Caesar Ciphers: An Introduction to Cryptography

Purdue University GK-12 2006-07

Lead developer and contact:
Lance Bryant
Purdue GK-12 Fellow
LBRYANT@MATH.PURDUE.EDU

Co-author and instructor:
JoAnn Ward
Klondike Middle School

Table of Contents

1. Overview

This lesson takes approximately 1-2 class periods. It begins with a discussion about cryptography, the science of secrets. We discuss the importance of secrets in today's world and then focus on a system for sending secret messages used by Julius Caesar around 100 B.C. Students make a Caesar wheel used for encrypting and decrypting coded messages. Students also learn how to crack the code without knowing the encryption key.

2. Purpose

The lesson was used for several purposes.

Provide an introduction to an interesting area of mathematics. Just as chemistry, biology, and other science fields are discussed in a science class, it is important to discuss a variety of fields in mathematics. Cryptography is naturally intriguing to students and is a good example of what is done in mathematics.

Challenge students' conception of mathematics. This lesson requires little computation or number sense. In fact, there is only one number (between -25 and 25) that is used in the cipher as the encryption key. Without numbers or computation, is this mathematics? This lesson can be a good opportunity to point out that it is concepts and problem solving that drives mathematicians and not the pure joy of crunching numbers.

Make a connection between mathematics and linguistics. Connections are often made between math and science for middle school students, but it is sometimes harder to find activities that incorporate the other disciplines. This activity makes mathematics more appealing for students who are interested in language arts and the study of languages.

This lesson can be a stand alone activity. In this way it is an easy and fun lesson for the students. I used it as an icebreaker with the students. However, this lesson can easily be used as a starting point for a variety of lessons. See section 9 for a list of a few activities that can follow this activity.

3. Objectives

The objectives for this project were to:

- Introduce students to an interesting area of mathematics
- Challenge students' conception of mathematics
- Provide a connection to mathematics and linguistics
- Student analysis of the strengths and weaknesses of the Caesar cipher and using this analysis to both compromise the system and improve it.

4. Indiana Standards Met

4.1. Math

4.1.1. Standard 7 - Problem Solving

Students make decisions about how to approach problems and communicate their ideas.

8.7.1 Analyze problems by identifying relationships, telling relevant from irrelevant information, identifying missing information, sequencing and prioritizing information, and observing patterns.
Example: Solve the problem: “For computers, binary numbers are great because they are simple to work with and they use just two values of voltage, magnetism, or other signal. This makes hardware easier to design and more noise resistant. Binary numbers let you represent any amount you want using just two digits: 0 and 1. The number you get when you count ten objects is written 1010. In expanded notation, this is $1 \leq 2^3 + 0 \leq 2^2 + 1 \leq 2^1 + 0 \leq 2^0$. Write the number for thirteen in the binary (base 2) system.” Decide to make an organized list.

8.7.2 Make and justify mathematical conjectures based on a general description of a mathematical question or problem.
Example: In the first example, if you have only two symbols, 0 and 1, then one object: 1, two objects: 10, three objects: 11, four objects: 100. Predict the symbol for five objects.

8.7.3 Decide when and how to divide a problem into simpler parts.
Example: In the first example, write expanded notation for the number five in base 2; begin with the fact that 5 = 4 + 1.

Students use strategies, skills, and concepts in finding and communicating solutions to problems.

8.7.4 Apply strategies and results from simpler problems to solve more complex problems.
Example: In the first example, write the first five numbers in base 2 notation and look for a pattern.

8.7.5 Make and test conjectures using inductive reasoning.
Example: In the first example, predict the base 2 notation for six objects, then use expanded notation to test your prediction.

8.7.6 Express solutions clearly and logically using the appropriate mathematical terms and notation. Support solutions with evidence in both verbal and symbolic work.
Example: In the first example, explain how you will find the base two notation for thirteen objects.

8.7.7 Recognize the relative advantages of exact and approximate solutions to problems and give answers to a specified degree of accuracy.
Example: Measure the length and width of a basketball court. Use the Pythagorean Theorem to calculate the length of a diagonal. How accurately should you give your answer?

8.7.8 Select and apply appropriate methods for estimating results of rational-number computations.

Example: Use a calculator to find the cube of 15. Check your answer by finding the cubes of 10 and 20.

8.7.9 Use graphing to estimate solutions and check the estimates with analytic approaches.
Example: Use a graphing calculator to draw the straight line $x + y = 10$. Use this to estimate solutions of the inequality $x + y > 10$ by testing points on each side of the line.

8.7.10 Make precise calculations and check the validity of the results in the context of the problem.
Example: In the first example, list the first thirteen numbers in base 2 notation. Use patterns or expanded notation to confirm your list.

Students determine when a solution is complete and reasonable and move beyond a particular problem by generalizing to other situations.

8.7.11 Decide whether a solution is reasonable in the context of the original situation.
Example: In the basketball court example, does the accuracy of your answer depend on your initial measuring?

8.7.12 Note the method of finding the solution and show a conceptual understanding of the method by solving similar problems.
Example: In the first example, use your list of base 2 numbers to add numbers in base 2.
Explain exactly how your addition process works.

5. Methods

5.1. Materials & Resources

The materials required for this activity are:
- Card Stock
- Scissors
- Paper fasteners

5.1.1. Introduction to the Activity (1 period)

The class starts with a discussion about secrets, who needs to keep secrets and who might be interested in finding out someone else's secrets. We then tell the students that there is a science of secrets called cryptography just like biology is the science of living things (one could use the term cryptology so that students make the connection that –logy refers to the science or study of something). Then we briefly discuss the life of Julius Caesar, in particular his military career. He often needed to send messages to his soldiers and used a coding system that today bears his name. We then discuss this system and show the students how it works.

The next step is to have the students construct a wheel that will help them encode and decode messages using Caesar's cipher. This requires that the students cutout the circles on the Caesar Wheel worksheet in section seven and put them together with a paper fastener. Then the students need to label the wheel according to the directions on the handout.

The class period can be concluded with the students practicing encoding and decoding messages. The easiest mistake to make is confusing the plaintext alphabet with the ciphertext alphabet.

5.1.2. Cracking Caesar's cipher (1 period)

The students should have an understanding of how the cipher works and be able to encode and decode messages using the wheel. Now it is time to discuss the strengths and weaknesses of the cipher. We ask the students what is good about this cipher. One of the strengths is how easy it is to use. The encryption key is one number between -25 and 25. Also encryption and decryption can be done very quickly using the wheel. This ease of use would be important for Caesar since his soldiers were likely uneducated and not capable of using a complicated coding system (In fact I read an article stating that during WWII, Russian soldiers were having trouble using advanced coding systems so the Russian military started using Caesar's cipher for some of their communications).

What about the weaknesses of the cipher. The most pressing issue for any coding system is security, can the system be deciphered without knowing the encryption key. Here we turn the discussion over to the students and have them analyze the cipher for exploitable features. There are two that are good to consider. First, there are only 25 possible encryption keys. Thus each could be tried until the message was decoded. Another thing to notice is that if we know how one letter should be deciphered, then we can determine the shift and decipher the entire message. Students are quick to say that since the message is composed of English words, there should be a way to use the structure of the English language to guess the shift. If the students struggle at this point, consider a specific example of a coded word and ask the class which letter appears most often in the code word. If we studied the English language perhaps we could determine which letter is used most often. Then our first guess would be that this code letter would be deciphered as the most used letter in the English alphabet. If this does not work, then we could try the second, and so on. The important thing for picking coded messages for this day is that the most used letter deciphers as e, a, t, n; the most used letters in English (in that order). The period concludes with the students getting a worksheet where they will mainly be cracking Caesar ciphers (see section 7).

6. Scope

This activity is best if done over two days. However this can be shortened. With an accelerated math class this can be done in one period. With other students, if the wheels are made in the last 10-15 minutes of the previous period, the activity can be done in one period.

7. Activities, worksheets, and templates

The following MS Word worksheets are available for use in this lesson:


Caesar Wheel

The following images, documents, PDFs are available for this lesson:

Cryptography Worksheets (there are two versions, the first is slightly harder)

Caesar Wheel

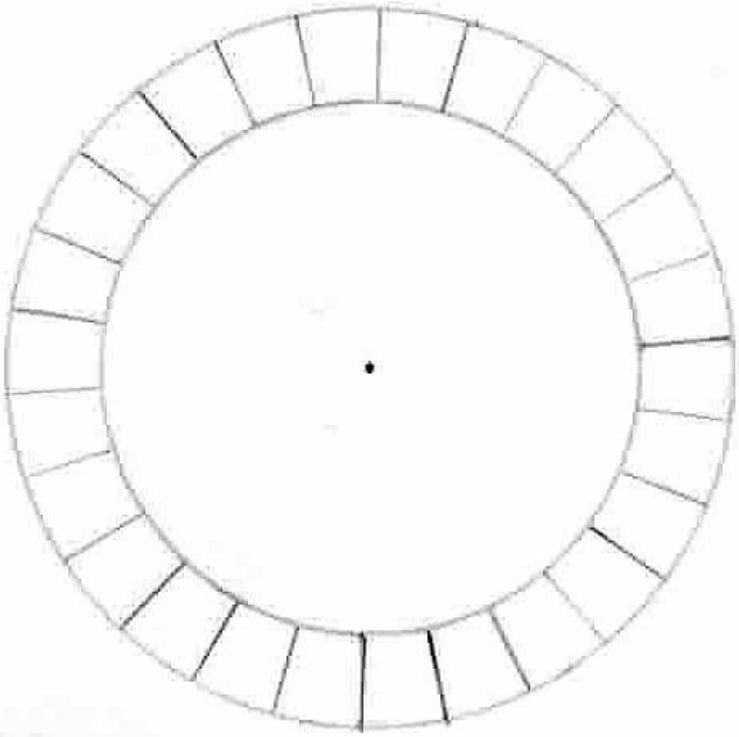
Directions:

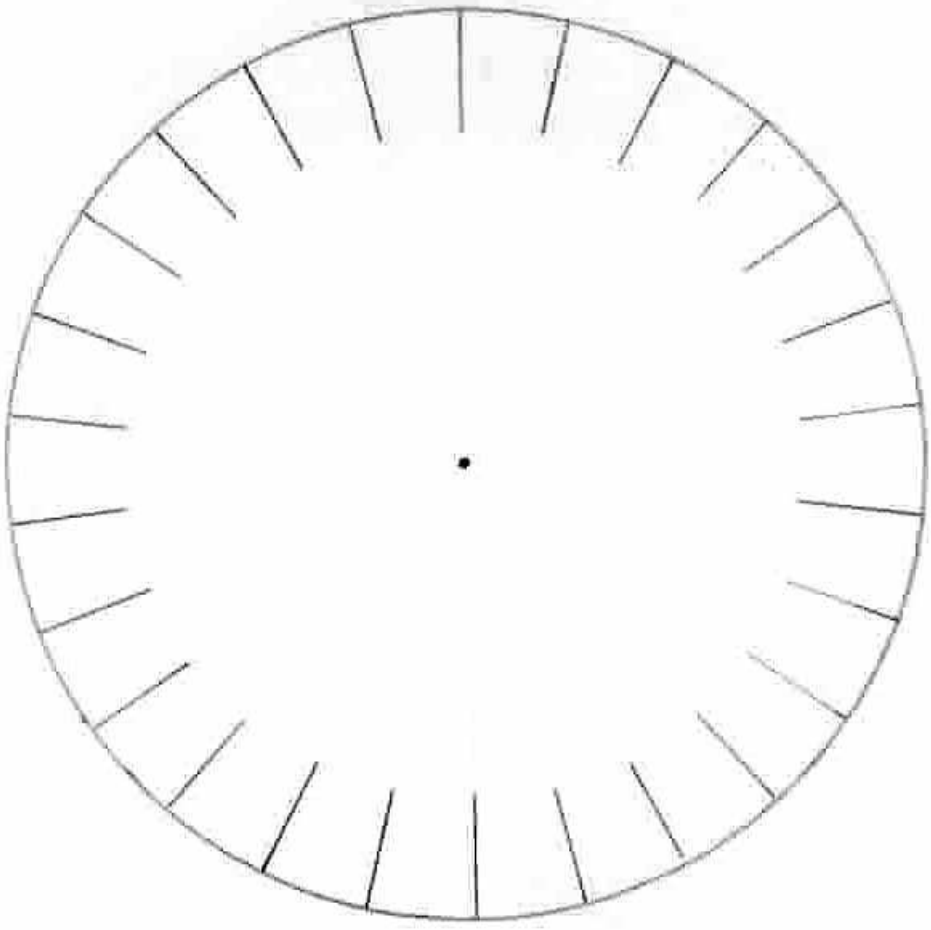
1. Carefully cut around the two circles
2. Write the alphabet in BLACK around the SMALL circle
3. Write the alphabet in RED around the LARGE circle
4. Fix the small circle onto the big circle using a paper fastener through the center (marked with a dot)

You are ready to use your Caesar Wheel

REMEMBER the plaintext letters are written in BLACK, the ciphertext letters are written in RED

ENCIPHERING = BLACK → RED
DECIPHERING = RED → BLACK





CRYPTOGRAPHY WORKSHEET

Name: _____ Class: _____

Encode the following messages.

(1) Caesar cipher with shift +3

hello tom

(2) Caesar cipher with shift +12

klondike nuggets

Decode the following messages.

(3) Caesar cipher with shift +5

ltytufwnx

(4) Caesar cipher with shift +21 = −5

adiyevhznwjiy

(5) Caesar cipher with shift +24 = −2

ncwrmlkyllgle

(6) (a) Caesar cipher with shift $+23 = -3$

aliip

(b) Caesar cipher with shift $+4$

aliip

(7) Caesar cipher using frequency analysis. Shift is _____

kbkxeutk

(8) Caesar cipher using frequency analysis. Shift is _____

espntaspcsldmppymczvpy

(9) Caesar cipher using frequency analysis. Shift is _____

kgyezuhxkgq

(10) Caesar cipher using frequency analysis. Shift is _____

xskixxsxlisxlivwmhi

CRYPTOGRAPHY WORKSHEET

Name: _____ Class: _____

Encode the following messages.

(1) Caesar cipher with shift +3

hello tom

khoorwrp

(2) Caesar cipher with shift +12

klondike nuggets

wxazpuwqzgssqfe

Decode the following messages.

(3) Caesar cipher with shift +5

ltytufwnx

go to Paris

(4) Caesar cipher with shift +21 = −5

adiyevhznwjiy

find James Bond

(5) Caesar cipher with shift +24 = −2

ncwrmlkyllgle

Peyton Manning

(6) (a) Caesar cipher with shift $+23 = -3$

aliip

dolls

(b) Caesar cipher with shift $+4$

aliip

wheel

(7) Caesar cipher using frequency analysis. Shift is $\underline{+6}$

kbkxeutk

everyone (e)

(8) Caesar cipher using frequency analysis. Shift is $\underline{+11}$

espntaspcsldmppymczvpy

the cipher has been broken (e)

(9) Caesar cipher using frequency analysis. Shift is $\underline{+6}$

kgyezuhxkgq

easy to break (e and a)

(10) Caesar cipher using frequency analysis. Shift is $\underline{+4}$

xskixxsxlisxlivwmhi

to get to the other side (t)

CRYPTOGRAPHY WORKSHEET

Name: _____ Class: _____

Encode the following messages.

(1) Caesar cipher with shift +3

hello tom

(2) Caesar cipher with shift +12

klondike nuggets

Decode the following messages.

(3) Caesar cipher with shift +5

ltytufwnx

(4) Caesar cipher with shift +21 = −5

adiyevhznwjiy

(5) Caesar cipher using frequency analysis. Shift is _____

kbkxeutk

(6) Caesar cipher using frequency analysis. Shift is _____

espntaspcsldmppymczvpy

(7) Caesar cipher using frequency analysis. Shift is _____

kgyezuhxkgq

(8) Caesar cipher using frequency analysis. Shift is _____

ncwrmlkyllgleylbhmckmlryly

(9) Caesar cipher using frequency analysis. Shift is _____

xskixxsxlisxlivwmhi

(10) (a) Caesar cipher with shift $+23 = -3$

aliip

(b) Caesar cipher with shift $+4$

aliip

CRYPTOGRAPHY WORKSHEET

Name: _____ Class: _____

Encode the following messages.

(1) Caesar cipher with shift +3

hello tom

khoorwrp

(2) Caesar cipher with shift +12

klondike nuggets

wxazpuwqzgssqfe

Decode the following messages.

(3) Caesar cipher with shift +5

ltytufwnx

go to Paris

(4) Caesar cipher with shift +21 = −5

adiyevhznwjiy

find James Bond

(5) Caesar cipher using frequency analysis. Shift is $\underline{+6}$

kbkxeutk

everyone (e)

(6) Caesar cipher using frequency analysis. Shift is $\underline{+11}$

espntaspcsldmppymczvpy

the cipher has been broken (e)

(7) Caesar cipher using frequency analysis. Shift is $\underline{+6}$

kgyezuhxkgq

easy to break (e and a)

(8) Caesar cipher using frequency analysis. Shift is $\underline{+24 = -2}$

ncwrmlkyllgleylbhmckmlryly

Peyton Manning and Joe Montana (n)

(9) Caesar cipher using frequency analysis. Shift is $\underline{+4}$

xskixxsxlisxlivwmhi

to get to the other side (t)

(10) (a) Caesar cipher with shift $+23 = -3$

aliip

dolls

(b) Caesar cipher with shift $+4$

aliip

wheel


Worksheet 1


Worksheet 1 (answers)


Worksheet 2


Worksheet 2 (answers)

8. Evaluation

The evaluation in this lesson was based on the worksheets.

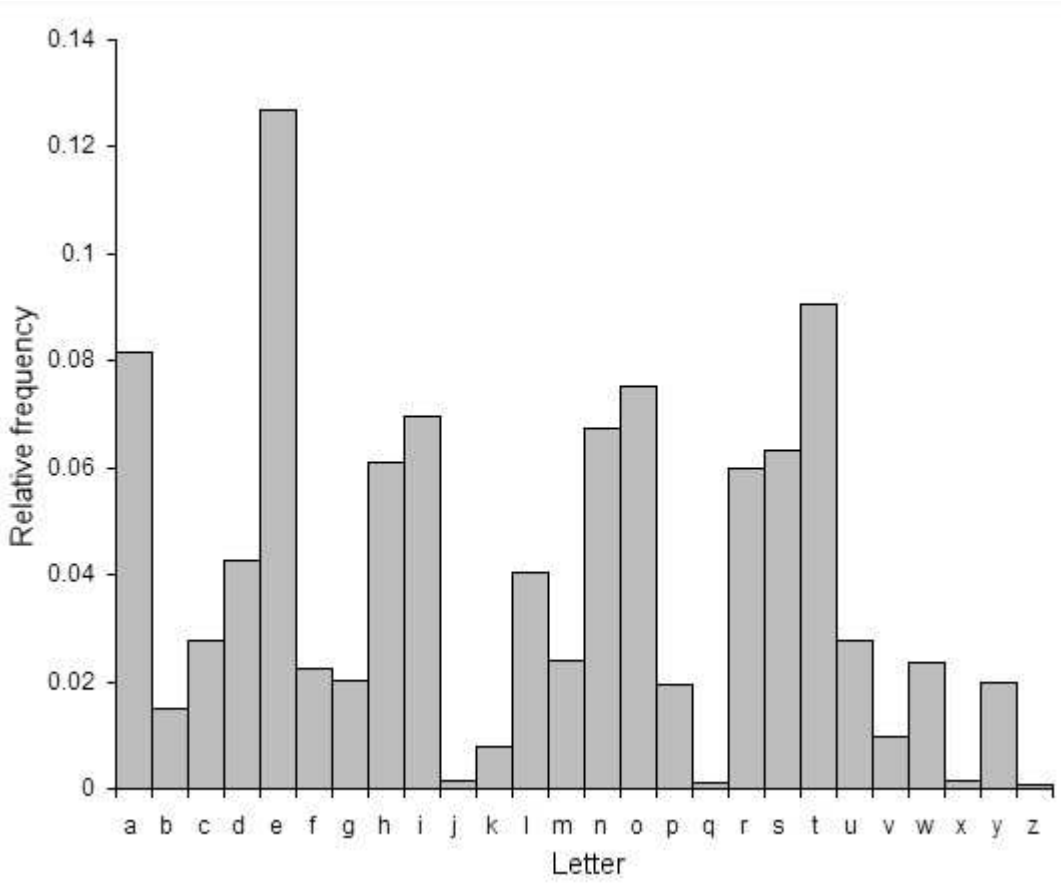
9. Extensions

9.1. Modular arithmetic

The most common example for teaching modular arithmetic to children is a clock. We count 1 to 12, but instead of going to 13, we start back at 1 again. If you are interested in teaching modular arithmetic, this activity can be slightly altered and provide an application. Number the letters of the alphabet 0 through 25 (or 1 through 26). Then when we shift for the cipher, the number 25 might become 30 for example. But this does not correspond to a letter. Thus we use modular arithmetic to see that 25 shifts to 4.

9.2. Bar graphs and frequency analysis

At the end of the activity students will have mastered cracking Caesar's cipher when the most used letter in the codeword deciphers to one of the most used letters in the English alphabet. Now ask the students how we can crack the cipher if this does not happen. This leads to making a bar graph that determines the frequency of use of each letter in the English alphabet. If the same is done for the coded message, then the shift can be determined by comparing the features of the two graphs. To make a frequency table for English, you could have each student pick a certain length of text (say two paragraphs) and make a bar graph showing the occurrence of each letter. You can then have students compare their graphs. How can each graph represent the frequency of use for the letters of the alphabet if the graphs are different? This leads to the notion of sampling size. You can also discuss the different types of writing that may have been used. What is the difference between novels, magazines, newspapers, blogs, or other sources of text in English? This can also be done with Spanish (and other languages) and compare the bar graphs of English and Spanish. Here is a commonly used distribution graph for English



Graphs for other languages can be found at
HTTP://PEOPLE.BATH.AC.UK/TAB21/FORCRYPT.HTML

9.3. Kid-RSA

To demonstrate the importance of mathematics, this lesson can be followed by another cryptography activity later in the year. The Caesar cipher was used at least as early as 100 B.C. Now we can compare this with a coding system developed in the 1970's known as RSA. This coding system uses mathematics in a critical way, and is much more secure. There is a kid-friendly version of RSA called kid-RSA developed by Neal Koblitz. More information about this can be found at HTTP://WWW.MATH.WASHINGTON.EDU/~KOBLITZ/CRLOGIA.HTML