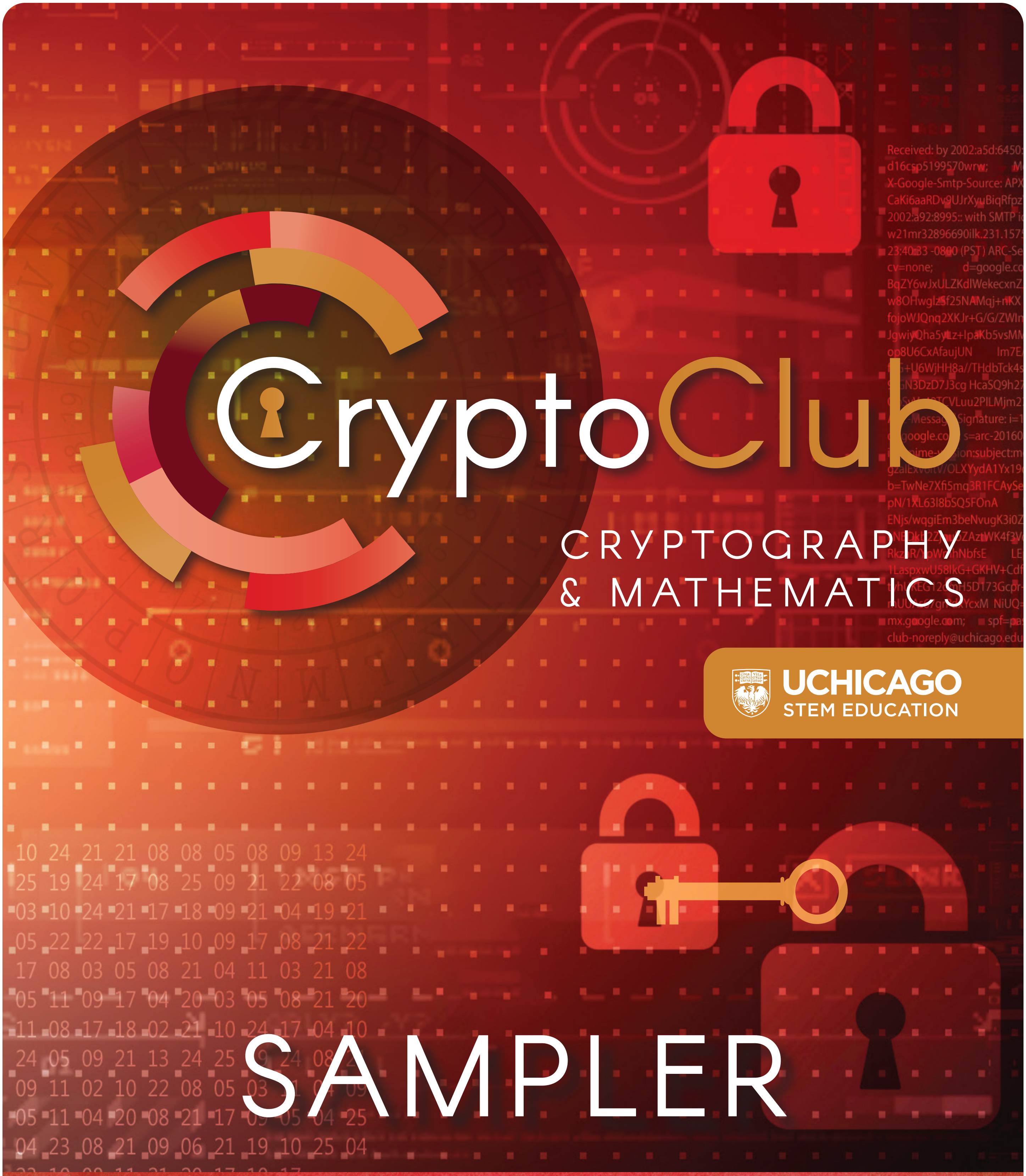


CryptoClub

CRYPTOGRAPHY & MATHEMATICS

UCHICAGO
STEM EDUCATION

SAMPLER

Kendall Hunt

Sampler Contents

This sampler is intended to be used as a brief introduction and preview of the full CryptoClub curriculum.

What is Cryptography?

Cryptography, the science of secret messages, is an intriguing math topic that is increasingly important in today's world. It is also a motivating setting for students to learn and apply mathematics skills.

Curriculum Design

The CryptoClub curriculum was developed with support from the National Science Foundation through an iterative design process that involved extensive testing with students and teachers around the country.

The curriculum is flexible and can be used as a semester long course, a supplement to an existing math curriculum or in math clubs. Some CryptoClubs meet a few times a week for about 10 weeks. Others meet weekly all year. It is adaptable to a variety of settings. Teachers have used it in their mathematics, technology, and elective classes, and in before and afterschool clubs. Others have used it in informal settings such as libraries, Boys and Girls clubs, 4-H programs, and YMCAs.

Mathematics in CryptoClub

Many people enjoy solving cryptograms that are commonly found in newspapers. Those are almost always encrypted with some type of substitution cipher, in which one letter of the alphabet is replaced with another. They can usually be puzzled out by taking advantage of familiar patterns in English, such as common letters, three-letter words, double letters, and so on. Whatever patterns might exist in the actual substitutions are rarely used to solve newspaper cryptograms.

In contrast, the ciphers explored in this book and most modern-day ciphers involve mathematical patterns. These patterns make it easier for the sender to communicate to the recipient how the message should be decrypted, but they also make it easier for an adversary to crack the code. Exploring mathematical patterns is a core experience for CryptoClub students.

The CryptoClub *Student Cipher Handbook* guides students to explore cryptography through problem-solving and critical-thinking activities that involve secret messages. In the activities, students apply mathematics from the middle-school curriculum as they make and break secret codes.

Students apply mathematics topics from the middle-school curriculum, such as decimals and percents, division with remainder, common factors, and negative numbers. They also apply pre-algebra skills such as pattern recognition and problem solving.

CryptoClub offers many opportunities to help students to develop the mathematical habits listed in the Standards for Mathematical Practice from the *Common Core State Standards for Mathematics (CCSS)*.

The CryptoClub project began at the University of Illinois at Chicago and is now located at the University of Chicago's Center for STEM Education. Through a series of grants from the National Science Foundation, the team has developed books and digital activities for teaching cryptography to middle school students. These curriculum materials were developed by mathematicians who have experience in mathematics education in both formal and informal settings, and tested by teachers and students in an iterative design process over six years, including a 2012-13 field test in 29 national sites.

UCHICAGO
STEM EDUCATION

Chapter Summaries

Each chapter of the *Student Cipher Handbook* follows a similar format: Students explore a message that was encrypted with a new cipher, looking for a pattern to describe the encryption method. The cipher details are then summarized and students practice encrypting and decrypting through games and activities that involve sending and receiving secret messages. After they understand the encryption method, they crack messages without knowing the encryption key. It is usually more challenging to crack a code, but that makes success more rewarding.

The order in which you teach the chapters is flexible, as long as the prerequisites for each chapter are covered first. Covering Chapters 1 – 6 in order gives a nice balance between numeric and other ciphers. If you have limited time and prefer to focus mostly on numeric ciphers, then Chapters 1, 2, 4, and 6 would make a good program. If you prefer a program with a variety of ciphers and less advanced mathematics content, you could cover Chapters 1 – 3. The Vigenère cipher of Chapter 5 is historically significant, since it was used in the American Civil War. An interesting program that avoids the numeric ciphers and includes the Vigenère cipher would be Chapters 1, 3, and 5.

Chapter 1. Caesar Ciphers

The chapter begins with a riddle that's answer has been encrypted by a simple shift of the alphabet. Students guess the answer, using their familiarity with English. They enter the data in a table, find a pattern to complete the table, and thus discover the Caesar cipher pattern. The cipher is then formally introduced, along with basic vocabulary of cryptography. They are introduced to three tools to help encrypt and decrypt with Caesar ciphers: the cipher table, cipher wheel, and Vigenère Squares. Later, students practice problem solving and English language skills as they crack messages—that is, decrypt without knowing the encryption key.

Vocabulary: cipher, Caesar cipher, encrypt, decrypt, crack, key, plaintext, ciphertext

Chapter 2. Additive Ciphers

Prerequisite: Chapter 1

The chapter opens with another riddle that has an encrypted answer. Students guess the answer, examine the pattern in a table, and discover the additive cipher pattern. In an additive cipher, they change letters to numbers and add or subtract a key. Special consideration is needed when adding gives numbers larger than 25 and when subtracting gives negative numbers. This involves concepts from modular (clock) arithmetic. After encrypting and decrypting, the chapter ends with cracking activities.

Math Content: mental arithmetic, addition and subtraction, negative numbers, modular (clock) arithmetic, commutative property, associative property

Chapter 3. Keyword and Other Substitution Ciphers

Prerequisite: Chapter 1

The chapter opens with a message that has been encrypted with a substitution cipher that has a less obvious pattern than the Caesar cipher. After cracking the message using familiarity with English and entering their substitutions in a cipher table, students discover the keyword cipher pattern. One way to crack any substitution cipher is to compare the frequencies of letters in the message with the frequencies of letters in English. In this chapter, students collect data to find the most common letters in a message. They then match these with the most common letters in English and begin to crack the message. Later, they examine English text more closely to find out for themselves the most common letters in English. After working with several substitution ciphers, they are invited to make their own ciphers with their own patterns.

Math Content: Data collection, frequency and relative frequency, changing fractions to decimals, changing decimals to percent, tallying

Chapter 4. Multiplicative Ciphers

Prerequisites: Chapters 1 and 2

The chapter opens with a message that has been encrypted with a multiplicative cipher. After cracking the message and entering numbers in the cipher table, students see a familiar multiplicative pattern. In a multiplicative cipher, letters are first changed to numbers and then encrypted by multiplying by a key. If the answer is greater than 25, it is replaced by the equivalent number mod 26, as is done in the additive cipher. Working in modular arithmetic is an important application of division with remainder. Students discover that the key for a multiplicative cipher has to be carefully chosen because some numbers do not make good keys. In this chapter, students learn two ways to decrypt a multiplicative cipher: using multiplicative cipher tables and using the multiplicative inverse of the key. Exploring inverses in modular arithmetic can reinforce students' understanding of what an inverse is in regular arithmetic. Cracking a multiplicative cipher when they don't know the encryption key is a chance to practice algebra. If they can figure out one letter of the message, they can set up an equation that, when solved, reveals the key.

Math Content: multiplication (up to 2-digit by 2-digit numbers), division with remainder with a 2-digit divisor, factoring, common factors, modular arithmetic, reducing mod 26, multiplicative inverses, solving linear equations

Chapter 5. Vigenère Ciphers

Prerequisites: Chapters 1 and 3

The chapter begins with a message for students to examine that contains several unusual patterns. They conclude that it could not have been encrypted with a simple substitution cipher. They are told that it was encrypted with the Vigenère cipher, which was used during the Civil War. The Vigenère cipher is interesting because it was once thought to be unbreakable, but today methods are known to crack it using nothing more than middle-grade mathematics. 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. After learning how to crack a Vigenère cipher, students tackle the opening message of the chapter. In working with the Vigenère cipher, students combine many mathematics skills and build confidence in solving complex problems.

Math Content: factoring, finding common factors, finding data in a matrix (Vigenère square), tallying data, combining data from several problems to solve a larger problem, finding prime factorizations, divisibility, exponents, finding common factors

Chapter 6. Affine Cipher

Prerequisites: Chapters 1, 2, and 3

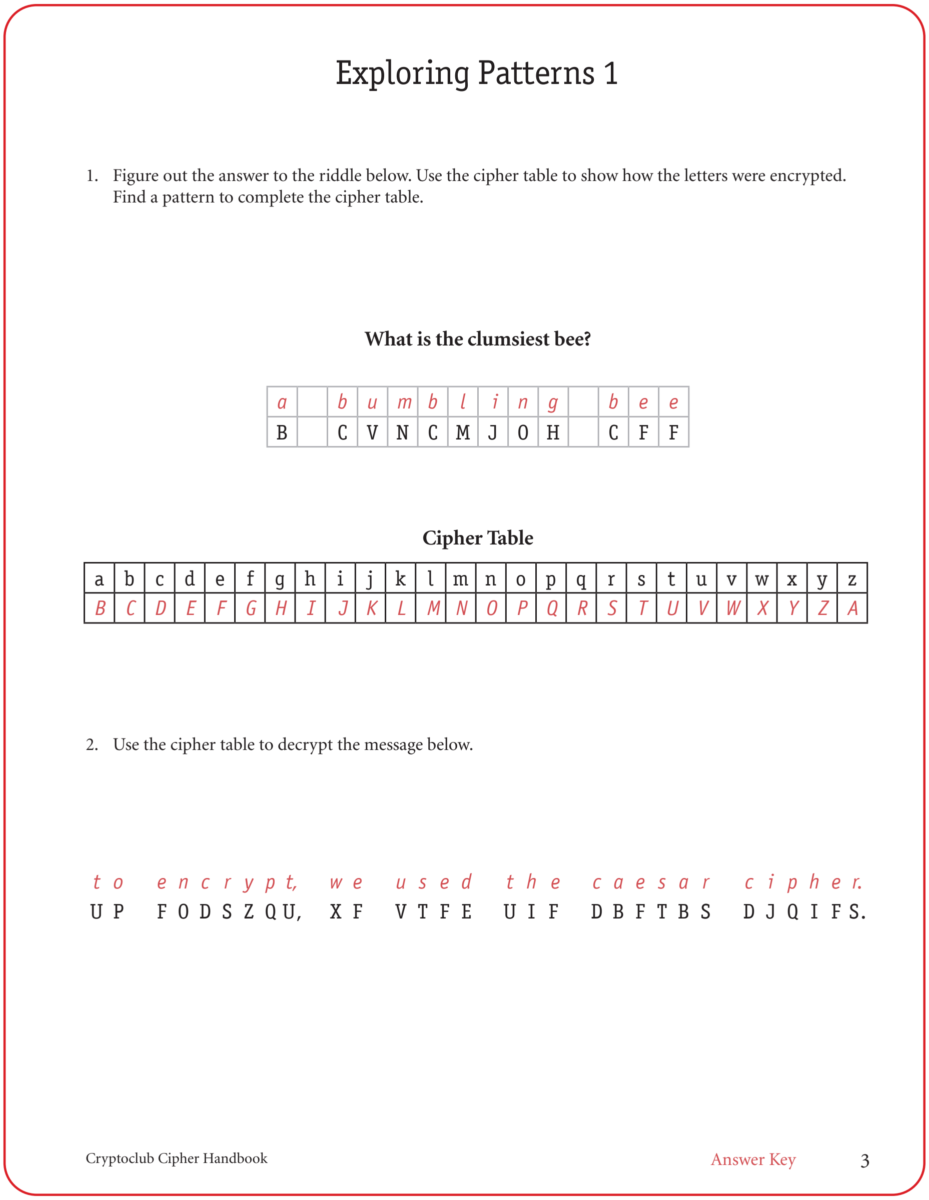
The affine cipher combines multiplication and addition. Working with affine ciphers is a good way for students to reinforce some of their algebra skills. For example, one way to crack an affine cipher is to solve systems of linear equations in two unknowns. Solving for the unknown reveals the key. As with the other chapters, this chapter begins with a message for students to examine. They explore the patterns in a cipher table and figure out the affine cipher for themselves. They encrypt and decrypt with various keys and then try their skills at the challenge of cracking several messages. Students who have studied linear equations in their math classes will recognize a similarity to the affine cipher.

Math Content: multiplication (up to 2-digit by 2-digit numbers), division with remainder with a 2-digit divisor, order of operations, arithmetic patterns, modular arithmetic, reducing mod 26, using multiplicative inverses, linear equations, solving two linear equations.

Games and Related Activities

The Games section describes games that provide a fun, engaging way for students to practice cryptography and math skills and increase their reasoning power. They include *Cipher Tag* and *Bucket Messages*, in which students create messages for others to decrypt, and *Crypto Jigsaw*, in which teams decrypt parts of a secret message and race to piece them together to reveal the whole message. A student favorite is a treasure hunt, in which teams follow a trail of encrypted clues to find a reward at the end.

Exploring Patterns 1



Exploring Patterns 1

1. Figure out the answer to the riddle below. Use the cipher table to show how the letters were encrypted. Find a pattern to complete the cipher table.

What is the clumsiest bee?

a		*b*	*u*	*m*	*b*	*l*	*i*	*n*	*g*		*b*	*e*	*e*
B		C	V	N	C	M	J	O	H		C	F	F

Cipher Table

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

2. Use the cipher table to decrypt the message below.

to encrypt, we used the caesar cipher.
UP FODSZQU, XF VTFE UIF DBFTBS DJQIFS.

Cryptoclub Cipher Handbook Answer Key 3

Each section of the *Student Cipher Handbook* begins with a page like this, which invites students to explore patterns in a cipher they have not yet learned about. The pattern they will observe on this page is that each letter is encrypted as the next letter in the alphabet. They can use their own observations and understandings about English to figure out the message. This gives them satisfaction and builds their confidence in their reasoning abilities.

A good way to introduce the cipher is to write the riddle at the top of the page on the board for students to solve before they open their books. Then ask them to open to the page and fill in the cipher table using the pattern they observed.

Cracking the message: If students need help cracking the message, ask:

- What could the one-letter word be? (*Probably **a** or **I***)
- The last two letters are the same. What 3-letter words end in a double letter? (*all, bee, baa, fee, see, etc.*)

Finding the pattern:

- What pattern can you use to complete the table? (*Each letter is encrypted as the next letter in the alphabet. The alphabet is shifted one letter to the left.*)
- What is the next letter after ***Z***? (*When the alphabet ends at Z in the table, it starts over again with **A** (**…, X, Y, Z, A**) and then wraps around to begin the table where it left off* (***B, C, …***)

After students have completed the cipher table, they should use it to decrypt the message at the bottom of the page. This will confirm that they used the correct pattern in the table.

After the class has discussed the page, explain that ciphers that shift the alphabet, such as the cipher given in the table, are called Caesar ciphers. They will be introduced formally on the next page.

Exploring Patterns 1

1. Figure out the answer to the riddle below. Use the cipher table to show how the letters were encrypted. Find a pattern to complete the cipher table.

What is the clumsiest bee?

B		C	V	N	C	M	J	O	H		C	F	F

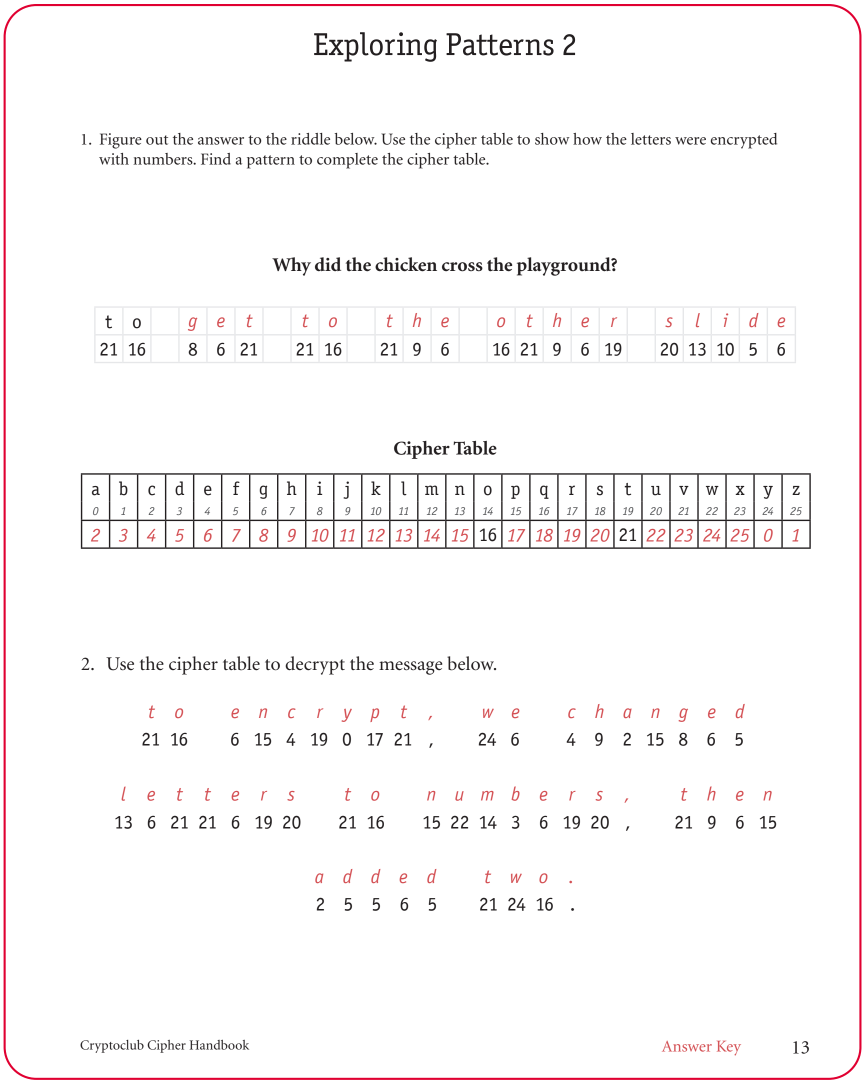
Cipher Table

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

2. Use the cipher table to decrypt the message below.

UP FODSZQU, XF VTFE UIF DBFTBS DJQIFS.

Exploring Patterns 2



Exploring Patterns 2

1. Figure out the answer to the riddle below. Use the cipher table to show how the letters were encrypted with numbers. Find a pattern to complete the cipher table.

Why did the chicken cross the playground?

t	o		g	e	t		t	o		t	h	e		o	t	h	e	r		s	l	i	d	e
21	16		8	6	21		21	16		21	9	6		16	21	9	6	19		20	13	10	5	6

Cipher Table

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

2. Use the cipher table to decrypt the message below.

t o e n c r y p t , w e c h a n g e d
21 16 6 15 4 19 0 17 21 , 24 6 4 9 2 15 8 6 5

l e t t e r s t o n u m b e r s , t h e n
13 6 21 21 6 19 20 21 16 15 22 14 3 6 19 20 , 21 9 6 15

a d d e d t w o .
2 5 5 6 5 21 24 16 .

Cryptoclub Cipher Handbook Answer Key 13

This page invites students to explore cipher patterns that involve numbers before being formally introduced to additive ciphers. They should use patterns from English, as well as their own ideas about what might make sense as an answer to the riddle in order to guess how to decrypt.

As they guess the answer to the riddle, they should put numbers into the table showing the letter-to-number correspondence. Then they should look for patterns in the table that help them fill in the rest of the numbers. Two letters are revealed to help students see how to place the numbers into a the cipher table

The answer to the riddle was encrypted with a cipher that changes letters to numbers (**a**→0, **b**→1, and so forth) and then adds 2 to the number.

Cracking the message: If students have trouble guessing the answer to the riddle, ask:

- Have you heard chicken riddles before? How does the answer to a riddle like this usually start? (*to get to the other...*)
- How did you figure out the last word of the answer? (*I found a pattern that helped to complete the table. Then I used the table to decrypt the last word. I got* ***slide***.)

Finding the pattern:

- What pattern do you see from left to right in the table? (*The numbers start at 2 and go up by one. The numberline is shifted two spaces to the left.*)
- How do the numbers in the second row of the **Cipher Table** compare with the numbers in the first row? (*They are 2 more, for example:* **e** *is 4 and under* **e** *is 4 + 2 = 6.*)
- What should happen at the end of the row? (**y**, **z** *should correspond to* **0**, **1**) NOTE: Some students may want **y z** to correspond to **26 27**, but they should see that then there would be no way to decrypt **0**, which appears in the bottom message. You can tell them that "wrapping around" is common practice.
- Does decrypting the message on the bottom of the page confirm the pattern? (*Yes.*)

After the class has discussed *Exploring Patterns 2* (page CH 13), you can explain that its table is the cipher table for the additive cipher with key 2. The small numbers in the first row are there to show how letters are changed to numbers. Throughout the book a letter-to-number table appears to aid in encrypting and decrypting with number ciphers. Additive ciphers will be introduced formally over the next few pages.

Exploring Patterns 2

1. Figure out the answer to the riddle below. Use the cipher table to show how the letters were encrypted with numbers. Find a pattern to complete the cipher table.

Why did the chicken cross the playground?

t	o																							
21	16		8	6	21		21	16		21	9	6		16	21	9	6	19		20	13	10	5	6

Cipher Table

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*
														16					21						

2. Use the cipher table to decrypt the message below.

21 16   6 15 4 19 0 17 21 ,   24 6   4 9 2 15 8 6 5

13 6 21 21 6 19 20   21 16   15 22 14 3 6 19 20 ,   21 9 6 15

2 5 5 6 5   21 24 16 .

Cryptoclub Student Cipher Handbook page 13

KEYWORD CIPHERS

Overview

In a **substitution cipher**, each letter of the plaintext is replaced by a different letter, number, or symbol. Both the Caesar cipher and the additive cipher are examples of substitution ciphers that are relatively easy to crack because of their shift pattern. Substitution ciphers that do not have any particular patterns are harder to crack, but they can be cumbersome to use because you need to write out the entire substitution table to tell someone how you encrypted a message.

In this chapter, students learn to use another substitution cipher, the **keyword cipher**. It can be described with a short keyword, so it is more practical for sending messages than a cipher that has no patterns at all. But it has the advantage that it is harder to crack than Caesar or additive ciphers.

It might seem that substitution ciphers would be difficult or impossible to crack—there are more ways to fill in a substitution table than you could write out in a lifetime. In fact, there are 26 × 24 × 23 × … × 2 × 1 = 403,291,461,126,605,635,584,000,00 0 possible ways to fill in a substitution cipher table. If you filled in one table per minute, it would take you about 767 quintillion years (that's a billion billion) to fill in them all. But you don't have to try every possible substitution to crack a substitution cipher—the patterns in English make cracking relatively easy to do.

Students might already be familiar with cracking substitution ciphers. The cryptograms that often appear in newspapers and magazines are usually encrypted with substitution ciphers. Readers usually crack them using nothing more than familiarity with English—knowledge of some common letters, double letters, short words, and so on.

Teaching

This chapter is different in some ways from other chapters. In addition to introducing a new cipher with exploring, encrypting, decrypting, and cracking activities, it has a data collection activity that explores letter frequencies and an activity in which students create their own substitution ciphers.

Letter frequencies are useful in cracking all substitution ciphers. Exploring the frequency of letters in English (pages CH 33-35) is a worthwhile activity that helps to reinforce students' understanding of decimals and percent. However, it is optional, depending on the time you have available. Whether students do this activity or not, the most common letters in English are provided (page CH 31), so students can use them to help crack messages.

Students will likely enjoy the opportunity (pages CH 36-37) to create their own ciphers. These pages are also optional, but worthwhile, and can lead to rich class discussions.

As in all chapters, the *Student Cipher Handbook* will help you introduce the key concepts and provide students with initial practice.

A more sophisticated approach to cracking substitution ciphers is to analyze the frequency of the letters in the message. The idea is to find the most common letters in the message, and match them with the most common letters in English.

Frequency analysis is an important tool for cryptographers, and exploring this technique for cracking messages is an interesting opportunity for students to use decimals and percents.

Prerequisite:
Chapter 1

Math Content: Data collection, frequency and relative frequency, changing fractions to decimals, changing decimals to percent, tallying

Vocabulary: keyword cipher, substitution cipher, frequency, relative frequency

Materials: calculators

Games
Directions for classroom games are found in the Games section. The following are suggested for this chapter:

Bucket Messages (page 90)
Crypto Jigsaw (page 92)
Cipher Relay (page 93)
Frequency Cracking Game (page 94)
Treasure Hunts (page 96)

Website:
The following website tools and activities are suggested for additional practice:

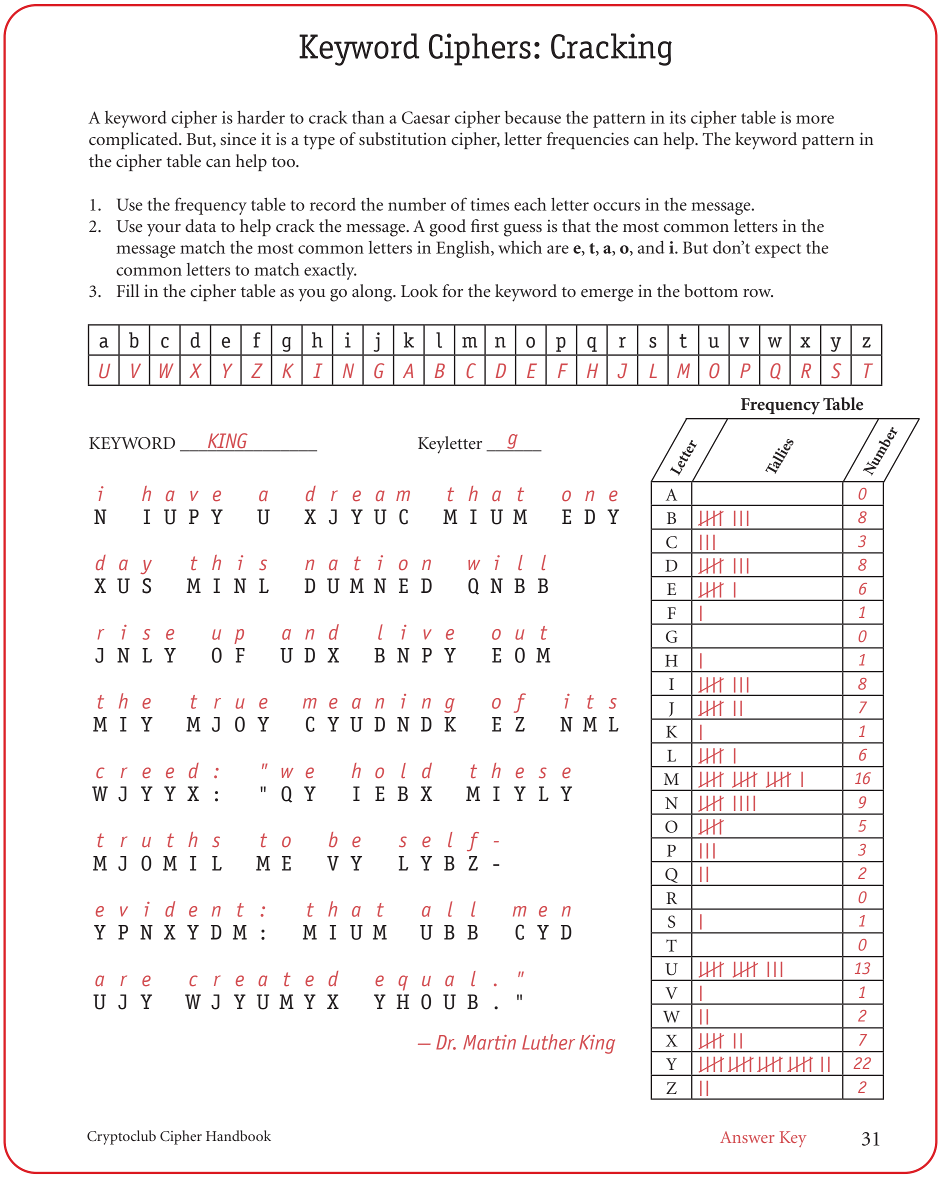
Cipher Tools Section:
Keyword
Substitution
Crack Substitution

Challenges Section:
Message Board
Joke Board
Group Message Board (teacher created)

Games Section:
Rogue Computer (a mission of *V.O.R.T.E.X*)

For Teachers Section:
Cipher Cracking Worksheet Generator
Treasure Hunt Clue Generator
Jigsaw Generator

Keyword Cipher: Cracking



Keyword Ciphers: Cracking

A keyword cipher is harder to crack than a Caesar cipher because the pattern in its cipher table is more complicated. But, since it is a type of substitution cipher, letter frequencies can help. The keyword pattern in the cipher table can help too.

1. Use the frequency table to record the number of times each letter occurs in the message.
2. Use your data to help crack the message. A good first guess is that the most common letters in the message match the most common letters in English, which are **e**, **t**, **a**, **o**, and **i**. But don't expect the common letters to match exactly.
3. Fill in the cipher table as you go along. Look for the keyword to emerge in the bottom row.

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	K	I	N	G	A	B	C	D	E	F	H	J	L	M	O	P	Q	R	S	T

KEYWORD KING Keyletter g

```
i   h a v e   a   d r e a m   t h a t   o n e
N   I U P Y   U   X J Y U C   M I U M   E D Y

d a y   t h i s   n a t i o n   w i l l
X U S   M I N L   D U M N E D   Q N B B

r i s e   u p   a n d   l i v e   o u t
J N L Y   O F   U D X   B N P Y   E O M

t h e   t r u e   m e a n i n g   o f   i t s
M I Y   M J O Y   C Y U D N D K   E Z   N M L

c r e e d :   " w e   h o l d   t h e s e
W J Y Y X :   " Q Y   I E B X   M I Y L Y

t r u t h s   t o   b e   s e l f -
M J O M I L   M E   V Y   L Y B Z -

e v i d e n t :   t h a t   a l l   m e n
Y P N X Y D M :   M I U M   U B B   C Y D

a r e   c r e a t e d   e q u a l . "
U J Y   W J Y U M Y X   Y H O U B . "
```

— Dr. Martin Luther King

Frequency Table

Letter	Tallies	Number
A		0
B	𝍸 |||	8
C	|||	3
D	𝍸 |||	8
E	𝍸 |	6
F	|	1
G		0
H	|	1
I	𝍸 |||	8
J	𝍸 ||	7
K	|	1
L	𝍸 |	6
M	𝍸 𝍸 𝍸 |	16
N	𝍸 ||||	9
O	𝍸	5
P	|||	3
Q	||	2
R		0
S	|	1
T		0
U	𝍸 𝍸 |||	13
V	|	1
W	||	2
X	𝍸 ||	7
Y	𝍸 𝍸 𝍸 𝍸 ||	22
Z	||	2

Cryptoclub Cipher Handbook Answer Key 31

On this page, students collect data to find the most common letters in the message. They use this information to guess the letter substitutions. Students are told that the five most common letters in English are **e**, **t**, **a**, **o**, and **i**. On *Letter Frequencies: Examining English Text* (page CH 34), they will examine English text more closely to find out for themselves the most common letters in English.

One way for students to collect the data is to work in pairs, with one partner calling out the letters of the message, while the other makes tally marks to record them. You can demonstrate how this works with a student naming the letters while you mark the tallies on the board. If students are unfamiliar with tallies, demonstrate how five marks are bundled together, with the fifth mark tying the previous four together.

An alternate way to collect the data is for each student in a group to be assigned a few letters to count. They go through the message counting the occurrences of their letters and share their results with the group. Note that if they count letters directly in this way, they do not need to go back later and fill in tally marks in the table—the tallies are a recording tool, not an end result themselves.

Since **Y** is the most common letter in the message and **e** is the most common letter in English, a good guess is that **e** was encrypted as **Y**. Similarly, letter frequencies suggest that **t** was encrypted as **M**. Students will probably notice that the frequencies are helpful in making initial guesses, but after they get started on a message, they will use their familiarity with the words that are emerging as stronger clues to the letter substitutions. For example, after decrypting **t** and **e**, they might notice **t** __ **e** in the fourth line and guess that it is the word **the**. This suggests that **I** should be decrypted as **h**.

As students enter substitutions in the table, they might recognize the keyword cipher pattern emerging in the bottom row. This will help them guess ways to complete the cipher table. They can try out their guesses by seeing whether their substitutions make sense in the message.

Keyword Ciphers: Cracking

A keyword cipher is harder to crack than a Caesar cipher because the pattern in its cipher table is more complicated. But, since it is a type of substitution cipher, letter frequencies can help. The keyword pattern in the cipher table can help too.

1. Use the frequency table to record the number of times each letter occurs in the message.
2. Use your data to help crack the message. A good first guess is that the most common letters in the message match the most common letters in English, which are **e**, **t**, **a**, **o**, and **i**. But don't expect the common letters to match exactly.
3. Fill in the cipher table as you go along. Look for the keyword to emerge in the bottom row.

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

KEYWORD ________________ Keyletter ______

N IUPY U XJYUC MIUM EDY

XUS MINL DUMNED QNBB

JNLY OF UDX BNPY EOM

MIY MJOY CYUDNDK EZ NML

WJYYX: "QY IEBX MIYLY

MJOMIL ME VY LYBZ-

YPNXYDM: MIUM UBB CYD

UJY WJYUMYX YHOUB."

Frequency Table

Letter	Tallies	Number
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		

Cryptoclub Student Cipher Handbook page 31

Cipher Relay

This game is an active version of *Crypto Jigsaw*. Players take turns going back and forth between two locations, as in a traditional relay race, carrying message pieces to decrypt. When all pieces have been decrypted, the team puts them together to reveal the complete message. The goal is to be the first team to complete the task. The structure of the game ensures that each player has a turn in decrypting.

Players:

Teams of 3–5 players.

Materials:

- Encrypted messages, cut into strips, one set for each team, as in *Crypto Jigsaw*. There should be at least as many strips as there are team members.
- Two envelopes to hold the message pieces for each team, one for the un-decrypted strips and another for the decrypted strips.
- Tools necessary to decrypt the message, such as cipher wheels, Vigenère squares, or calculators. This will depend on which cipher is used.
- Clipboards for each team (optional)

Before play begins:

Prepare the messages as for the *Crypto Jigsaw* game. Put a set of message strips into an envelope for each team. The *Jigsaw Generator* on *cryptoclub.org* can help.

The relay race needs plenty of room. Each team needs two locations, a starting location where the team lines up and a decrypting station about 10–15 feet away where players go to decrypt. A hallway works well for this, as long as the noise of the game won't disturb others in the building.

Play of the game:

To begin, one member from each team goes to the decrypting station with an empty envelope. The rest of the team members line up at the start, as if for a regular relay race. The first member in line holds the envelope of strips.

When the referee says, "Go," the first person in line takes a strip out of the envelope, gives the envelope to the next person in line and runs to to the decrypting station to join the teammate who is already there. The two players work to decrypt the message on the strip. When decrypted, they place the strip in the empty envelope. The original team member now runs back to the start, tags the first person in line and goes to the end of the line. When tagged, the player at the head of the line takes a strip out of the envelope, hands the envelope to the next person in line and runs to the decrypting station, where the two players decrypt the strip and place it in the envelope with the other decrypted strips. The person who arrived most recently stays there and the other person runs back to the start.

When the last strip has been decrypted, players run to the start, where the team works to put the strips into the correct order. When they have completed the jigsaw, they give it to the referee. The first team to complete the message correctly is the winner.

A good way to organize the finish of the game is to have each team label the strips 1, 2, 3, etc. in the correct order and return them to the envelope. As the teams finish, you can label the envelopes first, second, third, etc. in order of completion. After everyone finishes and you gather all teams together, open the first envelope and read the strips in order. If it is correct, this team wins. If not, open the envelope marked second. If the strips are in the right order this team wins, otherwise continue through the envelopes in order until there is a winner.

Tips:

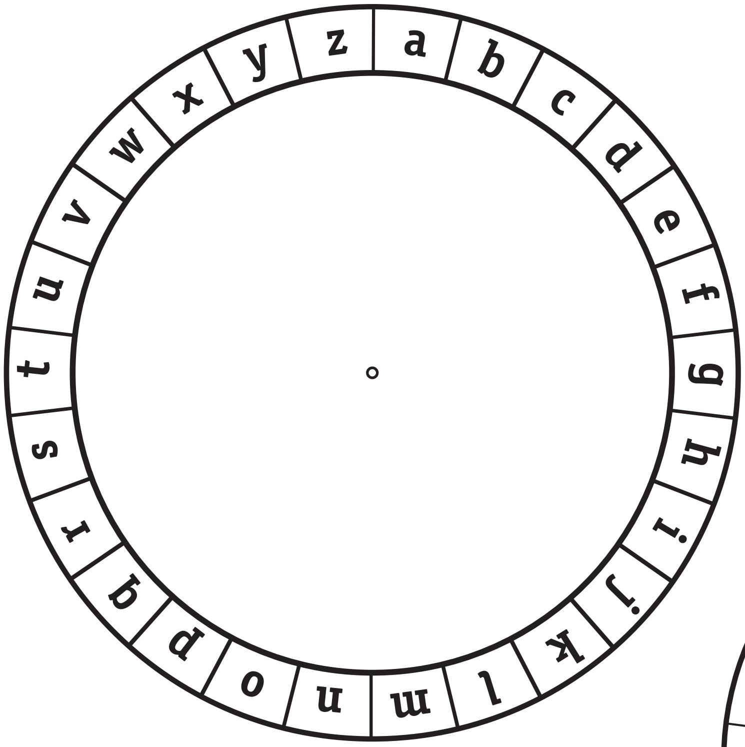
- There needs to be enough room to run so that the game is as exciting as a real relay race. If possible, going outdoors is always a good idea.
- Unlike *Crypto Jigsaw*, the whole team is not working simultaneously on the decryption phase of this game. However, players can take advantage of the expertise of their teammates by passing the techniques from one player to the next as they decrypt in pairs.

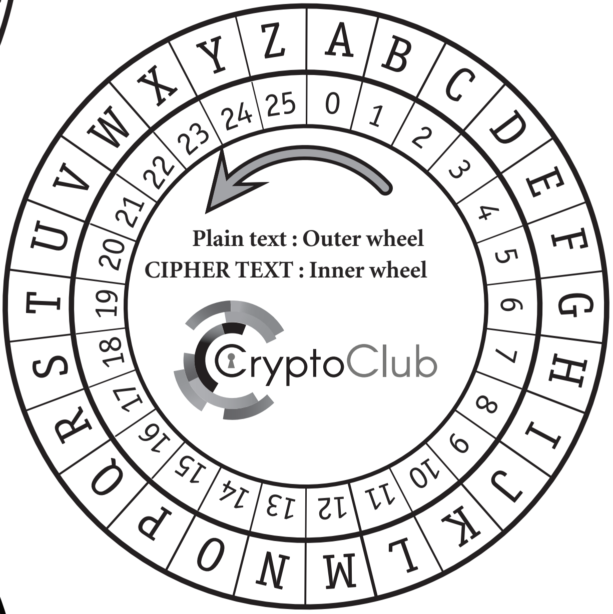
A player at the decrypting station welcomes a teammate who will help to decrypt.

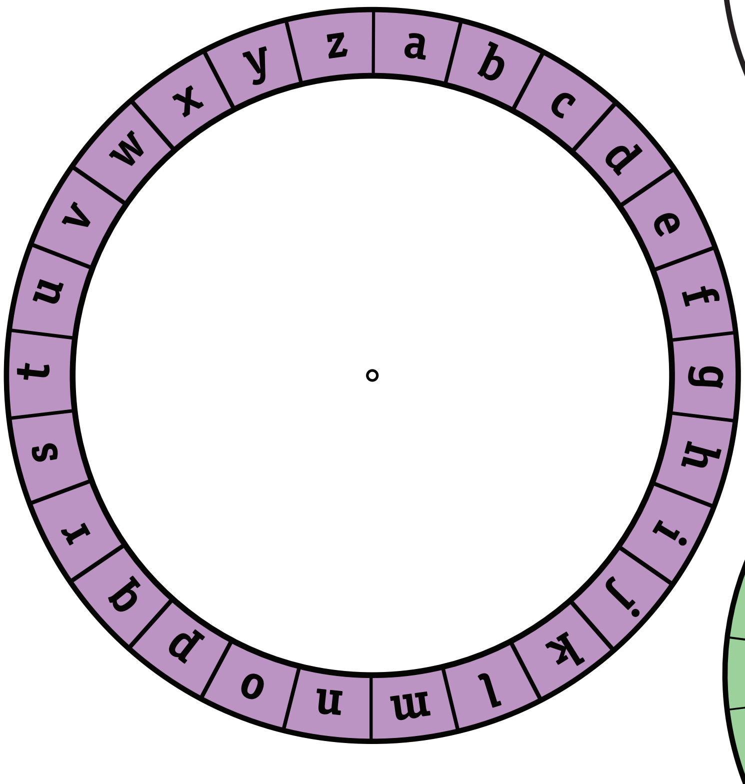
Cipher Wheels

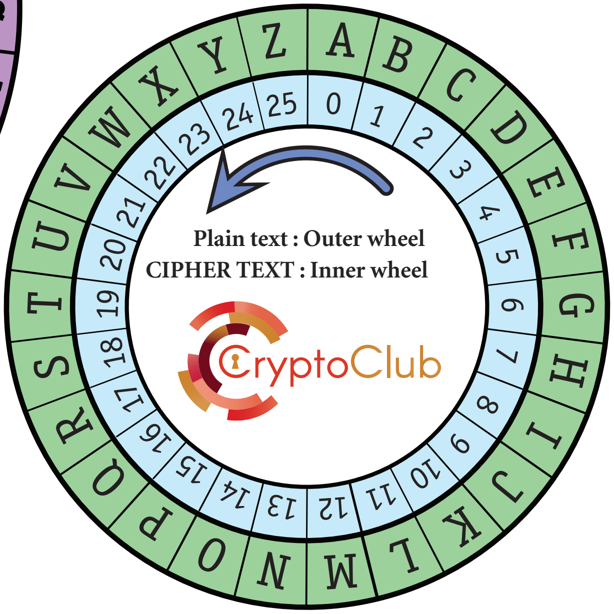
The cipher wheel is one of three Caesar ciphers introduced in Chapter 1.

Directions: *To make a cipher wheel, cut out two parts and fasten them together with a brad (paper fastener). Be sure to match the centers carefully so the letters line up properly when the wheel is turned.*









CryptoClub Connections to the
Common Core State Standards for Mathematics (CCSSM)

Standards for Mathematical Practices

Any rich mathematical application, such as cryptography, provides opportunities for students to develop good mathematical practices.

1. Make sense of problems and persevere in solving them.

The problems faced in cryptography are different from what students experience in regular math class. They give students opportunities to explore new techniques and to try out their own ideas. Perseverance is often needed to crack an encrypted message. Students reflect on their thinking and check whether the decrypted message makes sense.

2. Reason abstractly and quantitatively.

Arithmetic ciphers are a real-world application of modular arithmetic, which is usually taught at a higher level in an abstract mathematics course. Because students see the value of using modular arithmetic in this concrete setting, they can appreciate the value of abstraction. Students make sense of and connections between representations.

3. Construct viable arguments and critique the reasoning of others.

CryptoClub is a safe place for students to solve problems, explain their solutions and compare methods and strategies.

4. Model with mathematics.

In CryptoClub students use arithmetic models for letters to solve encrypted messages.

5. Use appropriate tools strategically.

The CryptoClub student is presented with an arsenal of tools, including online applications, for cracking messages and often needs to decide which ones to apply effectively.

6. Attend to precision.

CryptoClub students need to think about accuracy and efficiency when counting and calculating to encrypt and decrypt messages.

7. Look for and make use of structure.

Discussion of each cipher in the CryptoClub curriculum begins with an 'Exploring Patterns' activity that encourages students to think about the importance of patterns and structure in cryptology. They must make use of those structures to solve encrypted messages

8. Look for and express regularity in repeated reasoning.

In CryptoClub students create and justify rules and generalizations while encrypting and decrypting messages.

Standards for Mathematical Content

References to examples from the CryptoClub Cipher Handbook are given parenthetically

Grade 4. Operations and Algebraic Thinking 4.OA

3. *Solve multistep word problems posed with whole numbers and having whole-number answers using the four operations, including problems in which remainders must be interpreted. Represent these problems using equations with a letter standing for the unknown quantity. Assess the reasonableness of answers using mental computation and estimation strategies including rounding.*

All the arithmetic ciphers, additive, multiplicative and affine, require an understanding of modular arithmetic. Encrypting and decrypting with these ciphers encourages the use of mental computation, including estimation strategies. **(Arithmetic Ciphers, Chapter 2, 4, 6)** Division with remainder is one of the main tools used to operate in Mod 26 arithmetic. **(pages 43-44)** For example, a student might find 120 (mod 26) using a standard division algorithm.

5. Generate a number or shape pattern that follows a given rule. Identify apparent features of the pattern that were not explicit in the rule itself.

Learning each cipher in CryptoClub involves looking for patterns in the cipher table and in encrypted messages. **(Throughout, especially pages 3, 13, 37, 41, 46, 51ff, 67, 74ff)**

Grade 5. Operations and Algebraic Thinking 5.OA

Write and interpret numerical expressions.

1. *Use parentheses, brackets, or braces in numerical expressions, and evaluate expressions with these symbols.*
2. *Write simple expressions that record calculations with numbers, and interpret numerical expressions without evaluating them.*

Students are encouraged to write expressions to show calculations and to use algebraic rules to simplify calculations. **(Pages 19-20, 44, 48-49, 52, 72, 75)**

Analyze patterns and relationships.

3. *Generate two numerical patterns using two given rules. Identify apparent relationships between corresponding terms. Form ordered pairs consisting of corresponding terms from the two patterns, and graph the ordered pairs on a coordinate plane. For example, given the rule "Add 3" and the starting number 0, and given the rule "Add 6" and the starting number 0, generate terms in the resulting sequences, and observe that the terms in one sequence are twice the corresponding terms in the other sequence. Explain informally why this is so.*

In exploring patterns for multiplicative and affine ciphers, students generate this type of number patterns in mod 26. **(Chapter 3, 6; especially pages 41 and 67)**

Grade 5. Number and Operations in Base Ten 5.NBT

5. Fluently multiply multi-digit whole numbers using the standard algorithm.

All the arithmetic ciphers, additive, multiplicative, and affine, require strong arithmetic skills as described here. Multiplicative and affine ciphers involve arithmetic with 3-digit numbers to encrypt and decrypt and to find multiplicative inverses. **(Chapter 2, 4, 6)**

Grade 6. Ratios and Proportional Reasoning 6.RP

Understand ratio concepts and use ratio reasoning to solve problems.

3. *Use ratio and rate reasoning to solve real-world and mathematical problems*
   c. Find a percent of a quantity as a rate per 100.

During activities on frequency of letters, students apply and reinforce their knowledge of ratios and percent, as well as their understanding of proportional reasoning. **(Throughout, explicitly in pages 33 - 37)**

Grade 6. The Number System 6.NS

Compute fluently with multi-digit numbers and find common factors and multiples.

4. *Find the greatest common factor of two whole numbers less than or equal to 100 and the least common multiple of two whole numbers less than or equal to 12. Use the distributive property to express a sum of two whole numbers 1–100 with a common factor as a multiple of a sum of two whole numbers with no common factor. For example, express 36 + 8 as 4 (9 + 2).*

Finding common factors is a useful way to find the length of the keyword when cracking a Vigenère cipher. Numbers factored in CryptoClub are often larger than 100. **(pages 63 - 64)**

Apply and extend previous understandings of numbers to the system of rational numbers.

5. *Understand that positive and negative numbers are used together to describe quantities having opposite directions or values (e.g., temperature above/below zero, elevation above/below sea level, credits/debits, positive/negative electric charge); use positive and negative numbers to represent quantities in real-world contexts, explaining the meaning of 0 in each situation.*
6. *Understand a rational number as a point on the number line. Extend number line diagrams and coordinate axes familiar from previous grades to represent points on the line and in the plane with negative number coordinates.*
   a. Recognize opposite signs of numbers as indicating locations on opposite sides of 0 on the number line; recognize that the opposite of the opposite of a number is the number itself.

Even on the first day of CryptoClub, using the cipher wheel, students see the importance of 0. Later while studying additive ciphers, students use negative numbers to help encrypt and decrypt messages. Using a number wheel model for mod 26 arithmetic reinforces number line concepts from regular arithmetic. Students understand that subtraction 'undoes' addition and that adding the additive inverse of a number is the same as subtracting. **(pages 17ff)**

Grade 7. The Number System **7.NS**

Apply and extend previous understandings of operations with fractions to add, subtract, multiply, and divide rational numbers.

1b. Understand p + q as the number located a distance |q| from p, in the positive or negative direction depending on whether q is positive or negative. Show that a number and its opposite have a sum of 0 (are additive inverses).

Students can see the similarities and differences of additive inverses in regular arithmetic and mod 26 arithmetic. **(pages 17ff)**

2a. Understand that multiplication is extended from fractions to rational numbers by requiring that operations continue to satisfy the properties of operations, particularly the distributive property, leading to products such as (–1)(–1) = 1 and the rules for multiplying signed numbers. Interpret products of rational numbers by describing real-world contexts

Using the fact that negative times negative is positive can reduce computations mod 26. Students study other properties of operations such as multiplicative inverses mod 26, which reinforces their understanding of multiplicative inverses in regular arithmetic. **(Pages 48ff, 52ff, pgs 70ff)**

Grade 7. Expressions and Equations **7.EE**

Use properties of operations to generate equivalent expressions.

1. Apply properties of operations as strategies to add, subtract, factor, and expand linear expressions with rational coefficients.

Students learn to represent encryption and decryption using algebraic expressions. Facility in handling linear expressions builds an understanding of additive and multiplicative inverses mod 26, which are used to solve linear equations. **(Pages 17ff)**

Solve real-life and mathematical problems using numerical and algebraic expressions and equations.

3. Solve multi-step real-life and mathematical problems posed with positive and negative rational numbers in any form

Cracking a message encrypted with an affine cipher is a multi-step problem that requires the use of positive and negative numbers. **(Pages 74ff)**

Grade 7. Statistics and Probability **7.SP**

Use random sampling to draw inferences about a population.

1. Understand that statistics can be used to gain information about a population by examining a sample of the population; generalizations about a population from a sample are valid only if the sample is representative of that population. Understand that random sampling tends to produce representative samples and support valid inferences.

Throughout CryptoClub, students come to understand that different letters appear with different frequencies in the English language. They learn how to use frequency analysis to help crack messages. While learning about substitution ciphers and the Vigenère cipher, students construct their own experiments to determine the frequencies of letters in a message. **(Pages 31-35)**

Grade 8. Functions **8.F**

1. Understand that a function is a rule that assigns to each input exactly one output.

Substitution ciphers are examples of functions that can be represented in tables or by formulas. Starting from the beginning students see ciphers as in-out boxes. First as letter to letter functions and later as number to number functions. The CryptoClub student learns that an encryption scheme, as represented in a cipher table can be decrypted only when the decryption is a function. They learn that multiplicative encryption has an inverse exactly when the encryption key has a multiplicative inverse. This is an introduction to the concept of bijective functions. **(Pages 34, 35, 47)**

3. *Interpret the equation y = mx + b as defining a linear function, whose graph is a straight line*
4. *Construct a function to model a linear relationship between two quantities. Determine the rate of change and initial value of the function from a description of a relationship or from two (x, y) values*

Students learn that the encryption equation for an affine cipher looks like $Y = mx + b$, where m is the multiplicative key and b is the additive key. They come to see the connection with slope and y-intercept that they learn about in algebra class. **(Pages 72 - 75)**

Grade 8. Expressions and Equations 8.EE

3. Use numbers expressed in the form of a single digit times an integer power of 10 to estimate very large or very small quantities

Calculating the number of substitution ciphers is an example of a problem where students can come to terms with very large numbers. They use factorials to generate the answer and then scientific notation to understand that the number is indeed very large, approximately 4×10^{26}

7. Solve linear equations in one variable.

8. Analyze and solve pairs of simultaneous linear equations.

One technique for cracking a multiplicative cipher involves solving a linear equation mod 26. Similar techniques for cracking affine ciphers involve solving pairs of linear equations mod 26. **(Pages 52 and 75)**

Mathematics concepts used in ciphers in CryptoClub ciphers:

The following summarizes the mathematics topics found in CryptoClub, listed by cipher.

Caesar cipher:

Functions (encrypting and decrypting), reading tables, understanding 0, problem solving, recognizing patterns in the English language.

Keyword cipher and other substitution ciphers:

Bijective functions, frequency analysis, decimals and percent, counting problems.

Additive cipher:

Addition and subtraction, additive inverse, negative numbers, introduction to modular arithmetic, division with remainder.

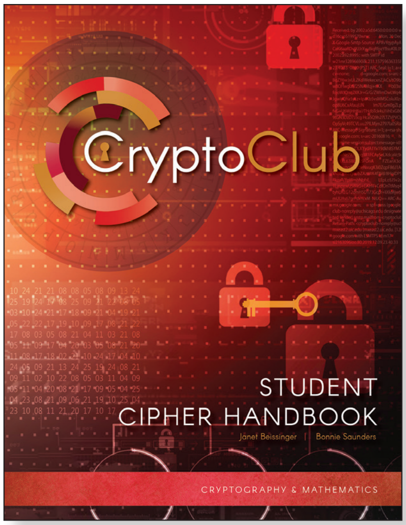
Multiplicative and affine ciphers:

Arithmetic patterns in modular arithmetic, reducing numbers mod 26 (division with remainder), bijective functions, finding multiplicative inverses mod 26, solving linear equations mod 26, solving simultaneous linear equations mod 26.

Vigenère cipher:

Frequency analysis, common factors

Program Components


CryptoClub
STUDENT
CIPHER HANDBOOK
Janet Beissinger | Bonnie Saunders
CRYPTOGRAPHY & MATHEMATICS

Student Cipher Handbook

The CryptoClub *Student Cipher Handbook* is the centerpiece of the CryptoClub curriculum. It is a student reference and workbook that is recommended for use in informal learning environments such as after-school and enrichment programs. It introduces ciphers in a way that encourages problem-solving and reasoning and provides engaging messages to encrypt, decrypt and crack. The *Student Cipher Handbook* can be used with whole-class instruction or with self-paced work in small groups.

CryptoClub
CRYPTOGRAPHY & MATHEMATICS
LEADER MANUAL
Janet Beissinger | Bonnie Saunders

Leader Manual + 3 Year License

The CryptoClub *Leader Manual* accompanies the CryptoClub *Student Cipher Handbook* and helps teachers lead a CryptoClub program. It provides suggestions for teaching, along with an answer key, and discusses connections to middle-grade mathematics. It also describes games and activities that provide students with additional practice in an engaging, informal way.

Online Resources

Flourish is an online platform that provides 24/7 access to the teacher eBook along with the following digital resources:

- Teacher Resources
- Treasure Hunt Clue Generator
- Cipher Cracking Worksheet Generator
- Jigsaw Generator