers. Someone might suggest repeatedly multiplying by 18 and reducing after each multiplication so that the numbers don't get too big. If not, then you can suggest this. They will probably agree that computing18^{23} this way takes too many multiplications to do comfortably, so you can next introduce the method of repeated squaring.

In modular arithmetic, the usual methods for raising to powers either don't work on the calculator or are too time consuming. This chapter reminds us that it is good to develop a variety of ways to solve problems so that effective ways can be chosen when needed. Here is a summary of the main ideas of this chapter that help to solve the problems:

- Raising the numbers to small powers first and then reducing before the answers get too big avoids round-off error.
- When the exponent is a power of two, squaring is a quick way to compute big powers from smaller powers, e.g. $x^4 = (x^2)^2$; $x^8 = (x^4)^2$; $x^{16} = (x^8)^2$.
- When the exponent is not a power of two, powers can be computed by combining results for smaller powers of two: $x^{23} = x^{16} \times x^4 \times x^2 \times x^1$.

Related Topics

The "Do You Know?" of this chapter is a reminder to be careful with password use.

Website

The calculator on the Cryptoclub website can handle larger numbers than a handheld calculator without problems from round-off error. But, all calculators and computers have limits on the size of the numbers that they can handle and need alternative methods for numbers that exceed their limits.

Unit 7

Public-Key Cryptography

In the mid 1970s a new kind of cryptography was developed—public-key cryptography—which changed the way people could send messages. It allowed users to communicate without previously agreeing on a secret key. This chapter introduces the basic ideas of public-key cryptography and focuses on the RSA cipher, a powerful public-key cipher used for Internet security today.

RSA involves raising numbers to powers and reducing in modular arithmetic. It uses large prime numbers, and cracking it involves factoring large numbers. The security of RSA relies on the fact that large numbers are difficult to factor. The application of prime numbers and factoring to cryptography has created renewed interest in these topics and has spurred mathematics researchers to seek efficient ways to test for primality and to factor numbers.

Working with RSA is an opportunity for students to practice and expand what they know about prime numbers and factoring, work with exponents in a flexible way, and learn about some of the issues involved in modern-day cryptography.

Chapter 18 introduces public-key cryptography and describes the RSA cipher as an example. RSA uses modular inverses to compute its decryption key, so Chapter 19 revisits modular inverses and considers examples when the modulus is different from 26. In Chapter 20, the final chapter, students choose their own public and private RSA keys. RSA is slow to implement because it involves long calculations, so it is often combined with another cipher. In this chapter, students combine RSA with the Vigenère cipher, using the Vigenère cipher to encrypt the messages and RSA to encrypt the Vigenère key.

Chapter 18

The RSA Cryptosystem

Summary

Public-key cryptography is introduced, and the RSA cipher is described. Students encrypt and decrypt a few short messages with RSA. Small numbers are used so that the computations are manageable.

Math Content

prime numbers
modular inverses
raising numbers to powers and reducing in modular arithmetic
relatively prime numbers
factoring

Key Vocabulary

public-key system
RSA cipher
encryption key
public key
decryption key
private key

Materials

calculators, one per student

Connections

mathematics research: large prime numbers and factoring

Teaching

Introduce the idea of public-key cryptography by asking students how they would send a message to someone who didn't know in advance what key would be used. How would they let that person know the key? They couldn't just send it in another message—if the original message could be intercepted, the one with the key could be too. Public-key ciphers avoid the problem of how to send a key by eliminating the need to send it. This makes public-key ciphers fundamentally different from the ciphers about which they have learned so far.

Have the class read the story at the beginning of the chapter, which summarizes public-key cryptography and introduces the RSA cipher. RSA was the first public-key cipher developed, and it is still in use today.

The problems in this chapter only ask students to do a few calculations because the calculations with RSA can be unexpectedly long. For example, although encrypting with the key (55,7) used in this chapter is not difficult—raising to the seventh power can be done easily on a calculator—decrypting is more involved. Decrypting involves raising to the 23rd power, which usually requires special methods to avoid calculator round-off error, such as those from the previous chapter.

After students explore methods for finding inverses in Chapter 19, they will be ready to choose their own public and private RSA keys. They will choose their keys and send their own messages in Chapter 20.

Related Topics

It might surprise students to learn that computers cannot do everything. Some problems are too long to solve, even with a computer. Factoring and prime testing of large numbers are such problems. The quest for better cryptography techniques has spurred renewed interest in mathematical research of problems such as these. This chapter is an opportunity to remind students that new methods to solve mathematics problems continue to be discovered.

The "Do You Know?" of this chapter discusses the many uses of cryptography in today's world. Begin a class list of places students and their families notice cryptography being used in everyday transactions.

Website

The Cryptoclub website has a calculator that can raise numbers to powers and reduce in modular arithmetic, avoiding overflow problems. It can also find modular inverses.

Recommended Reading

The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptogrphy, by Simon Singh (Doubleday, 1999).

This book gives an interesting account of the development of cryptography through the ages, including the development of public-key cryptography.

Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age, by Steven Levy (Viking, 2001).

This book tells how a group of mathematicians and programmers went outside the normal government security channels to make strong encryption available for ordinary people. It gives a very interesting account of the struggle between the government's need for security and individual citizens' rights to privacy in the age of technology. The level of the book is for older readers.

Chapter 19

Revisiting Inverses in Modular Arithmetic

Summary

Students review what they learned in Chapter 14 about inverses. They explore ways to find inverses mod *n* for different values of *n*.

Math Content

reducing mod *n*
relatively prime
efficient trial and error methods to find inverses mod *n*

Key Vocabulary

inverse

Materials

calculators, one per student

Connections

Thomas Jefferson and James Madison

Teaching

In order to decrypt the RSA cipher, students will need to find the inverse of their encryption key. In this section, we present a few trial-and-error methods for finding modular inverses that will work for the relatively small numbers that students use here.

One benefit of finding modular inverses through these trial-and-error methods is that it solidifies students' understanding of what an inverse is. In fact, the task of finding a modular inverse is a multi-step problem that reinforces understanding of several concepts: divisibility, remainder, inverse, and relatively prime numbers. The goal of shortening the task, as Jenny and Evie do in the story, sharpens their understanding of the issues.

There is a method (the Extended Euclidean Algorithm) that can be used to compute inverses directly, but it is beyond the scope of this book. Motivated students could research this method and learn how to use it.

Related Topics

The "Do You Know?" of this chapter is an amusing anecdote about a message sent from Thomas Jefferson to James Madison a few years after the nation's founding. It reminds us that even great leaders can be forgetful.

Website

The trial-and-error method of finding modular inverses is cumbersome for large numbers. Students who use large numbers for their RSA keys can use the modular calculator on the Cryptoclub website to help find the inverses they need.

Chapter 20

Sending RSA Messages

Summary

In this chapter students choose RSA keys and set up a classroom public-key directory. Then, they combine the RSA and Vigenère ciphers to send messages. They use RSA to encrypt and decrypt keywords, which they use with the Vigenère cipher to encrypt and decrypt messages.

Math Content

exponents
modular inverses
reducing in modular arithmetic
raising numbers to powers

Materials

calculators, one per student
Vigenère square (inside cover) or cipher wheel, one per student

Connections

British discovery of public-key cryptography

Teaching

In this chapter students use the RSA cipher. First, they choose their public encryption keys and list them in a class directory so that they can send each other messages. They also find their corresponding private decryption keys, but they don't put them in the directory. It is a good idea for students to work with partners so they can check their calculations.

In the beginning, students should use small values for p and q in their keys so that the calculations are easier. After awhile, some students may realize that when p and q are small, then $n = p \times q$ is easy to factor and their decryption keys can be figured out by others. When they want to make keys that are harder to figure out, they can choose larger prime numbers with which to work.

The next step is to use RSA to encrypt and decrypt messages. One drawback of RSA is that the calculations can take a long time. For this reason, cryptographers sometimes combine ciphers, using a faster cipher to encrypt the message and RSA to encrypt a keyword for that cipher. That way they get the advantage of RSA—they don't need to worry about how to secretly get the keyword to the receiver—without the disadvantage of lengthy computing time. In this chapter, we combine RSA and the Vigenère cipher in this manner. Recall that the Vigenère cipher needs a keyword to tell you how to set the wheels. We use the Vigenère cipher to encrypt messages and RSA to encrypt the keyword. After students do the problems in the book, they can combine RSA with some of the other ciphers that they have learned.

The surprising thing about public-key ciphers such as RSA is that the keys can be listed in a directory for everyone to see. Using the classroom directory to send messages will help students understand this feature. To send a message to another group, students first encrypt it with their favorite cipher. Then, they look up the group's public key in the directory and encrypt that cipher's key or keyword using RSA and the group's public key. The message can be posted for all to see, but no one will know the keyword to decrypt unless they know the private RSA key.

Students who want to explore RSA more deeply can investigate other ways to assign letters to numbers. We have used the simple method of assigning **a** = 0, **b** = 1,…, and so on, but with this method, RSA is essentially a substitution cipher—it substitutes the values calculated by the RSA encryption formula for each letter. So, in spite of the sophisticated RSA calculations, our messages can be cracked with frequency analysis if they are long enough. To avoid this problem and get the full power of RSA, a different method is needed to change letters to numbers. In serious applications of RSA, a method is used that changes a block of letters to a many-digit number.

Related Topics

The "Do You Know?" in this chapter is about the British discovery of public-key cryptography. It is another example of how people throughout history have made important contributions but did not receive credit for their work. Because of the secrecy involved with cryptographic work, this is a common occurrence.

Website

After students understand the formulas of RSA, you can encourage them to work with large numbers so that their keys are more difficult to factor. Making and breaking each others' codes involves finding large prime numbers, factoring large numbers, and finding modular inverses. The calculator on the Cryptoclub website can help.

Treasure Hunts

In this section we describe three variations of treasure hunts—two types of classroom hunts and one electronic hunt. In each hunt, students follow a trail of clues to find some sort of treasure at the end, but the hunts differ in the amount of preparation needed to implement them. You can do all three at different times and repeat them with different clues.

The classroom hunts involve clues that are hidden in the classroom or on the playground. In the first type of hunt, you make and hide the clues. In the second type, the students make and hide the clues. In each case, you need to hide a small "treasure" at the final location. It is fun if you put the treasure in some mysterious box that resembles a small pirate's chest. Treasures can be gold foil-wrapped chocolate coins or more practical rewards such as pencils. It is good to have enough for everyone to share, not just a prize for the first group that finds the treasure.

The third and easiest for you to use is the online "Stormy Night Treasure Hunt" that is on the Cryptoclub website, since it is already prepared. This is an animated adventure that students progress through by decrypting clues at the computer.

Teacher-Made Hunts

In this type of hunt, you choose the hiding places and make the clues that describe them. In each hiding place, you leave an envelope containing copies of the clue (one for each student or group) that describes the next location, encrypted with a cipher you want your students to practice using. During the hunt, you can have each group solve every clue and progress through the hunt at their own pace. Or, you can have the class work together, with groups solving parts of each clue and sharing their results with the class. This way, the class progresses through the hunt together.

Here are two ways groups can progress through the hunt:

- **Groups solve clues at their own pace.** In this type of hunt, each group solves every clue. To avoid the problem of everyone crowding around the same location and seeing where other groups go next, consider staggering their starting locations. Group 1 starts at Location 1, Group 2 at Location 2, and so on. You can think of the clues as being part of a big circle, with groups starting and ending at different places in the circle. When groups finish, they bring their clues to you as proof they have visited every location, and you then give them a final clue that describes the location of the treasure.
- **Class progresses through the hunt together.** In this method, the groups share the work of decrypting the clues. Divide each clue into parts and write the parts on separate slips of paper—one part for each group. Each group decrypts their part of the clue, then the groups read their parts aloud to hear the whole clue. For example, here is a clue divided into parts for four groups:

  Group 1: The first place that
  Group 2: you should look is
  Group 3: where you can go
  Group 4: to get a book.

  By dividing up the clue, the information learned by each group is not enough to reveal the next location—the bookcase—until it is combined with all parts of the clue. This helps keep the class together.

Materials

treasure (in a "treasure chest")
envelopes, one for each location
clues, at least one copy of each clue for each group, preferably one for each student ("Teacher-Made Treasure Hunt Clues," six pages in *Blackline Masters*, contain clues for a sample teacher-made classroom hunt with clues divided into parts for four groups.)

Preparation

1. Choose five or six locations and prepare clues that describe them.
2. Place copies of each clue in an envelope labeled with that clue's number. (It helps to write a note to yourself on the back of the envelope that reminds you where you plan to hide the clue—in the location described by the previous clue.)
3. At each location, hide the clue that describes the next location. Hide the treasure at the final location.
4. Start the hunt by distributing Clue 1 to all the groups.

Tips

- It is good if each student has a copy of the clue to write on. If groups work on different parts of the clue, clip together copies of the parts to make clue packets for each group. Label each clue packet with the group's number.
- If your hunt is in a large area, it is better to have groups solve full clues than to have the class work together to solve them, since it will be hard to keep the class together to share their answers.
- Use the Cryptoclub website to help you encrypt your clues quickly. Also, if your students will have computer access during the hunt, choose the computer as one of your locations and put a clue on the website's Message Board for them to retrieve electronically. You can make this clue longer since they have the tools of the site to help decrypt.
- The Vigenère cipher can cause problems if clues are divided into parts for groups to solve. This is because students will naturally write the keyword above the first letter of their part of the clue, but this might not match the way you encrypted the message if you started the keyword at the beginning of the clue.

Student-Made Hunts

After students have participated in a teacher-made hunt, they may enjoy writing and hiding their own clues. Student-made hunts take less preparation on your part, and students enjoy using their creativity to choose and describe the locations. It spoils the fun if they know too many of the clues in advance, but if each group makes and hides only one clue, there will still be enough clues they don't know to make the hunt enjoyable. However, careful coordination is needed so that everyone understands which clue they will hide.

To organize the hunt, divide the class into five or six groups, and assign the groups numbers: Group 1, Group 2, etc. Each group chooses a secret spot and describes it in a clue, but they don't hide their own clue in that spot. Instead, they give their clue (in a sealed envelope) to the group whose number is one less than theirs. Then, they hide the envelope containing the clue from the group whose number is one more than theirs in their secret spot. (Group 1 gives their clue to the teacher. The last group hides the final clue, which is prepared by the teacher.)

Materials

treasure (in a "treasure chest")
envelopes, one for each group
copies of "Make-Your-Own Treasure Hunt Student Instructions" (page in *Blackline Masters*), one for each group

Preparation

1. Hide the treasure.
2. Make the final clue that describes the location of the treasure. Encrypt the clue and put it in an envelope marked "Final Clue". (The last group will hide your clue in their secret spot, but they will not read it.)
3. Have students make and hide their clues, according to the instructions on the student page.
4. Start the hunt by giving all groups Clue 1 (prepared by Group 1).

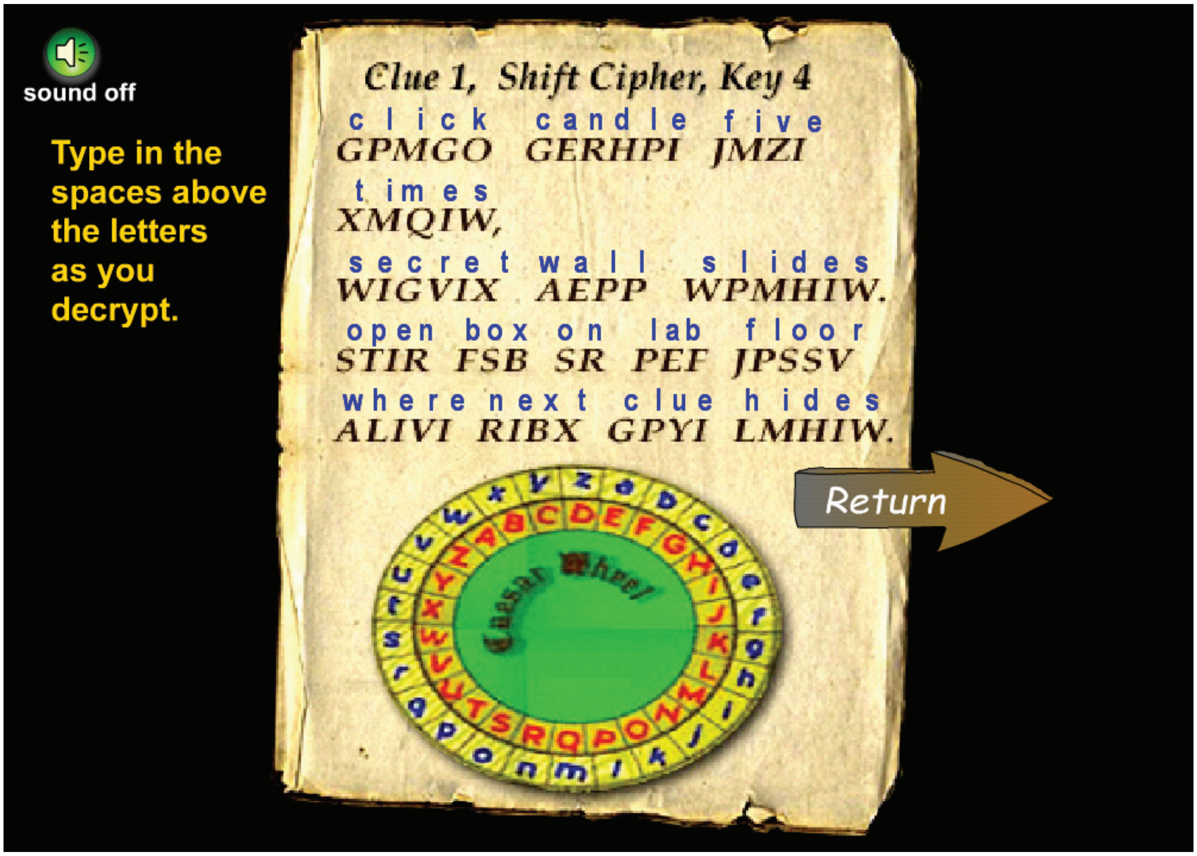
Tips

- Make sure everyone understands the procedure for hiding the clues before you begin. Students might not realize that they don't hide their own clue in their secret hiding place.
- Students can make poetic clues; for example, "The next place for you to look Is on the shelf near a red book." Or, they can make simpler clues; for example, "Look under the table in the corner by the door."
- You might want to ask students to give you their clues the day before the hunt so that you can check their encryptions.
- The clue envelopes need to contain at least one copy of the clue for each group.

The Cryptoclub Website´s Treasure Hunt

After your students have completed Unit 1, they will be ready to try the “Stormy Night Treasure Hunt” on the Cryptoclub website (http://cryptoclub.math.uic.edu). If you have a slow Internet connection (such as dial-up), it is best to download the treasure hunt instead of playing it online. If your students do not have Internet access, you can copy the downloaded game onto a CD and transfer it to their computers.

The figures on the next three pages are the website treasure hunt’s clues and their decryptions as they are at the time of this publication.



Type in the spaces above the letters as you decrypt.

Clue 1, Shift Cipher, Key 4

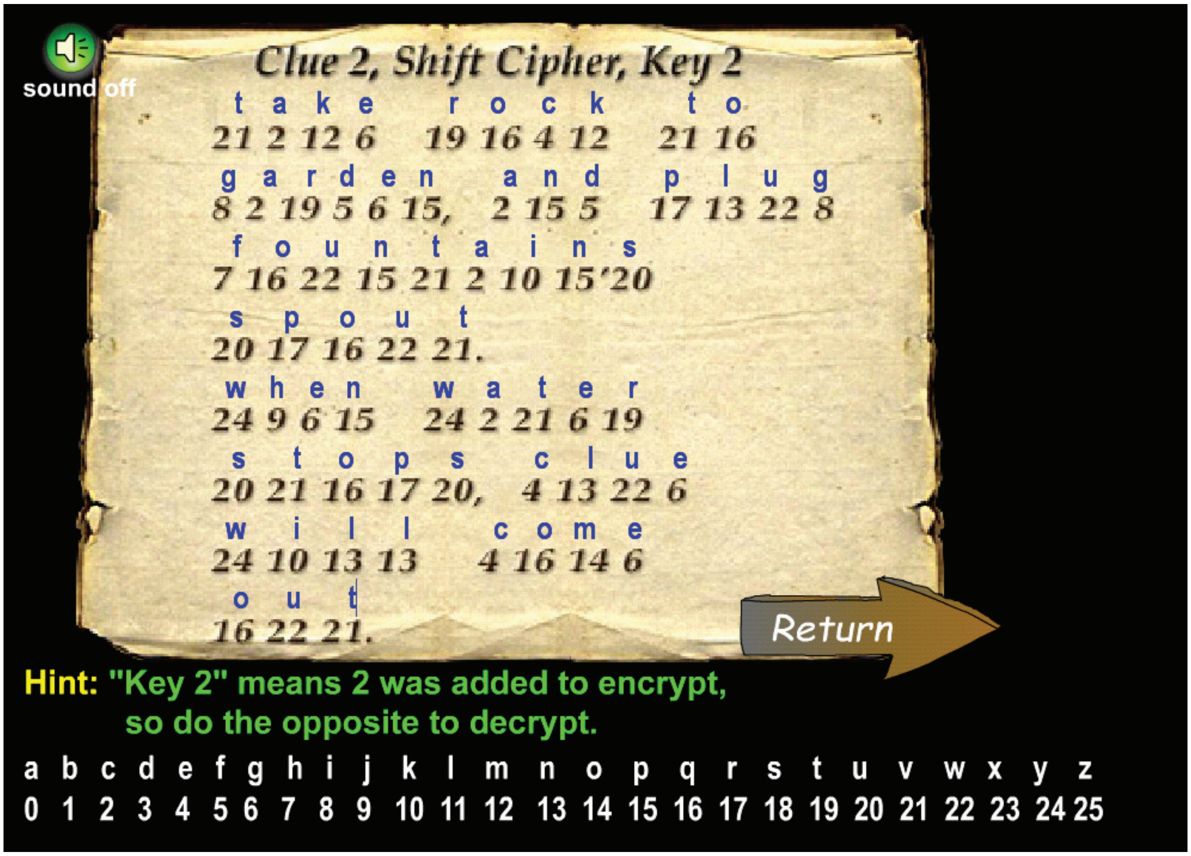
click candle five
GPMGO GERHPI JMZI

times
XMQIW,

secret wall slides
WIGVIX AEPP WPMHIW.

open box on lab floor
STIR FSB SR PEF JPSSV

where next clue hides
ALIVI RIBX GPYI LMHIW.



Clue 2, Shift Cipher, Key 2

take rock to
21 2 12 6 19 16 4 12 21 16

garden and plug
8 2 19 5 6 15, 2 15 5 17 13 22 8

fountains
7 16 22 15 21 2 10 15'20

spout
20 17 16 22 21.

when water
24 9 6 15 24 2 21 6 19

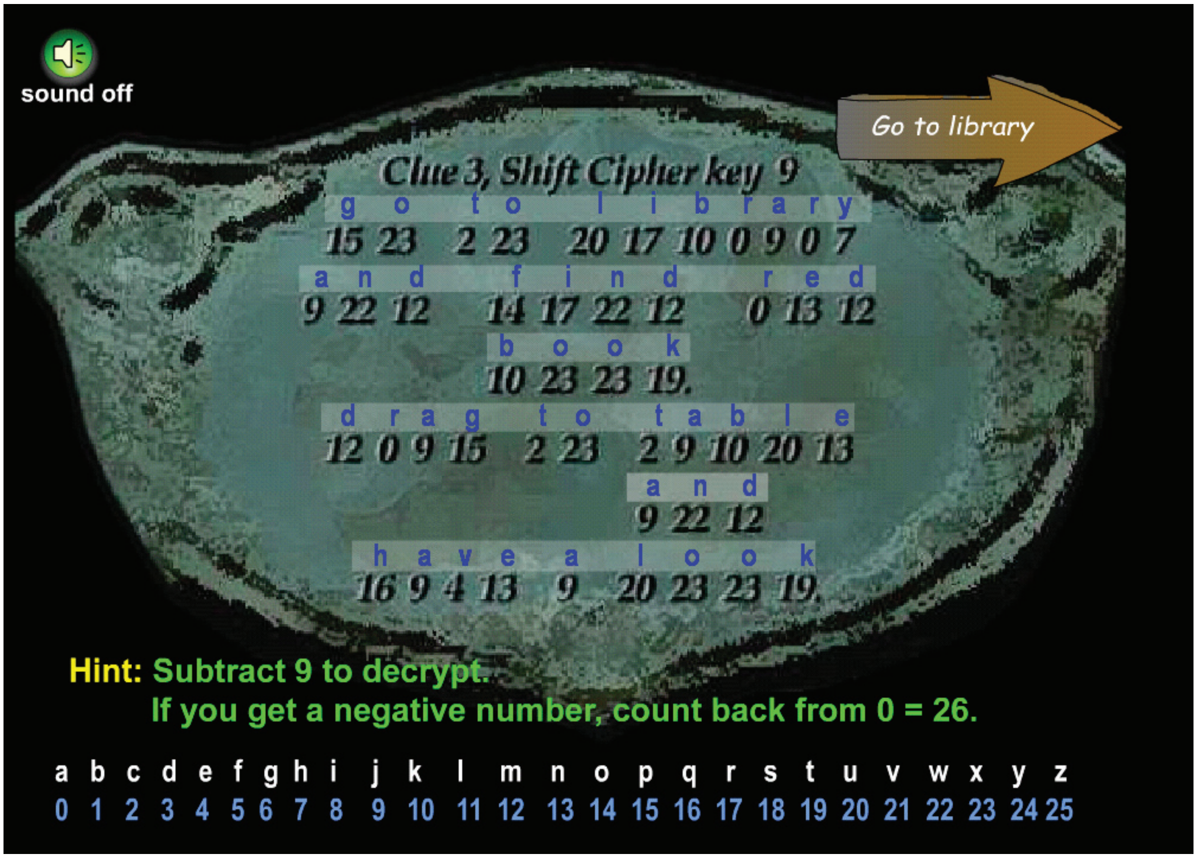
stops clue
20 21 16 17 20, 4 13 22 6

will come
24 10 13 13 4 16 14 6

out
16 22 21.

Hint: "Key 2" means 2 was added to encrypt, so do the opposite to decrypt.

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



Clue 3, Shift Cipher key 9

go to library
15 23 2 23 20 17 10 0 9 0 7

and find red
9 22 12 14 17 22 12 0 13 12

book
10 23 23 19.

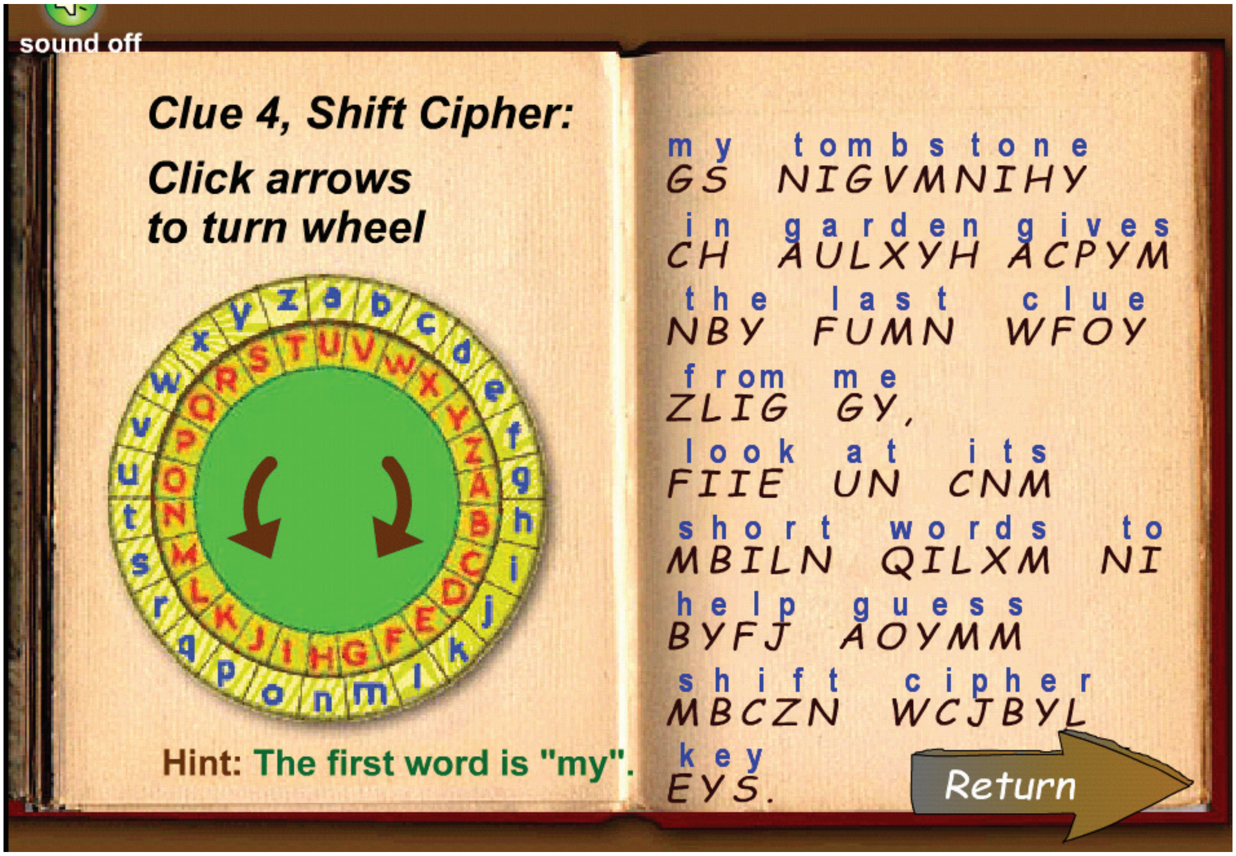
drag to table
12 0 9 15 2 23 2 9 10 20 13

and
9 22 12

have a look
16 9 4 13 9 20 23 23 19.

Hint: Subtract 9 to decrypt. If you get a negative number, count back from 0 = 26.

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



sound off

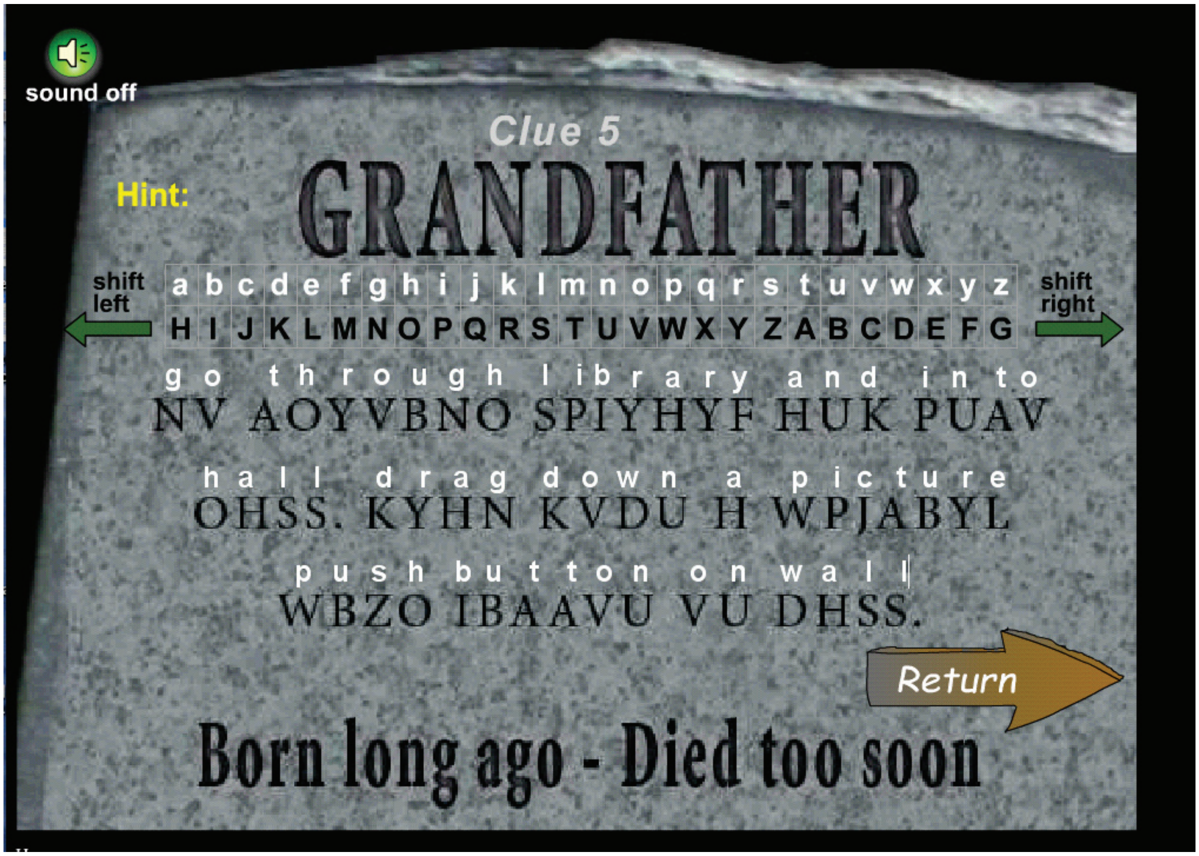
Clue 4, Shift Cipher:

Click arrows
to turn 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
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

Hint: The first word is "my".

my tombstone
GS NIGVMNIHY
in garden gives
CH AULXYH ACPYM
the last clue
NBY FUMN WFOY
from me
ZLIG GY,
look at its
FIIE UN CNM
short words to
MBILN QILXM NI
help guess
BYFJ AOYMM
shift cipher
MBCZN WCJBYL
key
EYS.



sound off

Clue 5

Hint:

GRANDFATHER

shift left

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
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

shift right

go through library and into
NV AOYVBNO SPIYHYF HUK PUAV
hall drag down a picture
OHSS. KYHN KVDU H WPJABYL
push button on wall
WBZO IBAAVU VU DHSS.

Born long ago - Died too soon