The Great Eggscape, Part II: The Foo Yung Rescue

Target Audience

Geared toward middle school students, this lesson addresses State of Indiana standards in Science, Math, and English while engaging students in an adventure in which they learn about the relevant topic of cryptology.

This lesson can be modified to fit older audiences by:

- Allowing students to choose which cipher they would like to use to encipher their message
- Having students use the Hill Cipher which incorporates matrix operations (see "Cryptography Resources" at end of lesson)
- Have students write their own missions in which cryptography or steganography must be used
- Have students develop a mission that is based on a historical event in which cryptography was used

Mission Synopsis

Poor Prince Eggbert! Only a few days ago, Eggbert was narrowly rescued from the clutches of the evil chef Dr. Breakfast. While on his way back to his father's kingdom, Prince Eggbert's entourage was ambushed by Dr. Breakfast's evil henchmen. Eggbert and a few of his personal guard have narrowly escaped, but they know that Dr. Breakfast is close behind, hoping to recapture and ransom Eggbert. After conferring on the situation, Eggbert and his remaining entourage decide that the best course of action they can take is to hide in the Foo Yung forest and wait for reinforcements.

As one of the bravest in Eggbert's personal guard, your mission, should you choose to accept it, is to send a secret message to King Meringue, Eggbert's father. In this message, you must indicate where Eggbert is hiding in the forest. If Dr. Breakfast intercepts and understands this message, he will be able to track down and capture Eggbert. Thus, you must use steganography or cryptography to encode and protect your message. If you are successful, you will be handsomely rewarded by King Meringue, Eggbert's father.

Indiana Standards Addressed

Science:

6.1.1 Explain that some scientific knowledge, such as the length of the year, is very old and yet is still applicable today. Understand, however, that scientific knowledge is never exempt from review and criticism.

7.1.5 Identify some important contributions to the advancement of science, mathematics, and technology that have been made by different kinds of people, in different cultures, at different times.

7.72 Use different models to represent the same thing, noting that the kind of model and its complexity should depend on its purpose.

8.2.6 Write clear, step-by-step instructions (procedural summaries) for conducting investigations, operating something, or following a procedure.

Mathematics:

6.2.1 Add and subtract positive and negative integers.

6.3.1 Write and solve one-step linear equations and inequalities in one variable and check the answers.

6.3.2 Write and use formulas with up to three variables to solve problems.

6.3.9 Investigate how a change in one variable relates to a change in a second variable.

6.7.1 Analyze problems by identifying relationships, telling relevant from irrelevant information, identifying missing information, sequencing and prioritizing information, and observing patterns.

6.7.4 Apply strategies and results from simpler problems to solve more complex problems.

6.7.5 Express solutions clearly and logically by using the appropriate mathematical terms and notation. Support solutions with evidence in both verbal and symbolic work.

6.7.10 Decide whether a solution is reasonable in the context of the original situation.

7.2.1 Solve addition, subtraction, multiplication, and division problems that use integers, fractions, decimals, and combinations of the four operations.

7.3.1 Use variables and appropriate operations to write an expression, a formula, an equation, or an inequality that represents a verbal description.

7.3.3 Use correct algebraic terminology, such as variable, equation, term, coefficient, inequality, expression, and constant.

7.7.1 Analyze problems by identifying relationships, telling relevant from irrelevant information, identifying missing information, sequencing and prioritizing information, and observing patterns.

7.7.4 Apply strategies and results from simpler problems to solve more complex problems.

7.7.5 Make and test conjectures by using inductive reasoning.

7.7.6 Decide whether a solution is reasonable in the context of the original situation.
7.7.12 Note the method of finding the solution and show a conceptual understanding of the method by solving similar problems.
8.7.1 Analyze problems by identifying relationships, telling relevant from irrelevant information, identifying missing information, sequencing and prioritizing information, and observing patterns.
8.7.4 Apply strategies and results from simpler problems to solve more complex problems.
8.7.5 Make and test conjectures by using inductive reasoning.
8.7.12 Note the method of finding the solution and show a conceptual understanding of the method by solving similar problems.

English:
6.1.1 Read aloud grade-level-appropriate poems, narrative text (stories), and expository text (information) fluently and accurately and with appropriate timing, changes in voice, and expression.
6.1.3 Recognize the origins and meanings of frequently used foreign words in English and use these words accurately in speaking and writing.
6.1.5 Understand and explain slight differences in meaning in related words.
6.2.5 Follow multiple-step instructions for preparing applications.
7.1.2 Use knowledge of Greek, Latin, and Anglo-Saxon roots and word parts to understand subject-area vocabulary (science, social studies, and mathematics).
7.1.3 Clarify word meanings through the use of definition, example, restatement, or through the use of contrast stated in the text.
8.1.4 Verify the meaning of a word in its context, even when its meaning is not directly stated, through the use of definition, restatement, example, comparison, or contrast.

Materials

- Activity Sheet 1: Methods of Secret Communications
- Chalkboard, Whiteboard, or Overhead Transparency

Procedures

1. After debriefing the class on "The Great Eggscape" activity (optional), read the mission synopsis to the entire class or ask students to take turns reading the activity sheet aloud.
2. Break the class into small groups of 3-5 students. Use team roles and responsibilities, if appropriate (recorder, reporter, timekeeper, etc.)

3. Hand out Activity Sheet #1. Ask students to take turns reading the activity sheet aloud. If appropriate, discuss the origins of the words "steganography" and "cryptology." Ask students if they can think of any other words that use the same roots. Periodically stop to check for comprehension by asking questions and providing examples of ciphers.
4. Elicit example ciphers from students, if appropriate.
5. Focus on the Caesar cipher. On the board, show an example that demonstrates how to change the alphabet into numbers (with a=0, z=25) and how the alphabet cycles (i.e. if your key is to shift every letter 2 spaces, then Z would become B). If appropriate, and if time permits, discuss how this is an example of modular arithmetic, discuss other examples (i.e. time), and show students how to write the operation.
6. Explain the mission:
    i. Each group must pick a spot in the classroom as a hideout for Eggbert and his entourage.
    ii. Each group must then construct a short, easy to understand message that tells King Meringue where and how to find Eggbert. The teacher should emphasize the procedural nature of the message.
    iii. Next, each group should pick a key (no greater than 25 and no less than -25) and encode the message using the Caesar cipher, making sure to keep their key secret from the other groups. The group should then write their cipher and key in the form of a mathematical expression (this may be changed to a sentence for younger audiences).
7. Once all of the groups are finished encoding their messages, a volunteer from each group should write their encoded message on the chalkboard, whiteboard, or overhead transparency.
8. Finally, each group must attempt to decrypt the other group's messages and to find the expression (or sentence). The first group to decrypt all the messages receives a handsome "prize" from King Meringue.
9. At the end of the class, time permitting, a representative from each group should present their message and the method they used to encode it.

Assessment Options:

- Oral Report: Explain your team's rationale for choosing and using the given key.
- Essay: For each message, explain your method of decrypting the message (see included rubric).
- Optional: Assign awards for team-work, creativity, and innovation.

Extension Ideas

- English, Vocabulary: Incorporate the six highlighted words into vocabulary studies.
- English, Creative Writing: Short stories that fill out and chronicle the Great Eggscape adventures.

- English, Writing & Research: Research topics related to cryptography and steganography.
- Social Studies, Historical Knowledge: Research the historical uses of cryptography (see resources below).
- Social Studies, Civics and Government/Individuals, Society, and Culture: Investigate legal, governmental, and ethical issues surrounding the uses of cryptography and steganography.
- Mathematics: Use substitution cryptography to learn about frequency distribution, and frequency tables.
- Mathematics: Use the Vigenere Cipher, a polyalphabetic cipher, to learn about data modeling.
- Mathematics, Problem Solving: Create your own cipher.
- Science, Scientific Inquiry: Use a systematic scientific method to analyze an encoded message.

Cryptography Resources

- CERIAS K-12 Education Website: http://www.cerias.purdue.edu/k12/
- National Cryptologic Museum: http://www.nsa.gov/museum/
- Spy Letters of the American Revolution: http://www.si.umich.edu/spies/
- Classic Ciphers: http://raphael.math.uic.edu/~jeremy/crypt/intro.html
- Lessons that discuss and incorporate the Hill Cipher:
  http://www.nsa.gov/programs/mepp/hs/alg14.pdf
  http://www.wpi.edu/Academics/Depts/Math/CIMS/imphss/modules01/enigma.doc

Call to Teachers

We at CERIAS would appreciate any feedback regarding this lesson plan as well as the suggested extension ideas. If you would like to help CERIAS improve this and other information security related lesson and unit plans, please contact Matt Rose at mrose@cerias.purdue.edu.

Rubric Made Using:
RubiStar (http://rubistar.4teachers.org)

Explanation of Deciphering Methods

Teacher Name: _____

Student Name: _____

CATEGORY	4	3	2	1
Explanation	Explanation is detailed and clear.	Explanation is clear.	Explanation is a little difficult to understand, but includes critical components.	Explanation is difficult to understand and is missing several components OR was not included.
Strategy/Procedures	Typically, uses an efficient and effective strategy to solve the problem(s).	Typically, uses an effective strategy to solve the problem(s).	Sometimes uses an effective strategy to solve problems, but does not do it consistently.	Rarely uses an effective strategy to solve problems.
Mathematical Terminology and Notation	Correct terminology and notation are always used, making it easy to understand what was done.	Correct terminology and notation are usually used, making it fairly easy to understand what was done.	Correct terminology and notation are used, but it is sometimes not easy to understand what was done.	There is little use, or a lot of inappropriate use, of terminology and notation.
Neatness and Organization	The work is presented in a neat, clear, organized fashion that is easy to read.	The work is presented in a neat and organized fashion that is usually easy to read.	The work is presented in an organized fashion but may be hard to read at times.	The work appears sloppy and unorganized. It is hard to know what information goes together.

Activity Sheet #1

Steganography: Steganography is a type of secret communication where the existence of a message is concealed. You can remember this by looking at the two parts of the word "stegano – graphy." Both parts are of Greek origin. The Greek word steganos means "covered," and the Greek word graphein means "to write." Thus, a literal translation of steganography could be "covered writing." The most simple form of steganography is hiding messages and images within larger pictures, such as the hidden symbols that can be found in the US dollar bill (can you find the spiders?).

There are several different forms of steganography:

Invisible Inks: Even in ancient times, invisible inks were used to hide messages. One example is using lemon juice on off-white parchment; only by holding the parchment up to a light will you be able to see the secret message.

Music Cipher: In this method, notes on a scale correspond with letters in the alphabet. The message can be communicated through sheet music, or actual sound.

Null Cipher: A null cipher is a type of hidden message where the real message is "camouflaged" in an innocent sounding message. A famous example of a null cipher is one sent by a German Spy in WWII: *Apparently neutral's protest is thoroughly discounted and ignored. Isman hit hard. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.* Taking the second letter in each word the following message emerges:

Pershing sails from NY June 1.

Digital Images: This fairly new method of steganography exploits the properties of digital images to hide messages. If you zoom in close enough on a digital image, you will notice that the image is really composed of thousands of different-colored dots. It is possible to change up to half of the dots and trick the human eye into seeing only the surface image. If a person (or a computer) knows what to look for, he can also see the hidden picture.

A related but separate technology involves watermarking. Watermarking is a technique that embeds an image inside another image. For instance, many pieces of fine stationary have watermarks. US paper currency also uses watermarks; hold a new ten or twenty-dollar bill up to a light source to reveal the watermarks.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Cryptography: Cryptography is a type of secret communication that uses encryption, which is a way to scramble the real message, also known as the plain text message, into a meaningless cipher text, something that looks like a jumble of letters or numbers. The only way to decrypt, or figure out, the real message, is to use a "key":

You can remember what cryptography means by looking at the two parts of the word. The Greek word kryptos, which means "secret" is combined with the Greek word logos, which means "word." As with steganography, there are several different types of encryption:

The Caesar Cipher: Named after the Roman Emperor Julius Caesar, this ancient cipher uses a very simple method. The first step is to assign a number to each letter of the alphabet, where A = 0, and Z = 25. The next step is to pick a "key." If the key equals 5, then the plaintext (normal) alphabet becomes the ciphertext alphabet shown below:

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

So how can you "break" a Caesar cipher? First, look for breaks between words. If you see one letter standing alone, there is a good chance that it is "I" or "A." Also, look for repeated letters and double letters. (HINT: Did you know that there are no words in English that have a double Q in them?)

Keyword Substitution: A keyword substitution uses, yes, a key word, such as "count" instead of a number for the key. To write a keyword cipher, first write out the alphabet, then write the keyword directly below the first few letters of the alphabet. Complete the second row by writing, in order, the unused letters.

Thus, if we use "count" as our keyword, our keypad becomes this:

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
c o u n t a b d e f g h I j k l m p q r s v w x y z

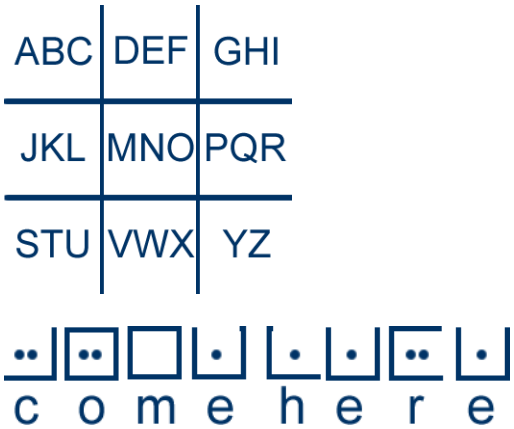
The keyword does not have to start at the beginning of the alphabet, though. For example, imagine that our keyword is still count, but we also have to know that it starts at "k" (note that the ciphertext alphabet wraps around the word "count"):

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
m p q r s v w x y z c o u n t a b d e f g h I j k l

Breaking a keyword code without the key is very difficult. However, you can use the same methods that are suggested for breaking Caesar Ciphers.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

The Pigpen Cipher: This very ancient cipher is the combination of a tic-tac-toe board and the alphabet. Each part of the alphabet is represented by the part of the "pigpen" that surrounds it. If the letter you need is the second one in that area of the pen, then the code represents this with a dot as well; if the letter you need is the third one in that area of the pigpen. Here is an example of a pigpen cipher:



Breaking pigpen ciphers is not very difficult, as long as you can recognize the "letters"; sometimes pigpen ciphers are hidden within steganographic messages!

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu